Survey on Block Cipher-Text Cryptography Algorithms

Dipak S. Kharpas
Computer EngineeringSPPU
Pune University,
Maharashtra, India

Yogesh S. Khandve
Computer Engineering SPPU
Pune University,
Maharashtra, India

Omkar M. Dani
Computer EngineeringSPPU
Pune University,
Maharashtra, India

Sandesh D. Godase
Computer Engineering. SPPU
Pune University,
Maharashtra, India

Bhagyashree Dhakulkar
Dr.D.Y.Patil School of
Engineering &Technology
Savitribai Phule Pune University,
Maharashtra, India

ABSTRACT
Cloud storage is an online data storage and it is located as centrally.Cloud data ownerprovidethe facility for users to online store their data and access from any location. Though it has reliable for the user to achieve a secure and dependent cloud storage service. Ina key aggregate crypto-systemkey is generated fordifferent attributes of data in different cipher text classes and its associated keys. It derived aggregate key on the basis of attribute and identitywhich, depending on the different classes according to cloud data owner. By using this technique aunique cryptographic key achieves. It is optimallysecure for cloud data and privacy preserving key generating process.The cloud data ownerdecidesthe access levelof the data, such as public, private and hierarchyaccess level in order toenhance the data access capability in a data sharing cloud mechanism.Blowfish is thebest data security algorithm. It is higher security and faster execution as compared toother cryptographic algorithms. The blowfish algorithmis a secure for storing data in the cloud.It is an effective derivation of secret key generation and key management.

General Terms
Cipher-text, Encryption, Decryption,Data Sharing,Key Aggregate Cryptosystem,cloud storage.

Keywords
AES, DES, KAC, DES, IDEA,Blowfish,IDEA,ABE,IBE.

1. INTRODUCTION
Now-a-days cloud is the best storage for storing users confidential information.It provides all types of services for those users who use online resources. Cloud provide the best option to store, access, update their data. Many users are accessing the cloud space since Google Drive,DropBox. Even though common users are getting aware of its access and convenient use for data storage. Now-a-days all user use internet. Cloud is best for storing data online. It is located as centrally hence it should be able to fulfill every needs of the user from any corner of the world.One of the main issue in cloud service is the safety of data saved on a cloud. To make that data safe is one of the problems. Because the cloud data user cannot put complete and blind trust on the cloud provider for security and privacy of their data. Cloud user is un-aware of what happens to their data after saving it on the cloud. Is it confidential and integrated from another user and cloud provider itself. There are many Cryptographic Algorithms to solve this type of issue. One of the method is that the owner of the datait has to provide the permission to access to complete data instead of selected data because for selected data access, permission cannot be granted. Another method is separated encryption. In that data is encrypted separately one-by-one and private keys are sent to the user who actually request for that data. But it is quietly impossible in practical use and time complexity and space complexity is issue occurs. Before sharing data in cloud first data is encrypted with attributes. Secret keys are combined and get converted to one single aggregate key and sendtote uservia email or message. Due to this Time, cost, complexity even though space can be saved.That aggregate key is only used to decrypt data with which the aggregate key was formed and encrypted. By this the other data from same user don't get affected and remains safe from receiver user.

2. CRYPTOGRAPHY
Cryptography is a technique to hide the secret information from unauthorized users who is not authenticated.It encodes the secret information using mathematical techniques into cipher-text which is unreadable format, and then transforming that message back to its original form.

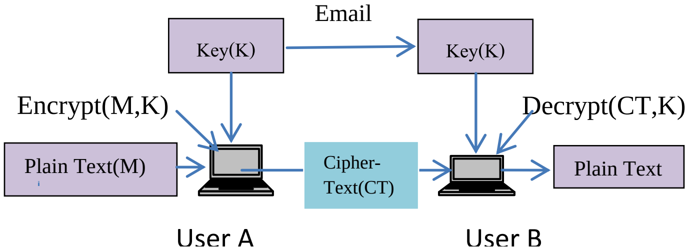

Fig 2.1 SymmetricEncryption And Decryption

Plaintext - the original message.**Ciphertext** –It is the unreadable format of message **Key** –key is nothing but some critical information which is used by the algorithm (cipher).It's known only to the sender & receiver. **Cipher** – The Cipheris a mathematical model for converting an original message into the unreadable form called as cipher-text. In fig 2.1 User A encrypt plain text using their Secret key by using analgorithm(cipher) and generate's cipher-text and send to the User B..After Receiving secret key and cipher-text then user Decrypt the Message using algorithms which are used by the sender.

