Enhancing the Security of Cloud Computing by Building Hybrid Cryptography Algorithms

Tahera Begum
Lecturer
Dept. of Information & Communication Technology
Moinuddin Adarsha Mohila College
Sylhet-3100, Bangladesh

Md. Ebrahim Hossain
Assistant Professor
Dept. of Computer Science & Engineering
Leading University
Sylhet-3100, Bangladesh

ABSTRACT
In the present circumstances, the Cloud Computing is very well-known and flexible technology. It provides massive data centre to handle the large amount of information. The Cloud Computing benefits the organizations to handle their large volume of information. The major issue in cloud computing is data security, because most of the customers are sharing same cloud. This study aims at designing a new security method by using a hybrid cryptosystem, for data security in the cloud. The necessity for the current investigation is to protect data from unauthorized access or hackers in cloud at the time of data transmission by encrypting the user data. Cloud computing constitutes several security issues including data access control, identity management, auditing, integrity control and risk management. So, this hybrid cryptosystem is designed and comprises of both symmetric and asymmetric cryptography algorithm in which Blowfish symmetric algorithm deals with data confidentiality whereas, RSA asymmetric algorithm deals with an authentication. This method also includes the Secure Hash Algorithm – 256 (SHA-256) for data integrity. This study concluded that the proposed method provides high security on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, like net, server, and storage application.

Keywords
Cloud computing, Cryptography, Blowfish, RSA, SHA-256

1. INTRODUCTION

1.1 Cloud computing
Now-a-days most people and firms are migrating to cloud because the cloud is much cheaper and convenient. For some computer owners, finding enough storage space to hold all the data they acquired is a real challenge. Some people buy large quantity of data or larger space hard drives and still faced with storage space challenges. Most computer owners that are eager to make space for new information might delete entire folders worth of old files. With this new technology of cloud computing people are finding it much easier to buy huge amount of space on cloud, this Cloud really refers to saving data to an off-site storage system maintained by a third party. Storing data in a remote location instead of storing information on our computer's hard drive or other local storage unit.

1.1.1Characteristics of cloud computing:
1.1.1.1 Resources pooling
Resource pooling means that a cloud service provider can share resources among several clients, providing everyone with a different set of services as per their requirements.

1.1.1.2 On-demand self-service
It enables the client to constantly monitor the server uptime, abilities, and allotted network storage.

1.1.1.3 Scalability and rapid elasticity
This cloud characteristic enables cost-effective running of workloads that require a vast number of servers but only for a short period.

1.1.1.4 Measured and reporting service
Measuring & reporting service enable both the provider and the client to monitor and report what services have been used and for what purpose.

1.1.1.5 Security
Cloud services create a copy of the data that is stored to prevent any form of data loss. If one server loses the data by any chance, the copy version is restored from the other server. This feature comes handy when several users work on a particular file in real-time and a file suddenly gets corrupted.

1.1.1.6 Large network access

The client can access the cloud data or transfer the data to the cloud from any place just with a device and internet connection.

1.1.1.7 Economical
There is no covered up or additional charge which needs to be paid. The administration is economical, and often, some space is allotted for free.

1.1.2 Deployment models
There are four deployment models in cloud computing. These are:

1.1.2.1 Private cloud: Private Cloud is the one in which cloud infrastructure is established within the organization and provides limited access to the users. Since, only privileged users can access the resources on the cloud, it is considered as most secure of all other deployment models. It is deployed where the number of users accessing the information is small.

1.1.2.2 Public cloud: Public Cloud is the one in which cloud infrastructure is shared among different organizations. The public cloud is managed by some third party who lease out the resources to the organizations as per their demand. Hence, the public cloud supports the feature pay-as-you-go pricing. Public clouds are vulnerable to data tampering as there are multiple organizations accessing the applications on sharing basis and hence, it may give easy access to some intruder.

1.1.2.3 Hybrid cloud: Hybrid Cloud is the combination of different clouds. As it is the combination of models, it offers the advantages of multiple deployment models. It provides ability to

maintain the cloud as recovery of data is easy in this cloud. It provides more flexibility.

1.1.2.4 Community cloud: Community Cloud is the one in which the cloud infrastructure is shared between different organizations with same interests or concerns. The organizations having same requirements (like security, policy, etc.) agree to share the resources from the same party or cloud vendor. Hence, community cloud is basically a public cloud with enhanced security and privacy just like that in private cloud. The infrastructure may be maintained within the organization or outside the organization.

