World Wide Journal of Multidisciplinary Research and Development

World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 188-195
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

P. Selvarani
Research Scholar, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

N. Malarvizhi
Associate Professor, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

Correspondence:
P. Selvarani
Research Scholar,, Computer Science and Engineering
Vel Tech Dr. RR & Dr.SR Technical University, Avadi, Chennai, India

Analysis on Data Security Issues and Cryptographic Algorithms in Cloud Computing

P. Selvarani, N. Malarvizhi

Abstract
Cloud computing is an emerging technology which reduces storage burden for a data owner. When the data owner needs to access the data which is provided by the cloud vendor there is a chance for the intruders to change/modify the data. This is because data owners do not have direct control on data. So the data security is the big challenge in cloud computing. It is necessary to increase the data security level, and need to protect the data against unauthorized users in cloud computing. To achieve higher data storage security in cloud computing traditional authentication techniques can be used. There exists many security algorithm which is used to implement in the cloud computing. Symmetric, Asymmetric and hashing. Symmetric algorithm consist DES,AES, Triple DES, and Blowfish. Asymmetric algorithm consist RSA,D-H, IKE,DSA etc. This paper ensures various data security issues allied to cloud computing and reviews on cryptographic algorithms used for data security purpose. While comparing above algorithms blowfish is efficient. Because blowfish is a strongest encryption algorithm, very fast and highly secured. Along with this Multimodal bio cryptography techniques can be used to increase the security level. The combination of biocryptographic technique forms the key for Blowfish algorithm. Thus by using this technique one can secure the data from unauthorized users.

Keywords: Cloud Computing, Data Security, Cryptographic algorithm, Encryption/Decryption Blowfish.

Introduction

Cloud computing is an internet based computing that relies on sharing computing resources rather than having local server or personal devices to handle applications. One of the primary usage of cloud computing is data storage. Using cloud storage, users can remotely store and retrieve their data from anywhere anytime anyplace and any devices. Cloud has three types of services. They are Software as a service, Platform as a service and Infrastructure as a service. Cloud services are provided by the different cloud providers like Amazon, Google, Microsoft, IBM and etc. The users can utilize these services (IaaS, PaaS and SaaS) based on their requirement. Usage of these three services, user's data's are stored on the cloud. So the Cloud providers are maintaining the user's data in cloud environment like security of the data in the cloud, access control and authentication in the cloud. Data security becomes more and more important in cloud computing. When users put their data on the cloud the data integrity protection is challenging.

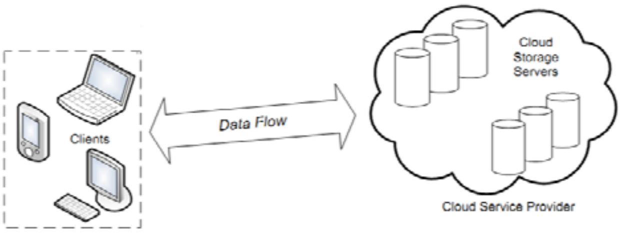

Fig. 1: Cloud Data Storage Architecture

The cloud data storage architecture used in this work is based on the model proposed by Cong Wang et al. [1], as shown in Fig-1. The different entities are the Client and Cloud Storage Server.

Client: The user store large amount of data in the cloud and relies on the service provider for maintenance. This can either be an individual user on a large organization.
Cloud storage server: An entity which is managed by a cloud service provider, has significant storage space and computation resources to maintain client's data.

Data Security Issues In Cloud

The security requirements in service oriented cloud computing model are as follows:

Data security

The provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. [3]

Data Privacy

The providers should ensure that all critical data are masked and that only authorized users have access to data in its entity. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Data confidentiality

The cloud users want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. [2]

Fine-grained access control

The provider should facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. [4]
The effective implementation for the above mentioned security issues would be encrypting data by using certain encryption techniques, which allows flexibility in specifying differential access rights of individual users in a feasible way.