3. KEY-AGGREGATE CRYPTOSYSTEM

In a key aggregate cryptosystem [2] use anaggregate key for encryption and decryption.During generating aggregate key it defines a user level hierarchy. Aggregate key is nothing but a collection of various user's secret keys. Encryption of the messages can be done by using encryption algorithms. Thus the generated master secret key is used to create an aggregate key in the process of extraction. The generated aggregate key sent to delegate securely as an email or through portable devices. Finally, any client with an aggregate key able to decrypt the data associated with this key receive though the process called Decrypt.The key aggregate crypto-system provides abetter performance in order to reduce the computational complexity of the overall algorithm. Key aggregate crypto-system is a technique that improves the operatibilty of algorithm and reduce the complexity in computation. The cipher-text classes have their own private key by using that key it can only decrypt. The KAC generate the aggregate key from the various secret keys. This aggregate key hasmore power to decrypt any of that cipher-text class.The Receiver can get the aggregate key from a sender or data owner via email so that receiver can decrypt the same data that encrypted by same aggregate key. By this other data that are outside cipher class remain hidden to the receiver. Another feature is that the key size of cipher text, master secret key and aggregate key remains constant. Ciphertext class doesn't require establishment with each other though KAC is flexible.

4. KEY-AGGREGATE ENCRYPTION

In Key-Aggregate-Encryption, users perform encryptionusing public-key and the identifier of ciphertext class and cipher-text are classified into a different class .To extract secret keys for different classes by using the master secret key.Aggregation key uses to specify the access policy based on different classes of cipher-text.Aggregate key provides the more security and efficiency.

Architecture

1. **Setup:**The setup phase generates the Public Key and Master Key.
2. **Keygen:**The keygen phase takes master key MK as input and S i.e. set of attributes that describe the keyand generate outputs asa private secret key SK.
3. **Encrypt (PK,i,M):**Encrypt phase performed by anyone who is the owner of the data. Encrypts the data 'Message(M)' by using public key and the index i denote cipher class and generate outputs CT which cipher-text.
4. **Extract (MSK,S):** Extract phasetake set of indices of the cipher class along with the master secret key asinputand generate aggregate key.
5. **Decrypt(Ks, S, i,CT):-** The decryption phase takes as input Ks which is generated by extract phase.on input Ks,set S ,an index i denote ciphertext class CT.Then it will decrypt the ciphertext andreturn anoriginal message.