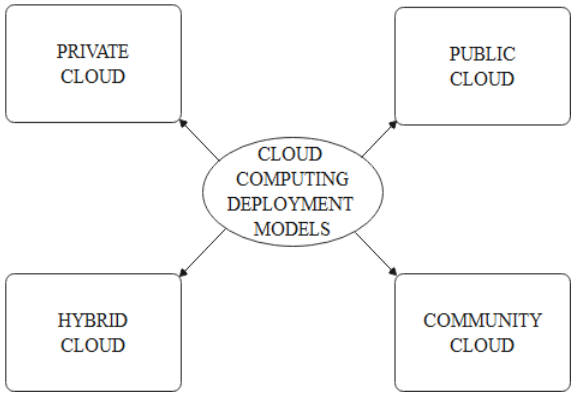

Fig 1: Cloud computing deployment models

1.1.3 Service models

Cloud computing generally provides three services, namely, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure-as-a-Service (IaaS).

1.1.3.1 Software as a Service (SaaS): SaaS permits people to use cloud-based web application. Email services such as Hotmail and Gmail are the example of Software as a Service (SaaS).

*1.1.3.2 Platform as a Service (PaaS)***:** PaaS denotes cloud platforms that provide runtime environments for developing, testing, and managing applications, examples of PaaS would include Heroku and Google App Engine.

*1.1.3.3 Infrastructure-as-a-Service (IaaS)***:** IaaS is a cloud facility and service that offers basic computing storage, infrastructure, servers and networking resources. To paraphrase this, IaaS is a virtual data centre wherein major IaaS providers include Amazon Web Services, Microsoft Azure and Google Compute Engine.

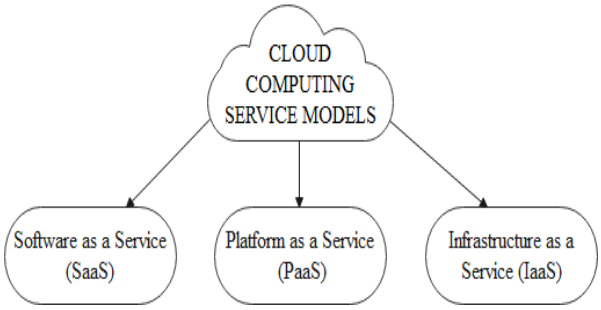

Fig 2: Cloud computing service models

1.2 Cryptography

Cryptography which plays an important role in terms of information security and protection of information. Cryptography is concerned with the process of converting ordinary plain text into unintelligible text and vice versa. It is a method of data storage and transmission in a particular form so that only those for whom it is intended can read and process it. Cryptographic algorithms are the study of techniques for ensuring the secrecy and/or authenticity of information. Cryptography classified as Symmetric cryptography and Asymmetric cryptography techniques.

1.2.1 Characteristics of cryptography:

1.2.1.1 Confidentiality

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

1.2.1.2 Integrity

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

1.2.1.3 Non-repudiation

The creator/sender of information cannot deny his or her intention to send information at later stage.

1.2.1.4 Authentication

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

1.2.2 Types of cryptography

Cryptography can be divided into following three categories depending upon the types of key used: secret key (symmetric) cryptography, public key (asymmetric) cryptography and hash functions.

1.2.2.1 Symmetric cryptography

Symmetric encryption transforms plaintext into cipher-text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher-text. The various algorithms for symmetric key cryptography are not limited to (AES, DES, and Blowfish).

1.2.2.2 Asymmetric cryptography

Asymmetric key encryption or public key cryptography uses different keys to encrypt and decrypt information. In this methodology, each of the participants of the communication has two keys; one is public key which is shared with all the participants, and the other is private key which is secret and only the intended receiver knows it. Though the public and private keys are apparently different, these are mathematically related. Each of the public key has a corresponding private key. This technique can provide integrity, authentication, and non-repudiation. A few standard Asymmetric Key Algorithms are ElGamal, ECC, RSA, DSA, Diffie-Hellman.

1.2.2.3 Hash functions

Hash functions are termed one-way encryption other than the message digests. To ensure it inconceivable for the details or length of the plaintext to recapture hash values computed on the basis of plaintext rather than fixed length. To encode passwords a lot of OS frequently employ hash function. In addition, it gives a mechanism to confirm software integrity checking it used to defend the file from not been adjusted by virus or hacker. To give a digital fingerprint of a file's contents hash methods are frequently adopt.

SHA-1, SHA-2, SHA-3, MD4 and MD5 are some of the regular Hash key algorithms.