Top Security Threats in the Cloud Computing

The cloud industry is addressing severe security concerns. These issues are happening again and again. The cloud server has to be sure that the customer does not go through any problem such as data theft or data loss. There is also a chance where an intruder can hack the cloud. Cloud computing faces many security issues according to cloud alliance surveys. Some of the major security issues which are faced by the Cloud computing are:

- Data Loss
- Data Breaches
- Account Hijacking
- Shared technologies vulnerabilities
- Affected software
- Security on Cloud Vendor side
- Security on data owner side
- Malicious insiders

Data Loss

Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. Accidental deletion happens more often than a lot of people may think.

Data Breaches

A data breach in which sensitive is an incident, confidential or protected or data has potentially been gone through, stolen or utilized by individual hackers to do so. We can also define this as the disclosure of the document unintentionally.

Account Hijacking

If someone uses stolen credentials to hijack cloud computing services, they can eavesdrop on others' transactions, manipulate data, redirect users to illegitimate sites, and even compromise the availability of cloud services, often resulting in litigation for cloud service providers.

Shared technology vulnerabilities

Because shared technology elements weren't designed for strong compartmentalization in a cloud environment, hackers have increased their attacks in these areas in an effort to interrupt the operations of other cloud customers and gain unauthorized access to data.

Affected software

Cloud Provider should have the full permission to access the server for monitoring and maintenance. By doing this the third party user who is not having permission to access the file can be restricted. Thus the client files can be prevented from any infected application.

Security on Cloud Provider level:

Cloud owner should be making sure that the server is well protected from all the malicious threats it may come across. A Cloud is good only when there is a good security provided by the cloud provider to the customers

Security on data owner level:

Even though the cloud provider has provided a good security layer for the data owner, the data owner should make sure that because of its own action, there shouldn't be any data loss or breaching of data who are using the same Cloud.

Malicious insiders

If a third party without your knowledge should gain access to your server, considerable damage can be done. Such intruders can steal the details of client organizations and assets, damage valuable brands, steal confidential information, or even take complete control of the cloud, with little or no risk of detection.

Data Life Cycle –Cloud Security & Privacy

Figure 2 shows Data life cycle which consists Personal information should be managed as part of the data used by the organization.
Protection of personal information should consider the impact of the cloud on each phase.

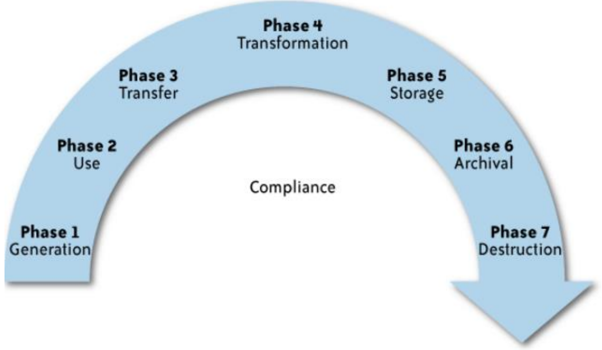

Fig. 2: Data Life Cycle.

Data Storage In Cloud Offers So Many Benefits To Users:

Cloud Data provides unlimited data storage space for storing user's data. Users can access the data from the cloud provider via internet anywhere in the world not on a single machine. We do not buy any storage device for storing our data and have no responsibility for local machines to maintain data.

Within the cloud computing world, the virtual environment lets users' access computing power that exceeds that contained within their own physical worlds. To enter this virtual environment, it does not require the exact location of their data nor the other sources of the data collectively stored with theirs. To ensure data confidentiality, integrity and availability (CIA), the storage provider must offer capabilities that, at a minimum, include: a tested encryption schema to ensure that the shared storage environment safeguards all data; harsh access controls to prevent unauthorized access to the data; and Scheduled data backup and safe storage of the backup media.

Related Work

The authors Shashi Mehrotra Seth et al, [5] proposed a contemporary review of comparative analysis of encryption algorithms like AES, DES and RSA for data communication by using encryption time; memory usages output byte and battery power. Based on text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while the difference in encryption time is very minor in case of AES and DES algorithms. RSA consumes longest encryption time, high memory usage and less output byte.

The authors Pratap Chandra Mandal et al, [6] studied the evaluation of performance of selected symmetric key algorithms. From the simulation they concluded that Blowfish cryptographic algorithm has better performance than other algorithms. Secondly AES gives better performance than DES and 3DES in terms of throughput and decryption time.