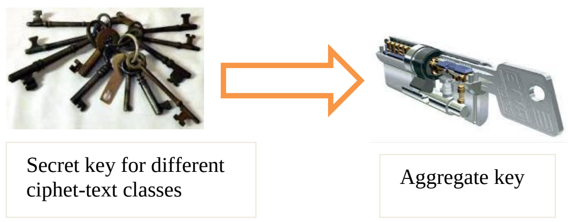

Fig 4.1 multiple secret keys and Aggregate Key

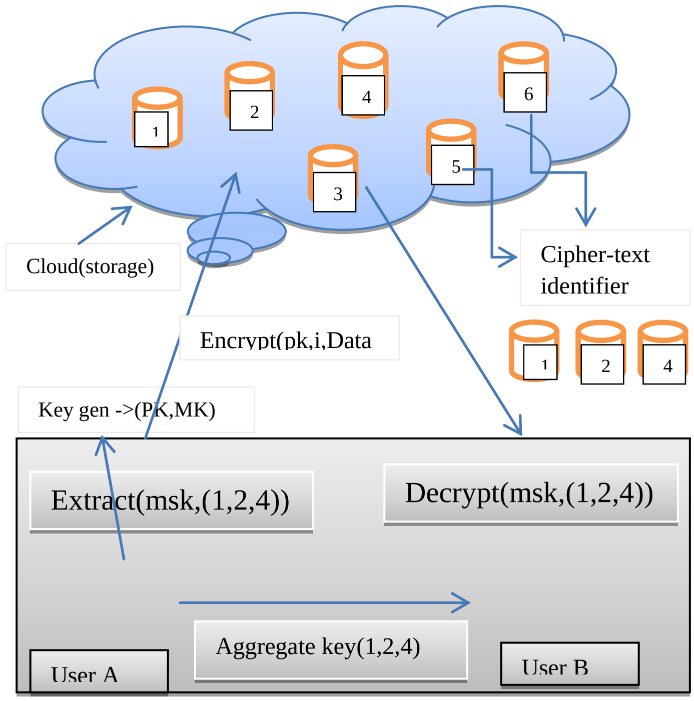

Fig 4.2 Data sharing in the clouds using KAC

The above figure shows how the data has been shared in the cloud. Suppose a user 'A' wants to share the data 1, 2, 4 to another user 'B' then the user A generates an aggregate key using the attributes of 1, 2, 4 and sends it to the user B vai email. The user B thus decrypts the required data by performing the setup to generate the parameters, and then the keys are generated followed by the encryption process.In the extract process generates the aggregate key and then this key is used by user B to decrypt the data.In the traditional methods the key assignment will be provided separate keys for every data to be decrypted. This will increase the key generation process as well as consume much larger space.

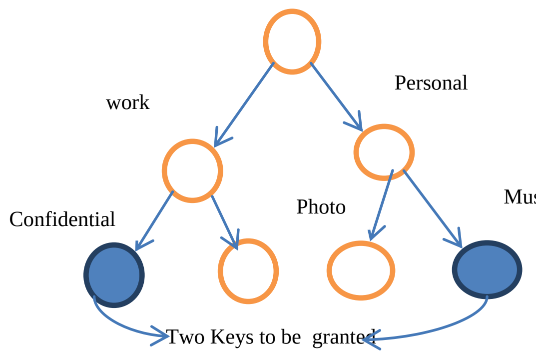

Fig 4.3 Key assignments for traditional cryptographic scheme

Here in the above figure four separate keys are to be granted for the availability of these files. The KAC uses only half of the no. of keys than in the traditional crypto-system schemes.

For example, in the figure

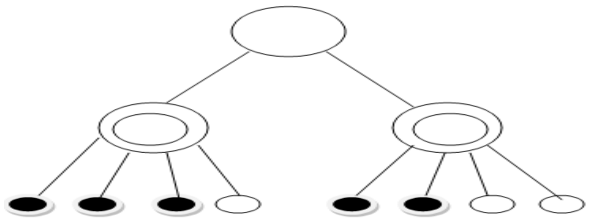

Fig 4.4 Key assignments in KAC

Only two different keys have to be provided for the access of five data. Hence the hierarchical level of classification of data has a more advantageous level than the data arranged in class level.

5. CRYPTOGRAPHIC ALGORITHMS

There are two types ofcryptographic methods for encryption and decryption..

1.Symmetric Key Algorithm

2.Asymmetric key algorithm

There are lots of crypto-graphic algorithms used public key system and secret key system for encrypting data and most of all comes under the these categories. In this symmetric key algorithm shared key called as secret key used to encrypt and decrypt plain text. It's doing everything in one single key.IDEA, DES,3DES, AES issymmetric algorithm .The symmetric algorithm used is having many advantages even though it comes with certain problems like power consumption, high execution time, cost complexity and very low throughput. The encryptions and the decrypt procedure are consuming a large amount of time. Hence it increases its execution time along with the power consumption. Since the time taken to execute higher the cost, complexity is also higher. Even though the compressed data storage mechanism proposesby the algorithm , the cipher text classes occupy a higher space in the cloud network. To over these issues to a limit we come forward with the proposed system.The Asymmetric key algorithm is also called as public key algorithm. Public key and private key is used for encryption and decryption in asymmetric algorithms.That means encryption, are performed by one key and decryption are performed by another key. It overcomes the drawback of symmetric algorithm. Symmetric algorithms easy to hack by anyone but asymmetric are difficult to hack by anyone .Diffie-Hellman and RSA,DSAthese are asymmetric algorithms.Asymmetric algorithm is more secure, but it takes more time for encryption and decryption.