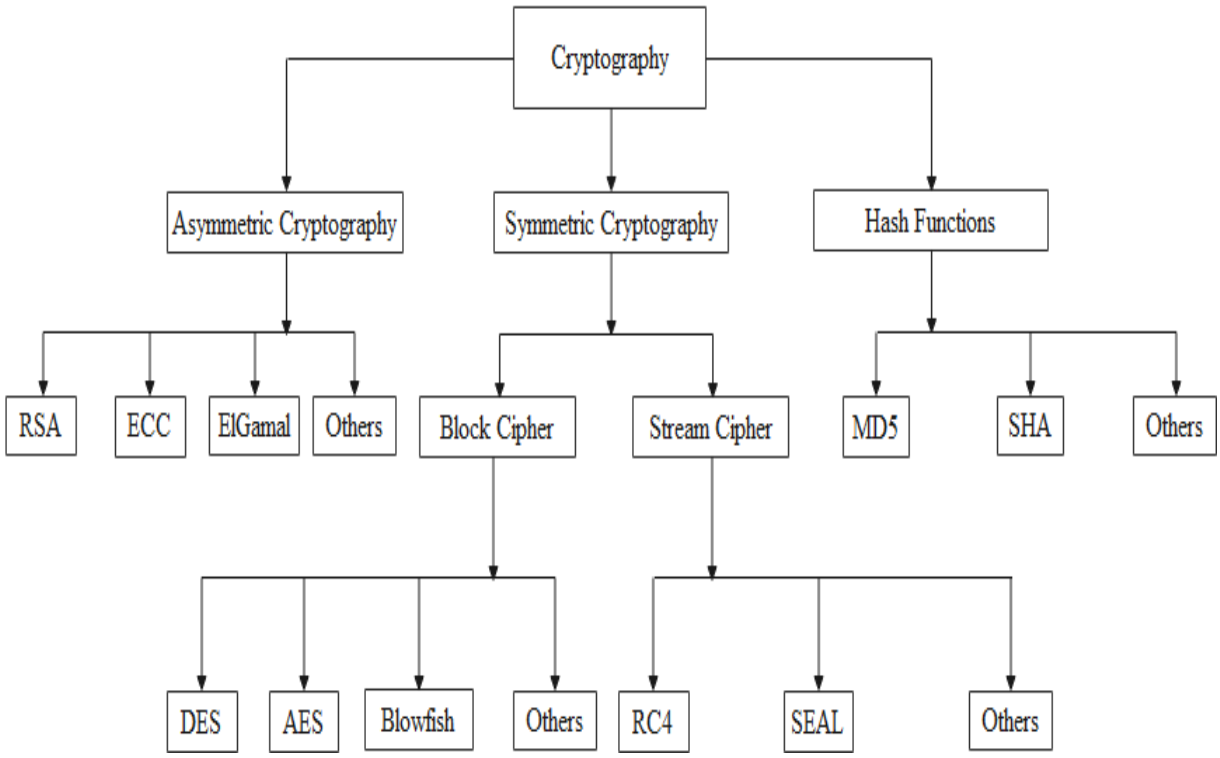

Fig 3: Types of Cryptography and Various Cryptographic Algorithms

2. LITERATURE REVIEW

1) Jain and Agrawal have proposed a hybrid cryptography algorithm using a combination of two symmetric cryptographic techniques, Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA) to strengthen the encryption algorithm. Authors are mainly concerned about the security of sensitive data transfer over different networks for example Military data and Banking transactions etc.

2) Sunita Rani and Ambrish Gangal "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints" proposed a hybrid algorithm for securing the user data initially the message will be encrypted with the Ceaser cipher and the result will be encrypted with the RSA algorithm and result will be again encrypted with mono alphabetic substation method.

3) Ali defined a hybrid encryption algorithm using Advanced Encryption Standard (AES) and Blowfish encryption algorithm for specific application like in bank, military, big websites those handle big data base, and in network companies etc. Author also examined different encryption algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Blowfish Encryption algorithm and Rivest Shamir Adleman (RSA) Encryption algorithm with the help of Statistical Tests.

4) Jasleen Kaur and Dr. Sushil Garg, "Security in Cloud Computing using Hybrid of Algorithms" in the proposed work blending with Digital Signature with RSA algorithm and Blowfish algorithm. Initially a hash is framed to create message digest, for sign the document RSA private key algorithm was used for encryption and for verifying the document Blowfish algorithm was used.

5) Najar and Dar, have proposed efficient, tough and secure hybrid encryption algorithm design with the help of Symmetric key algorithm like Advanced Encryption Standard (AES) and Asymmetric key algorithm like Rivest Shamir Adleman (RSA) algorithm which is responsible for management of key, and Secure Hash Algorithm-1 (SHA-1) used for digital signature.

3. SYSTEM MODEL

3.1 Methodology

This new hybrid cryptography method includes the combination of both symmetric and asymmetric algorithm for more excellent result. Each cryptography method follows the encryption and decryption process. In encryption process the original data is transformed into cipher data, which is not understand by any human or person. To get the original data from cipher data decryption process is used. In this study two time encryption and decryption process is performed because the use of symmetric and asymmetric algorithm.
Before encryption and decryption, RSA, Blowfish and SHA-256 are discussed here.