The authors Gurjeevan Singh et al, [7] studied throughput analysis of various selected encryption algorithms like DES, AES, 3DES and Blowfish. The simulation results shows the numerous points like Blowfish has better performance than other algorithms followed by AES in terms of throughput and 3DES has least performance than others.

The authors Chhaya Nayak et al, [8] studied the performance of selected symmetric encryption algorithms used in cryptography. Security of information in transit is a very important task in secured communication. Many ciphers are available which have been developed by using arithmetic and logical operations. The two important desirable properties of the cryptosystems are its speed and security. The security of the algorithm is based on the key size. The increase in the key size reduces the speed of the algorithm. But in turn increases the security. Thus the aim of the designer is to design efficient cryptosystems with acceptable speed and appreciable security strength with large key length. Implementation procedures also play a major role in cryptosystems design.

[9] High level of security is reciprocally proportional to system performance and maintenance cost. Hence, if all data storages have to be provided with the highest level of security, it would degrade the performance of the system. So here we have proposed a framework to provide appropriate level of security to different data according to their class of sensitivity with respect to confidentiality, integrity and authenticity.

Problem Statement

Cloud data can be attacked in two ways. Insider attack and outsider attack. Insider as an administrator can have the possibility to hack the user's data. Insider attack is very difficult to be identified. So the users should be very careful while storing their data in cloud storage. Even though the data is accessed by the third party, they shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage. Cryptography is a technique applied for encryption and decryption. Usually unimodal biometric techniques are used. The existing unimodal bio cryptography techniques often have limitations such as consciousness to noise, intra class consistency, data aspect, and other factors. So there is a need to merge two or more biometric techniques for the higher security of the cloud data.

Cryptographic Technique

The following fig 2 shows the frame work of the cryptographic technique. The message is converted in to cipher text along with the encryption key. Again the cipher text is converted to original message only using decryption key. There are 3 types of algorithm namely symmetric key encryption algorithm, Asymmetric key encryption algorithm and Hashing.

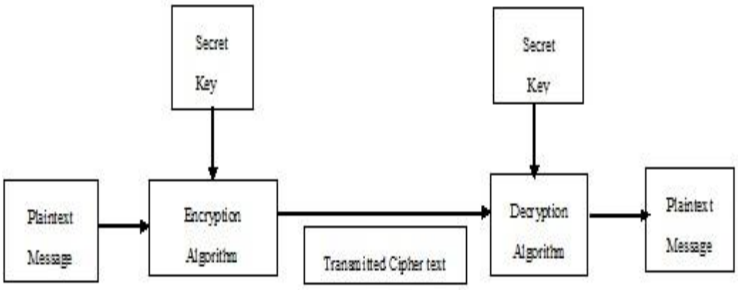

Fig. 3: Cryptographic Technique

Symmetric Key Algorithm

Symmetric key algorithm use same key for both Algorithm is divided into two types. Block cipher and stream cipher. In block cipher input is taken as a block of plain text of fixed size. In Stream cipher one bit at a time is encrypted. Some of the popular symmetric-key algorithms used in cloud computing are: Data Encryption Standard, Triple Data Encryption standard and Advanced Encryption Standard and Blowfish algorithm.

Data Encryption Standard Algorithm

The following Figure 3 shows Data Encryption Standard. It is designed by IBM in 1976. DES is a symmetric encryption algorithm by using 56 bit key size. DES uses 64 bit block. It uses balanced Feistel structure... Feistel function for this are – expansion, substitution, key mixing and permutation and for the encryption process of DES there are two permutations, one is initial and the other is final permutation and 16 Feistel rounds are used to generate the key, for each round 48-bit key is generated from the cipher key [10].

```
function DES_Encrypt (M, K) where M = (L, R)
M ← IP(M)
For round← to 16 do
Ki ← SK (K, round)
L← L xor F(R, Ki)
swap(L, R)
end
swap(L, R)
M ← IP-1(M)
return M
End (Algorithm 1: Data Encryption Standard)
```