5.1 DES

DES [2] is a Data Encryption Standard. It uses56 bit key size and 64 bit block of data for encryption. The Data Encryption Standard is the block cipher algorithm.It performs 16 rounds for encryption and decryption. It is afirst encryption standard.It used 64 bits key size with 64 bit block size of the data element. DES algorithm is not so much better for providing security.This algorithm isan insecure block cipher-text algorithm.

5.2 3DES

3DESis a new versionof DES algorithm [2]. It requires 64 bit block sizealong with 192 bits key size.Thisalgorithm is developed for overcoming the drawback of DES.It is same as DES but the only difference is we apply 3 times, i.e on 2^{nd} time we apply DES on previously encrypted ciphertext by DES. Due to this strategy we achieve higher security than previously used DES algorithm. It is slowerthan other block cipher methods.

5.3 RC2

RC2is Block cipher encryption algorithm developed in 1987.It usesa secret key for encryption. It uses64 bit block of data and key which is variable.Therange of key size varies from 8 bits to128 bits. RC2algorithm [2] isnot so much good for security.It is vulnerable becausethe related key attack using 2^{34} chosen plaintext is possible.

5.4 RC 5

RC5 is a 32/64/128 bit block cipher algorithm developed by Ronald Rivest in 1994.It is Symmetric Block cipher algorithm.It has a variable number of Rounds,word size and a secret key.It usesthe data dependent operations.It required low memory. Due to the data-dependent rotations, differential cryptanalysis and linear cryptanalysis is not possible. The key used is strong if it is long.If the key size is very less thanthisalgorithm is weak.

5.5 RC6

RC6 algorithm are derived from RC5.The Advanced EncryptionStandard algorithm has some drawback. To overcome these drawbacks RC6 was designed. RC6 [2] has a 128bitblock size.It performs encryption/decryption using 128, 192 and 256 bits of key sizes.

Comparison of RC algorithms;

Algorithms	RC2	RC4	RC5	RC6
Year	1987	1987	1994	1998
Cipher	Block	Stream	Block	Block
Block size	64	2064	32,64,128	128,192,256
Key size	8-128 default 64	1-256	0-2048	128,192,256
Rounds	16	256	0-255	20(Recommended)
Possible attacks	Differential, Linear	BEAST	Differential	Correlation
Security	Vulnerable	Vulnerable	Vulnerable	Considered vulnerable
Operation used	+,,&,~,ror, Rol.	+,mod ,xor.	+,-,<<<, >>>,xor, mod	+,,*,<<<, >>>,xor,mod

5.6 Identity Based Encryption with compact key

IBE means identity-based encryption[3]. It is a public-key encryption technique. In this algorithm public-key of the users can be set as an identity, for e.g.email address, mobile number. Thesecret key is generated by using user's identity. The cloud data owner take the public parameter and a user identity to encrypt a message. The recipient can decrypt this cipher text by using his secret key. Each user has its own identity by using this identity secret key are generated for each user.In this way collect all secret keys which are coming from different identity of users. All these secret keys combine into single keys called as aggregate key.Key aggregation means collection all secret keys.This significantly increases the costs of storing and transmitting cipher-texts, which is impractical in many situations such as shared data in cloud storage. As Another way to do this is to apply the hash function to the string denoting the class, and keep hashing repeatedly until a prime is obtained as the output of the hash function.it used compact key for encryption.This compact key helps to decrypt cipher text.