3.1.1 RSA

RSA is an asymmetric cryptographic technique that uses private key and public key. Messages are encrypted by using the public key of specific receiver and decryption is done by using the private key of receiver. The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

3.1.1.1 Features of RSA:

- Public/private key generation.
- Encrypt with either public or private key.
- Decrypt with matching public or private key.
- Create digital signatures.
- Verify digital signatures.

- Supports key sizes ranging from 512 bits to 4096 bits.
- Supports hash algorithms: MD5, SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), and more.
- Thread safe.

The steps involved in the process are:

1. Choose two distinct large prime numbers, p and q.
2. Calculate n = p*q.
3. Calculate $\phi(n) = (p-1)*(q-1)$.
4. Select an integer *e* such that $1<e<\phi(n)$ and gcd(*e*, $\phi(n)$) =1; that is, *e* and $\phi(n)$ are co-prime.
5. Calculate d such that $e*d = 1 \bmod \phi(n)$.

- n is known as the modulus for public and private keys.
- *e* is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

The pair *(e*, n) forms public key and the pair (d, n) forms private key. To compute cipher text (C) of message (M) uses the following equation

$$C = M^{e} \bmod (n) \quad (1)$$

To decrypt the cipher text (C), use the following equation.

$$P = C^{d} \bmod (n) \quad (2)$$

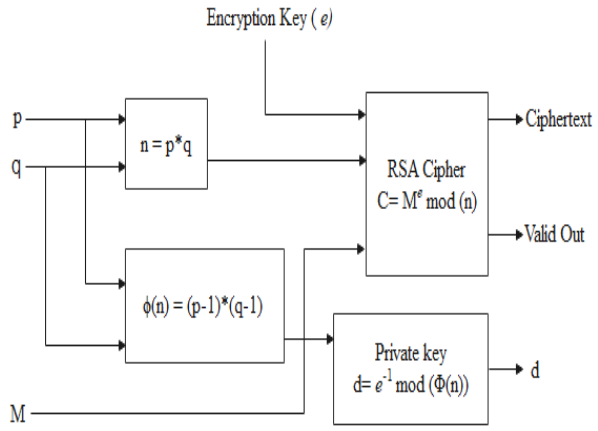

Fig 4: Block diagram of RSA algorithm

3.1.1.2 Advantages of RSA algorithm:

• RSA is stronger than any other symmetric key algorithm.
• RSA has overcome the weakness of symmetric algorithm i.e. authenticity and confidentiality.

3.1.1.3 Disadvantages of RSA algorithm:

1. RSA has too much computation.

3.1.2 Blowfish

Blowfish is a symmetric encryption algorithm, that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. It was designed and developed by Bruce Schneier in 1993.

3.1.2.1 Features of Blowfish:

• Fast: Blowfish encryption state on 32 bit microprocessors.
• Compact: Blowfish can execute in less than 5KB memory
• Simple: Blowfish uses only primitive operations such as addition, XOR and table lookup making its design and manipulation simple
• Secure: Blowfish has a variable key length up to a maximum of 448 long, making it both flexible and secure.

3.1.2.2 Basic operations:

1. **Sub key Generation:**

- Key Size is variable but blowfish algorithm generates very large sub-keys. The key size is in the range of 32 bits to 448 bits or 14 words.
- Concept of P-array consists of 18, 32 bit sub-keys
- There are 4 S-boxes containing 256 entries of 32 bits
- P-array is initialized first then four s boxes with fixed string
- Then P-arrays are XORed with sub keys from P1 to P18. Once the sub keys are generated the encryption process begins.

2. **Data encryption and decryption:**

This process involves the iteration of a simple function 16 times. Each round contains a key-dependent permutation and key and data substitution.

- Blowfish is a very fast algorithm which takes 64 bit input as plaintext and generates 64 bit output cipher text.
- It uses the concept of P-array which uses 32 bit sub keys and there are 18 P-arrays P1 to P18
- Blowfish Algorithm runs 16 times i.e. 16 rounds

A graphical representation of the Blowfish algorithm appears in Figure-5. This structure is known as Fiestal network. Graphical representation of F appears in Figure-6. The function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results are then added and XORed together to produce the output. Because Blowfish is a symmetric algorithm, the same procedure is used for decryption as well as encryption. The only difference is that the input to the encryption is plaintext; for decryption, the input is cipher text.