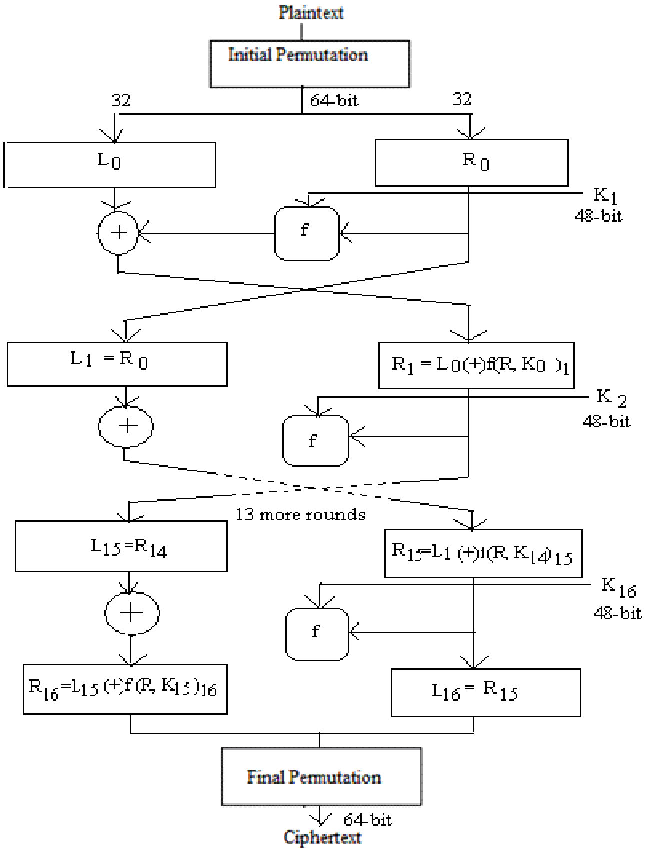

Fig. 4: Data Encryption Standard

AES Algorithm

The following figure 4 shows Advanced Encryption Standard. It is Designed in the year 1999 by NIST AES is a symmetric key block cipher, AES are so simple that can be easily implemented using cheap processors and a minimum amount of memory. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits.[11,12].

```
Cipher(byte[] input, byte[] output)
 {
byte[4,4] State;
copy input[] into State[] AddRoundKey
for (round = 1; round < Nr-1; ++round)
{
SubBytes ShiftRows MixColumns AddRoundKey
}
SubBytes ShiftRows AddRoundKey
copy State[] to output[]
}
```

Algorithm 2: Advanced Data Encryption Standard

DES vs. AES

Table 1: DES vs. AES

Design Feature	DES	AES
Year	1976	1999
Block Size	64	128
Key Length	56	128,192,256
No Of Rounds	16	9,11,13
Encryption Primitives	Substitution, Permutation	Substitution, Shift, binary
Cryptographic Primitives	Confussion,Diffussion	Confussion,Diffussion
Design Rationale	Open	Open
Selection Process	Secret	Secret, but accept open public comment
Source	IBM Enhanced by NSA	Independent Cryptography (ECB,CBC,CFB,OFB)

Triple Data Encryption Standard

The following figure 5 shows Triple Data Encryption Standard. It is Developed in 1998 this is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES.It requires always more time than DES because of its triple phase encryption characteristics. [12] Triple DES with three keys is used by many applications such as PGP, RC5, IDEA, two-fish, CAST, etc.It provides an easy and efficient way of increasing the key size of DES to protect against brute force attack [13]

```
For j = 1 to 3
{
Cj,0 = IVj
For i = 1 to nj
{
Cj,i = EKEY3 (DKEY2 (EKEY1 (Pj,i Cj,i-1)))
Output Cj,i
}
} Algorithm 3: Triple DES
```

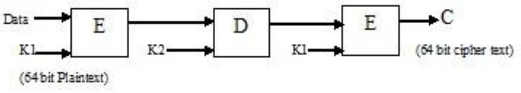

Fig. 5: Triple DES

RC-5 Algorithm

RC-5 (Ron-Rivest) RC-5 Algorithm was developed in 1994. A block-cipher supporting a variety of block sizes (32, 64, or 128 bits), key sizes, and number of encryption passes over the data. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow. [11]

```
A = A + S[0];
B = B + S[1];
for i = 1 to r do
A = ((A Xor B) <<< B) + S[ 2 * i ]
B = ((B Xor A) <<< A) + S[ 2 * i + 1]
```

Algorithm 4: RC-5

IDEA

International Data Encryption Standard Algorithm was developed in Switzerland 1991. It consists 8 rounds. This block cipher uses 64 bits block of message and 1 bit key. IDEA is quite difference than DES. It is used in Pretty Good Privacy(PGP). This encryption algorithm suffer from narrow bicliques attack.[14,15].