5.7 Attribute Based Encryption

ABE [4] is an Asymmetric key encryption algorithm.That means it used public key strategy for encryption). This algorithm is based on secret key of users and cipher-textwhich are dependent upon the user's attributes. Duringthe encryption process it specifies an access control policy over userattributes.The successful decryption of ciphertext possible if and only if the set of attributes of user key equal to the attributes of ciphertext.The size of the ciphertext is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes. In attribute based encryption [4]each cipher-text associated with an attribute of users. For examplethe secret key for the policy (1 ,3 ,6 ,8) one can decrypt cipher text, tagged with class 1, 3, 6 or 8. The key size is increased linearly when the number of attributesis increased.

6. CIPHER-TEXT ALGORITHMS

6.1 AES Algorithm Description

AES is a block cipher-text algorithm which follows symmetric way to encrypt data. In this algorithm encryption and decryption perform by using the same key. AES has 128-bit blocksize of the data element.On AES key size not fixed it varies like 128,192 or 256 bits.AES use term name 'state' in which there is 4x4 column major order matrix of bytes.

The number of cycles of repetition is as follows:

a. 10 cycle repetition is required for 128 bit keys.

b. 12 cycle repetition is required for 192 bit keys.

c. 14 cycle repetition is required for 256 bit keys

1 Key Expansions

There are a number of rounds, each needing its own key, so the actual key is stretched out and transformed to give portions of key for each round.128 bit key is required separately for each round.

2.Initial round:-

1.Add-Round-Key : it performs the bitwise xor operation.It adds the add-round key initially.

3. Round

Each and every round of encryption process requires the following four types of operations:

1. Sub-Bytes :-It performs non-linear substitution step where each byte is replaced with another according to a lookup table.
2. Shift-Rows :-It shifted cyclically the last three rows of the state in a certain number of steps.
3. Mix-Columns :-It mixesthe columns of the state and then combining the four bytes in each column.
4. 4 Xor-Round Key.

4. Final Round(without mixed column)

1. Sub-Bytes
2. Shift-Rows
3. Add-Round-Key

Decryption is the reverse process of encryption and using inverse functions: InvSub-Bytes, InvShift-Rows, InvMix-Columns.

6.2 Blowfish AlgorithmDescription

Blowfish [6] is a symmetric block cipher-text algorithm which was designed in 1993 by a Bruce Scheier. It is one of the feasible algorithm for Encryption and Decreption process. It uses a block of 64 bits in size of data element and also used a key whose length varies from 32 bits to 448 bits, So that Blowfish is a best for securing data. It is suitable for applications for the key does not change often till the file encrypted. To overcome drawbacks of the data encryption standard, blowfish algorithm is designed. Blowfish is astronger algorithm for encryption and also give faster results compare to others symmetric algorithm.Characteristics of this algorithm are followed:

Faster: Data encryption process requires26 clock cycles per byte on 32-bit microprocessor.

Compactness:It required less memory to execute efficiently.

Simple:It uses XoR, addition, lookup table for storing a 32-bit operands.

Secure:It is more secure because length of key size is variable.

The range of key size 32 to 448 bits. It usesdefault 128 bits key length.

Blowfish algorithm encrypts block data of 64-bits at a time.

There are two methods needed for encryption and decryption.

1. Key-expansion

2. Data Encryption

1. Key Expansion:The key expansion is processedtoconvert a key of 448 bits into different sub-keys, making it to a size of 4168 bytes. Blowfish usesa number of sub-keys. These keys usedfor any data encryption or decryption operation.

The n-array consists of 18, 32-bit sub-keys:

N1, N2,N3,… N18 .

Four 32-bit Q-Boxes consist of 256 entries each:

Q1, 0, Q1,1,………..Q1,255

Q2, 0, Q2,1,………..Q2,255

Q3,0, Q3,1,………..Q3,255
Q4,0, Q4,1,………..Q4,255

2. Data Encryption:During encryption 16 round is required for the encryption process. In data encryption method Each separate round consists of a key dependent transformation and a key and data dependent changeover.It performed XORs and the additions to the 32-bit words.

6.2.1 Pseudo code

Blowfish Algorithm requires16 rounds to compute.