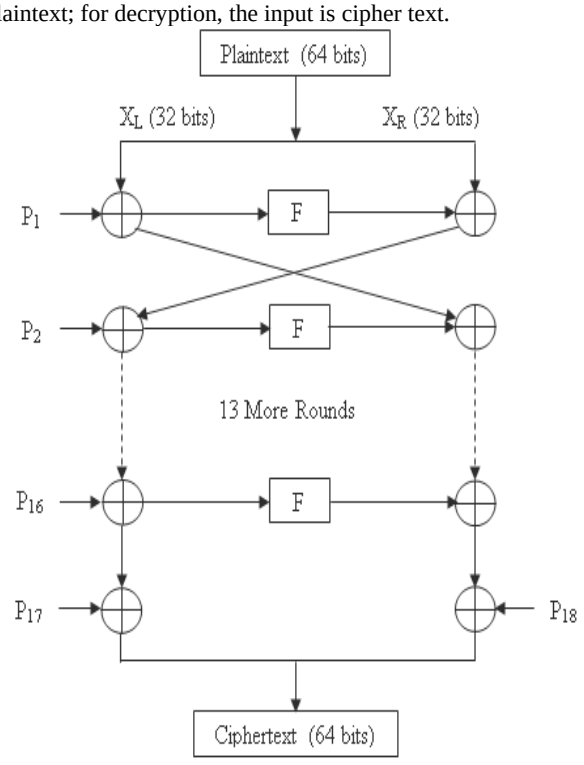

Fig 5: Graphical representation of Blowfish algorithm

P is an array of eighteen 32-bit integers. S is a two-dimensional array of 32-bit integer of dimension 4x256. Both arrays are initialized with constants, which happen to be the hexadecimal digits of π (a pretty decent random number source). The P-array and S-array values used by Blowfish are pre-computed based on the user's key.

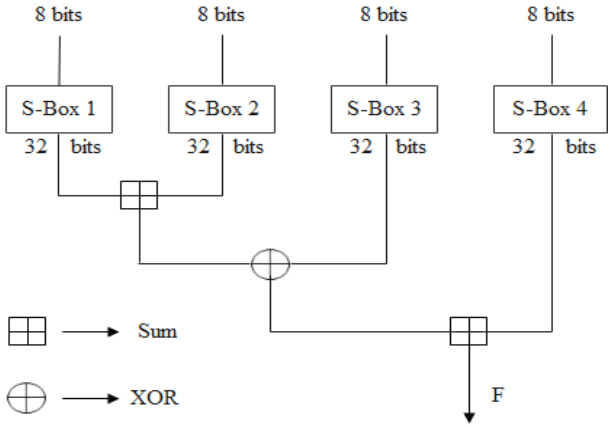

Fig 6: Graphical representation of Function module (F)

In effect, the user's key is transformed into the P-array and S-array. This process is known as sub-key generation. The key itself may be discarded after the transformation. The P-array and S-array need not be recomputed as long as the key doesn't change, but must remain secret.

3.1.2.3 Advantages of Blowfish algorithm:

- Faster than other encryption algorithms, such as the Data Encryption Standard (DES).
- Blowfish is unpatented and free to use. This means anyone can take and use Blowfish for whatever they want to.
- The Blowfish algorithm also has a lesser amount of operations to complete compared to other encryption algorithms.
- The key schedule of Blowfish takes a long time, but this can be advantageous, as brute force attacks are more difficult.

3.1.2.4 Disadvantages of Blowfish algorithm:

- The key schedule of Blowfish takes a long time, equivalent to encrypting 4KBs of data, which can be a disadvantage or an advantage. On the Disadvantage side, it takes a very long time to do.
- The small block size of Blowfish means that Birthday Attacks can occur and compromise the encryption algorithm.
- It is followed by Twofish, which was created to replace Blowfish, as it is better in most ways.

3.1.3 SHA-256

SHA-256 (secure hash algorithm) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function. The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a message digest function with a block size of 512- bit generates 256-bit message digest.
A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.

3.1.3.1 Basic operations:

- Boolean operations AND, XOR and OR, denoted by $\wedge$, $\oplus$ and $\vee$ respectively.
- Bitwise complement, denoted by $\neg$.
- Integer addition modulo 2^{32}, denoted by A + B. Each of them operates on 32-bit words. For the last operation, binary words are interpreted as integers written in base 2.
  - RotR(A, n) denotes the circular right shift of n bits of the binary word A.
- ShR(A, n) denotes the right shift of n bits of the binary word A.
- $A \| B$ denotes the concatenation of the binary words A and B.

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. It has several variants, all of which use the same algorithm but use different constants.