Asymmetric Key Algorithm

Asymmetric –key algorithm use different keys for both encryption and decryption. The two keys are Private Key and public key. The public key is used by the sender for encryption and the private key is used by the receiver for decryption. The most asymmetric key algorithm for cloud is: RSA, IKE, and Diffie-Helman Key Exchange

RSA Algorithm

RSA developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a public key cryptographic algorithm for data security. This is a most common encryption algorithm used by people to encrypt message with two keys. RSA algorithm encryption and decryption is based on the modular exponential and has two exponents, a and b, where a is used for public and b is used for private. Let the plaintext is M and C is cipher text, then at [14,15].

encryption $C = M^a$ mod n
decryption $M = C^b$ mod n.

Key Generation

Select 2 prime number p and q
Calculate n-pxq
Calculate ø (n)=(p-1)x(q-1)
Select integer a; gcd (ø(n),a)=1;1<a< ø(n)
Calculate b
Public Key: KU={a,n}
Private Key: KR ={b,n}

Encryption
Plain text: M<n
Cipher text: $C=M^e$ (mod n)
Decryption
Cipher text: C

Plaintext: $M=C^{d}(\text{mod } n)$

Algorithm 6: RSA Algorithm

Diffie-Helman Key Exchange-
D-H is created by the Whitfield Diffie and Martin Hellman In 1976.This algorithm depends on the complexity of discrete logarithm. Diffi-hellman basically used for key exchange between two users The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. [14,15]

D-H ALGORITHM

Q is a prime number and a is a root of q i.e a<q
Private Key Xa, public key $Ya=a^{XA}$ mod q,Xa<q
Private Key Xb, public key $Yb=a^{XB}$ mod q,Xb<q
Secret key by user A:
$K=(Yb)^{Xa}$ mod q
Secret key by user B:
$K=(Ya)^{Xb}$ mod q

Algorithm 7: Diffie-Helman Key Exchange

DSA: DSA was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [12]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [16].

ElGamal- This is an asymmetric algorithm used for transmitting digital signatures as well as for key exchange. El Gamal is based on the applicability of discrete logarithms. It is rely on the logarithmic number's characteristics or calculations of these numbers. [14]

ECC
Elliptic Curve Cryptography (ECC) was proposed by Koblitz [17] and Miller [18] in 1980s. ECC is a public key cryptographic scheme. It uses properties of Elliptic Curves to develop cryptographic algorithms. Security of ECC is based on the intractability of ECDLP i.e. Elliptic Curve Discrete Logarithm Problem. Elliptic Curves (EC) over finite fields are used to implement public-key protocols.

Proposed Work
In our proposed work we mainly focus on data security on cloud. To provide data security we use bio cryptographic technique such as fingerprint, iris and secret key. Because bio-cryptographic framework, as a safer authentication mechanism for Cloud storage sharing. Blowfish algorithm for Encryption and Decryption can be implemented to enhance security framework over the network. Blow fish algorithm is the better result algorithm which is used to secure the cloud data. This is decided after going through many other algorithms related this.

Data encryption and decryption in cloud using multimodal biometrics
Biometric Sample: Fingerprint and iris image can be processed and discarded at the end of the process.

Digitized Biometric Template: Derived from the biometric sample (Finger print and iris). It can be converted into 0's and 1's. (Biometric digitized). And can be store in the data base.

Secret key: Pin/Password (or) Cryptographic key-Discarded at the end of the process

Matching: The biometric sample (fingerprint & iris) and Cryptographic key which is derived from the same person (or) not should be identified.