1. The input data element B is of size 64 bits.

2. We get BL, BR by simply dividing B data element in two equal parts in size.

3. for i = 1to 16:

BL = BL XoR Pi

BR = F(BL) XoR BR
Swap BL and BR
After the sixteenth Round,

4. Swap BL and BR (Undo the last swap.)
5. BR = BR XOR P17
6. XL = xL XoR P18
7. Recombine BL and BR

6.3 Comparison of Cryptography Algorithm

Speed Comparisons of Block Ciphers				
Algorithm	**Clock cycles per round**	**# of rounds**	**# of clock cycles per byte encrypted**	**Notes**
Blowfish	9	19	18	Free, Not patented
Khufu/Khafre	5	32	20	Patented by Xerox
RC5	12	16	23	Patented by RSA Data Security
DES	18	16	45	56-bit key
IDEA	50	8	50	Patented by Ascom-Systec
Triple-DES	18	48	---------------	---------------

6.3.1 Comparison of AES and Blowfish Algorithm with respective Time in Second

Algorithm	Encryption/Decryption For 64 bits	CPU Time
AES	1.261816	1.54440990
BLOWFISH	0.850568721	0.07800050

The performance speed of the algorithm is also exciting. Chances are high to thinking that a 448 bit key length is too much. Blowfish has large key lengths still result of this algorithm isa much faster as compare the performance many other encryption algorithms.

7. CONCLUSION

After analyzing all these cipher-textalgorithmblowfishalgorithm has much more advantages as compared to the performance of many other algorithms.Blowfish can be marked as an excellent encryption algorithm.The speed of the AES algorithm is less as compared to blowfish algorithm. It is a time consuming process. Blowfish Algorithm is Faster, smarter, Better for encryption and decryption process.Thus the easily shared sensitive information in cloud storage by using this algorithm. It also compressesthe data in order to save cloud storage space.

8. ACKNOWLEDGMENTS

We would like to thankthose people who have guided us for doing this survey of cryptography algorithms.

9. REFERENCES

[1] Satish s Hottin, 2Mr. S.Pradeep ,M.tech, Computer Science SRM University, Chennai Assistant Professor SRM University, Chennai “Efficient Secure Date Sharing In Cloud Storage Using Key-Aggregate Cryptosystems”Vol 2 ISSN: 2321-9939

[2] Rimpi Debnath, Priyanka Agrawal, Geetanjali Vaishnav“DES,AES and triple DES symmetric key cryptography algorithm”.

[3] Jin Li, Jingwei Li, Xiaoeng,ChunfuJia and Wenjing Lou ” Identity based Encryption with outsourced Revocation in cloud computing”, vol0018,2013

[4] Minu George,Dr. C.Suresh Gnanadhas Saranya.” A Survey on Attribute Based Encryption Scheme in Cloud Computing”.

[5] Milind Mathur, Ayush Kesarwani“Comparison Between Des , 3des ,Rc2 , Rc6 , Blowfish And AES ” .

[6] Diaa Salama Abdul. Elminaam1, Hatem Mohamed Abdul Kader2 and Mohie Mohamed Hadhoud3“Performance Evaluation of Symmetric EncryptionAlgorithms”.

[7] Narender Tyagi Anita Ganpati “International Journal of Advanced Research in Computer Science and Software Engineering”

[8] Mrs. Komal Kate, Prof. S. D. Potdukhe “ Data sharing in cloud storage with key-aggregate cryp osystem.”

[9] Ramakrishna Jadhav1 ,Snehal Nargundi2 “a review on key-aggregate cryptosystem for scalable data sharing in cloud storage” International Journal of Research in Engineering and Technology ISSN: 2319-1163 | ISSN: 2321-7308

[10] RashmiNigoti1 ,Manoj Jhuria2 Dr.Shailendra Singh3 “A Survey of Cryptographic Algorithms for Cloud Computing”International Journal of Emerging Technologies in Computational and Applied Sciences “ISSN (Online): 2279-0055.

[11] https://www.academia.edu/6786694/An_Aggregate_Key_Based_Cryptosystem_for_Secure_Data_Sharing_in_Cloud_Computing.

[12] www.researchgate.net/publication/260710957”KeyAggregate_Cryptosystem_for_Scalable_Data_Sharing_in_Cloud_Storage key aggregate cryptosystem”.