The SHA-2 family of hash functions includes:

- SHA-224
- SHA-384
- SHA-256
- SHA-512
- SHA-512/224
- SHA-512/256

Table 1. Comparison between MD-5 and SHA

S. No	Comparison Parameters	MD-5	SHA
1	Security	Less Secure	High Secure
2	Message Digest Length	128 bits	160 bits
3	Attack required to find out original message	2^{128} bit operation	2^{160} bit operation
4	Attacks to try and find two messages producing the same MD	2^{64} bit operation	2^{80} bit operation
5	Speed	Faster, only 64 iteration	Slower, required 80 iteration

Table 2. Comparison of SHA Functions

S. No	Algorithm and Variant	SHA 0	SHA 1	SHA 2	
1	Output size	160 bits		256/224 bits	512/384 bits
2	Internal state size	160 bits		256 bits	512 bits
3	Block size	512 bits		512 bits	1024 bits
4	Max message size	2^{64} -1 bits		2^{64} -1 bits	2^{128} -1 bits
5	Word size	32 bits		32 bits	64 bits
6	Rounds	80		64	80
7	Operations	AND, OR, XOR, shr, ROT, ADD (2^{32})		AND, OR, XOR, shr, ROT, ADD (2^{32})	AND, OR, XOR, shr, ROT,ADD (2^{64})
8	Security bits	<34 (Collisions found)	<63 (Collisions found)	112 128	112, 128, 192, 256

Table 1 and Table 2, shows why SHA-2 is better than other hash algorithms such as MD-5 and SHA-1.

3.1.3.2 The benefits of SHA-256:

SHA-256 is using here because this 256-bit key is much more secure than other common hashing algorithms. Without going into too much technical detail, here are the key benefits of SHA-256:

- It's a secure and trusted industry standard: SHA-256 is an industry standard that is trusted by leading public-sector agencies and used widely by technology leaders.
- Collisions are incredibly unlikely: There are 2^{256} possible hash values when using SHA-256, which makes it nearly impossible for two different documents to coincidentally have the exact same hash value.
- The avalanche effect: Unlike some older hashing algorithms, even a very minor change to the original information completely changes the hash value—what is known as an avalanche effect.

3.1.4 Digital Signature Algorithm (DSA)

DSA stand for Digital Signature Algorithm. It is one of the Federal Information Processing Standard for making digital signatures, based on mathematical concept of modular exponentiation and discrete logarithm. It is used for digital signature and its verification. It was developed by National Institute of Standards and Technology (NIST) in 1991. It involves four operations:

1. Key Generation
2. Key Distribution
3. Signing
4. Signature Verification

A digital signature is a technique that binds a person or entity to the digital data of the signature. Now, this will binding can be independently verified by the receiver as well as any third party to access that data. It is a cryptographic value that is calculated from the data and a secret key known only by the signer or the person whose signature is that.

Why Blowfish, RSA and SHA-256 have been used in this proposed system?

Blowfish is an incredibly fast cipher that has a relatively simple structure and is very effective. It generates a really large key and this alone is a huge benefit to security. With the increase in speed of computer processing, Blowfish is able to create a much longer key so that it is much more difficult to try to hack the key value. And the way that it generates sub-keys means that each pair of sub-keys changes slightly. This prevents attackers from figuring out how the sub-keys were generated, and then gaining access to all the other known keys. In fact, Blowfish is especially solid against attacks because of the complexity of the sub key generation process. It does take longer for the sub keys to be generated, but for the security-conscious, it is time well spent. For each key, the encryption routine runs 522 times. Blowfish has gone through a great deal of analysis and testing to prove its merit. In fact, since it is license-free and available free for all uses, its creator encourages hacking attempts. The results of attempted hacking are posted for others to review and comment upon; the encryption method can then be tweaked as needed to ensure its continued success against the bad guys. The Blowfish algorithm is still relevant and firmly holds its position as the fastest. In terms of decryption of data, the blowfish algorithm lacks some speed. Apart from this minor issue, it is the best, and every network administrator and software developer must know how to implement it with their work and code.

The RSA algorithm is the basis of a cryptosystem, a suite of cryptographic algorithms that are used for specific security services or purposes which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. It is extremely elegant, simple, and well-tested. Current commonly used RSA key lengths include 1024 and 2048 bits.

The main reason technology leaders use SHA-256 is that it doesn't have any known vulnerabilities that make it insecure and it has not been "broken" unlike some other popular hashing algorithms.

3.1.5 Encryption:

Encryption process converts the original data into cipher data with the help of Blowfish algorithm. Blowfish algorithm is a symmetric key cryptography method, which uses secret key to encrypt the original data and send this key with encrypted data to the receiver. The risk involved in symmetric cryptography is the shifting of secret key over the internet. To overcome the risk of symmetric cryptography, RSA algorithm is used which is an asymmetric key cryptography method.