Biocryptrographic binding: This is done using biocryptographic algorithm such as blowfish

Cryptographic Technique used in cloud data security
Encryption: Initially we apply preprocessing for feature extraction from each biometric image. Then the fusion of feature level both fingerprint and iris are used for encryption key for blow fish algorithm. The output of the blow fish algorithm is cipher text which is stored in the cloud environment. The intruders cannot able to read the cipher text in the cloud environment.

Decryption: The data from cloud is accessed by corresponding user by a secret key which is framed by the combined bio-metric of Finger print an Iris for decryption. The user will get the original message after decryption. The data can be protected from unauthorized users

Biocryptogram: This is also called private biometric template. Use only information stored in the system.

Blowfish Encryption Algorithm
Blowfish algorithm is designed in 1993 by Bruce Shnier and it is included in a large number of cipher suites and encryption products. It take variable length key from 1-448 bits. It has 16 rounds. Each round consists data dependent permutation and data dependent substitution. Blowfish algorithm handles 2 parts of the data. Expansion of the key and Encryption of the data.

The expansion of key: Split the original key into set of sub keys. Specifically a key is no more than 448 bits is separated into 4168 bytes. The P-array contains 18-32 bit S-boxes. The P-array contains 18-32 bit sub keys while each S-box contains 256 entries. S-box accept 8 bit input and produce 32 bit output.

Encryption of data: 64 bit input is denoted with an x, While the P-array is denoted with Pi (Where i is the iteration. [15]
Divide x into two 32-bit halves: x**L**, x**R**
For i = 1to 16:
X**L**= X**L** XOR P**i**
x**R** = F(X**L**) XOR x**R**
Swap X**L** and x**R**

Next i
Swap **XL** and x**R** (Undo the last swap.)
x**R** = x**R** XOR P**17**
x**L** = x**L** XOR P**18**
Recombine x**L** and X**r**
Algorithm 5: Blowfish Encryption Algorithm.

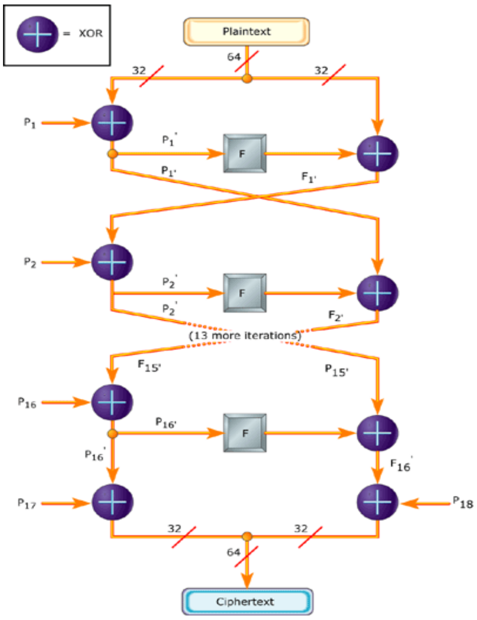

Fig. 6: Blowfish Encryption Algorithm

Comparison of Symmetric Key Encryption Algorithm

The following Table 2 shows comparison of Symmetric (Same key) Key Encryption algorithm. (DES, AES, Triple DES, IDEA and Blowfish Algorithm).)

Table 2: Comparison of Symmetric Key Encryption

Algorithm	**Year**	**Block Size**	**Key Size**	**No Of Rounds**	**Network**	**Attack**	**Possible Keys**	**Speed**	**Security Strength**
DES	1976	64	48,56	16	Feistel	Brute Force Differential, Linear Cryptanalysis	2^{128}	Very slow	High level security Security must not depend on secrecy of algorithm.
IDEA	1991	64	128	8,5	Lai-Massey scheme	Narrow bi-Lique	2^{128}	Fast	Secure
3DES	1993	64	168,112,56	16	Feistel	Brute Force	2^{168},2^{112},2^{56}	Slow	Security of DES mainly relies on non-linearity
Blow Fish	1993	64	32-448	16	Feistel	No of attack is known but suffering from week key	2^{32},2^{448}	Very Fast	Very fast, Highly Secure. Significantly faster than DES
RC-5	1994	32,64,128	0-2040	1-255	Feistel	Differential	2^{128}	Slow	Indeed in high security applications
AES	1999	128	128,192,256	10,12,14	Non-Feistel	Brute-Force	2^{128},2^{192},2^{256}	Very fast	Security strength equal or better than 3DES