Blowfish algorithm is responsible for encryption of data, which is selected by the user. Blowfish is a symmetric cryptographic algorithm which uses single key to encrypt and decrypt the original data. This single key is known as secret key. Secret key is transmitted with encrypted data over the internet and hence need to encrypt the secret key. This secret key is encrypted using RSA algorithm, which is an asymmetric cryptographic algorithm. RSA algorithm uses different key for encryption and decryption.

Signature generation phase provides the message authentication with the help of Digital signature using SHA-256. For secure transmission and authorization, digital signature is used. Digital

signature assures that the data is authorized by authenticated person; it is not modified by any third person during data transmission. Private Key is used for digital signature on message digest. Message digest is produced by applying Secure Hash Algorithm-256 (SHA-256) on encrypted user data.

3.1.6 Decryption:

In decryption process cipher data is converted into original data. In this cryptography method first phase is hybrid decryption phase and second phase is signature verification phase. Hybrid decryption phase is a reverse process of hybrid encryption phase. This phase is responsible for decryption of encrypted message with the help of RSA and Blowfish. First step, RSA decryption algorithm decrypts the encrypted key, which helps to get original data. Second step, with the help of decrypted key blowfish decryption algorithm decrypt the encrypted data.
In signature verification phase, message digest is generated using SHA-256 to verify the signature.

3.2 Proposed hybrid cryptography algorithm

The proposed hybrid cryptography algorithm consists of two processes one for encryption and the second for decryption, and it will be presented as following:

3.2.1 Encryption process:

Basic function of this process is to encrypt the user data to protect data from unauthorized access or hackers in cloud at the time of data transmission also. After encryption data will convert into cipher text.

(i) Select a secret key K between the ranges of 32 bits to 512 bits of variable length.

(ii) Encrypt (C) the selected file f, by applying Blowfish algorithm (B) with the help of secret key. Blowfish algorithm is a symmetric key cryptographic algorithm, which uses single key to convert the original data into cipher data and vice versa. This key is known as secret key or private key. It has a 64 bit block size and the length of key is from 32 bits to 448 bits.

$$C_f = CB_K(f)$$

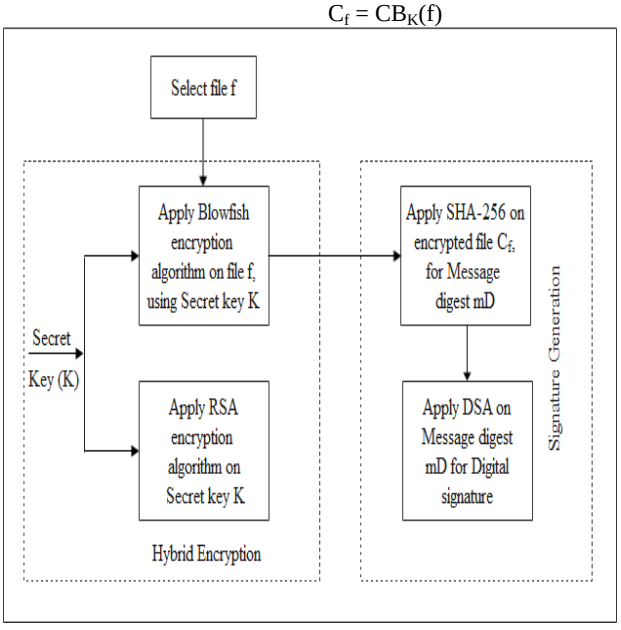

Fig 7: Encryption Process

(iii) Encrypt the secret key K, using RSA algorithm (R). RSA algorithm is an Asymmetric key cryptographic algorithm, which uses pair of key for encryption and decryption.

$$C_K = CR(K)$$

(iv) Apply SHA-256 (S) on encrypted file C_f to generate message digest (mD) or hash code. SHA stands for Secure Hash Algorithm, which is used to generate the message digest.

$$mD = S(C_f)$$

(v) Apply digital signature algorithm (d) on message digest to generate digital signature (D_s).

$$D_s = d(mD)$$

3.2.2 Decryption process:

Decryption process converts the cipher text into original data, so that user can read or access this data. Only authorized user can decrypt the cipher text or in other word only authorized user can access the data.

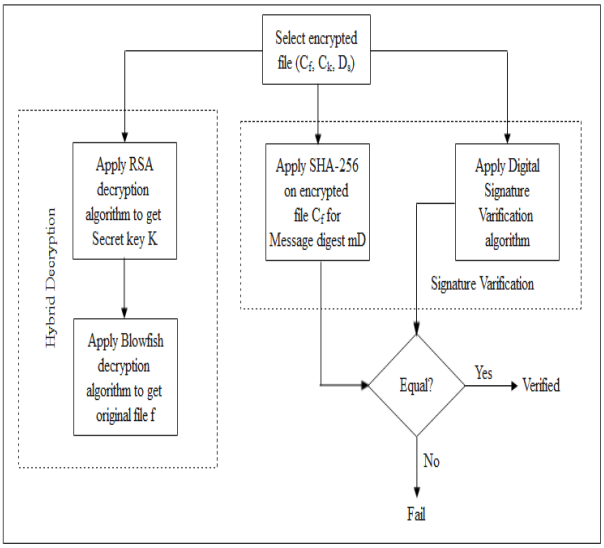

Fig 8: Decryption Process

(i) To get the secret key K, decrypt the encrypted secret key C_K by applying RSA decryption algorithm (PR).

$$K = PR(C_K)$$

(ii) Using above secret key, obtain the original file f, by applying blowfish decryption algorithm (PB) on encrypted file C_f.

$$f = PB_K(C_f)$$

(iii) Apply verification algorithm (V) of digital signature on digital signature (Ds) to get the expected message digest (mD) or hash code.

$$mD = V(Ds)$$

(iv) Compare this message digest or hash codes with the SHA-256 (S) generated message digest or hash code.

$$mD = S(C_f)$$

4. COMPARISON WITH THE EXISTING METHODS

Table 3. Comparison between existing and proposed cryptography algorithms.

Authors	Algorithm	Key size	Block size	Rounds	Security
Ali E.Taki El Deen	AES, DES	128 bits, 56 bits,	128 bits	10,12,14	Medium Security
Jain and Agrawal	DES, IDEA	56 bits, 128 bits	64 bits	16	Medium Security
Najar and Dar	AES, RSA, SHA-1	128 bits, 1024 bits and 160 bits	128 bits	10,12,14	Medium Security
Sunita Rani and Ambrish Gangal	Ceaser cipher, RSA	-	-	-	Highly Secure
Jasleen Kaur and Dr. Sushil Garg	RSA, Blowfish	1024 bits, 32–448 bits	64 bits	16	Medium Security
Proposed hybrid Cryptography algorithm	Blowfish, RSA and SHA-256	32–448 bits, 4096 bits and 256 bits	64 bits, 470 bits, 512 bits	64	Highly Secure

4.1 Advantages of proposed hybrid cryptography algorithm:

- Combination of symmetric cryptography (Blowfish), asymmetric cryptography (RSA), and hash function (SHA-256), this proposed method provides a very high level of security, performance and better key management.
- The proposed method will protect the user data, from unauthorized access at the time of transmission.
- Proposed system increased the difficulty level for unauthorized person or hacker to decrypt the encrypted data, through encrypted key, via RSA.
- Makes use of digital signatures for message authentication.

5. CONCLUSION AND FUTURE WORK

The hybrid cryptography algorithm is proposed using Blowfish, RSA, and SHA-256 algorithms. The combination of symmetric and asymmetric algorithm provides efficiency to proposed system. This hybrid algorithm is secure and authentication enabled process which provides high security for cloud computing by using SHA-256 algorithm.
As a future work, this hybrid algorithm can be constructed from different existence algorithms to improve the encryption and decryption process and compare it with this current work.

6. REFERENCES

[1] Mahavir Jain, and Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[2] Sunita Rani and Ambrish Gangal, "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012.

[3] Ali E.Taki El_Deen, "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, pp. 669-673, December- 2013.

[4] Jasleen Kaur and Dr. Sushil Garg, "Security in Cloud Computing using Hybrid of Algorithms" International Journal of Engineering Research and General Science Volume 3, Issue 5, September October, 2015.

[5] Jan Mohammad Najar, and Shahid Bashir Dar, "A New Design of a Hybrid Encryption Algorithm", International Journal of Engineering and Computer Science, Volume 3, Issue 11, pp. 9169-9171, November 2014.

[6] Self-study: Cryptography and its Types, retrieve from: https://www.geeksforgeeks.org/cryptography-and-its-types/, retrieve date: 5 July 2020.

[7] Self-study: Cloud computing, retrieve from: https://en.wikipedia.org/wiki/Cloud_computing, retrieve date: 1October 2020.

[8] Self-study: RSA (Rivest Shamir Adleman) algorithm, retrieve from: https://www.educative.io/edpresso/what-is-the-rsa-algorithm, retrieve date: 10 February 2021.

[9] Self-study: Encrypting data with the Blowfish algorithm, retrieve from: https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm , retrieve date: 13 March 2021.

[10] Self-study: Secure Hash Algorithm 2 (SHA-2), retrieve from: https://en.wikipedia.org/wiki/SHA-2, retrieve date: 18 April 2021.