Comparison of Asymmetric Key Encryption

Table 3

Algorithm	**Security**	**Std**	**Usage**	**Keys**	**Key Length**	**Attack**	**Encr/Decr**	**Dig.sig**	**Key Exg**
RSA	Based on the problem of factoring large Numbers	Free for all, Patented only in US	Used for confidentiality and key exchange as well as for digital sign	2	512 to 15,360	Brute forced and oracle attack etc	Yes	Yes	Yes
D-H	Vulnerable and secure	ANSI X9.42	Used for Key	2	2013,224 bits for q	Denial of service	No	No	Yes

	against eavesdropping		exchange		and 2048 bits for p	attack			
ECC	Based on difficulty to determine secret key k given kP and p	IEEE P1363	Implementing algorithm such as DSA	2	112 bit to 512 bit	Timing or simple and differential power attack.	Yes	Yes	Yes
EI-Gamel	Based on the Discrete logarithm (DLP)	FIPS-186-3	Used for both Encryption and RSA	2	2048	Chosen cipher text & malleability	Yes	No	Yes
DSA	secured	NIST/FIPS(1,2,3,4)	Use as same/Predictable values	1	Multiples of 64 b/w 512-1024	Private key	No	Yes	No

Table 3 shows Comparison of Asymmetric key encryption (Different key-Private & public) Some of the asymmetric key algorithm used in cloud computing are RSA, DSA, DH, ECC, EI-Gamel. Some algorithms are suitable for all users. for encryption & decryption provide secrecy, Digital signatures provide authentication, and key exchange provides of session key.

Conclusion

Data Security is a major concern of cloud computing.. There are many cryptographic algorithms that can be used over the cloud. To provide the data security by using bio cryptographic technique (like fingerprint iris and secret key) for higher accuracy and more security. Thus the combination of Finger print and Iris form the key for Blowfish algorithm to store the secured data from unauthorized users in cloud environment and further reduce the time for data encryption and decryption.

Future Enhancement

As discussed above there are many security algorithms which are currently used in a cloud computing environment. Thus by implementing blowfish algorithm in cloud environment cloud data can be secured. In future these comparisons of the existing algorithms are used in implementation process for the higher accuracy of the data security.

Result: To achieve high data security we can use combined biometrics with cryptographic technique using blowfish algorithm. To protect and secured the high security data from unauthorized users in cloud environment.

References

1. Cong Wang, Qian Wang,. Kui Ren, Wenjing Lou,: Ensuring data storage security in Cloud Computing, Quality of Service, 2009. IWQoS. 17th International Workshop on, vol. 186, pp.1-9, (2009).
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009
3. L.J. Zhang and Qun Zhou, —CCOA: Cloud Computing Open Architecture,‖ ICWS 2009: IEEE International.
4. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures‖ IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011
5. Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST Vol.2, Issue 2, June 2011.
6. Pratap Chandra Mandal, "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish", Journal of Global Research in Computer Science, Vol.3, No.8, August 2012.
7. Gurjeevan Singh, Ashwani Kumar Singla, K. S. Sandha, "Throughput Analysis of Various Encryption Algorithms", IJCST, Vol.2, Issue 3, September 2011.
8. Chhaya Nayak, "Performance of Various Algorithms Used in Cryptography", IJMIE, Vol.2.,Issue 7
9. The Consultative Committee for Space Data Systems, Encryption Algorithm Trade survey, Information report, CCSDS 350.2-G-1, Green Book, March, 2008.
10. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.
11. D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.
12. Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.
13. Mr. Gurjeevan Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue Singh, Mr. Ashwani Singla and 4, August 2011.
14. Hashizume, "An analysis of security issues forcloud computing", Journal of Internet Services and Applications 2013.
15. Rashmi, "A Survey of Cryptographic Algorithms for Cloud Computing". International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS),2013
16. Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC- 2010)
17. Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48, 203-209.
18. Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.