International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

Secure Communication with Blowfish Cryptography for Data Sharing on Cloud using Android Devices

J. Unni Kiran, P. Sai Kiran

Abstract: ***Communication over desktop applications and mobile applications has been increased. Requirement that the information security is very significant. This document is about encoding or decryption of text data from applications using block cipher called 64/128 Blowfish bit to extend security while sending data to the cloud. It rounds 16 times to and the key length must be multiples of 8. Java has accustomed implement a blowfish algorithm, in android programming and checking Blowfish encryption performance with other encryption algorithms based on network and energy usage. The proposed algorithm is meant using android(java).***

Keywords: Blowfish, data, encryption, decryption, communication, cloud, performance and block cipher.

I. INTRODUCTION

Securing information/data is necessary, data or information shared on cloud is very important task for the todays market, because most of the data has been attacking by the hackers by using different attacks so the encoding is very crucial task for the information technology to secure data from hackers. So, the encryption standards are become very popular to secure data in any storage by using different standards. Information security is of final concern as web attacks have developed more and more serious. Data/information encryption and decryption have applications in online communication, multimedia systems, banking, mobile applications, etc. Previously additional encrypting and decoding procedures suggested. To modify the information, secure from different attacks and for intellectual honesty, to overcome this issue there should be an encryption standard to encode the data before sending it to the cloud. Banking, information of the patient in hospitals deals with confidential information. Most of the data are collected and stored over the cloud across different networks. This information got leaked lead to false doing. So, in the present document, we are implementing the Blowfish algorithm to encrypt data before you can send data to Firebase(cloud).

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
Unnikiran J*, Computer Science and Engineering, K L University, Vaddeswaram, Guntur, India. Email: jaladiuk@gmail.com.
Dr. P. SaiKiran, Computer Science and Engineering, K L University, Vaddeswaram, Guntur, India. Email: psaikiran@kluniversity.in.

The standard is known as symmetric or private key encoding standard which is fastest and related to AES which is also known as single key encoding standard. The main aim behind the design of this proposal is to get them and the best security/performance trade-off over existing data. The Blowfish encryption/decryption algorithm gives better security. It has a longer key. The philosophy of the proposed security algorithm which is used to provide a security standard that gives fast performance when compared with other algorithms.

II. PROCEDURE

The data that has been sent to cloud across online means in web applications have the greatest demand all over the world. In the present situation, so many web applications are suffering from these attacks to secure the data that they have been published on the internet. There are so many applications are trying to secure the information that they published on the internet or online. Because, they are confidential, belongs to individuals or organizations. The data protection is crucial for organizations because the evolution of the information has become part of our life. The data encoding standards are improved. To the present attacks that can handle the situation of the attack's encryption techniques, they will use different standards to encode the data into different forms by using the data and keys as inputs. The reversal of the technique to decode data by using a key and the encoded data to get the original information. Not a single technique to encode and decode data. They will use different standards to do the process to get the original data in a very secure manner. In the algorithm, the key length is more so, while the encoding data the inputs play an important role. Similarly, while decoding the data using same key is also important to change the data into the original text. Thanks, the new techniques for securing the data from web attacks.

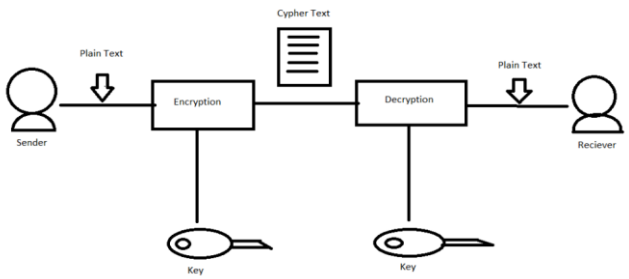

Fig. 1. Data flow.

Bruce Schneier designed a quick and free algorithm, in 1993 for the existing encoding algorithms. Since that time, it's been overhauled considerably, by now it is the popular encoding algorithm to secure data. Which is also powerful and quick to secure data in online and in web applications.The standards used the Blowfish could be symmetric structure Network, these will repeat for sixteen rounds to encode the data. The block size of this algorithm is 64 that they calculated in bits. Therefore, we can consider the key length from 32 to 448 bits depends on the users or client's point of view. So, there is a essentials standard that must follow initially to encode the data to make it work on microprocessors.

III. EXISTING TECHNIQUES

3.1 Triple Data Encryption Standard (TDES)

This algorithm is used as a substitute for the data encryption standard. In this standard, we use combining keys to make it rounds three. Here the message will be encoded to double of 168 where it is very hard to decode. Because the number of combinations is more it will take more execution time. The performance of this standard is low. But it takes very low memory. According to the length of the algorithm, while performing the task, the application may crash.

3.2 Advanced Encryption Standard (AES)

The encryption standard the people are using nowadays is advanced encryption standard. This is highly secured. The performance of this encoding technique is very good. Similarly, the decoding technique algorithm also shows better performance. It is developed in 2000. The developers are Vincent and Joan. This standard uses Rijndal block cipher. The standard uses 128, 192, or 256-bits for the key and the blocks. By considering the lengths of keys are 128-bit, the block cipher will handle in nine rounds. It will execute eleven rounds for a unit having 192-bit. For 256-bit, the execution will go for thirteen rounds. The drawback of this algorithm is it will use simple numerical framework. Every time, it uses the same encryption standard at every block. The Most significant problem with this symmetric encryption sender and receiver must have key coordination otherwise it won't decrypt the data.

3.3 Data Encryption Standard

Before DES, there is so much of data is hacked by using various attacks. Whatever it may be thanks to DES which is earliest data encryption standard. IBM has acquired the standard. In 1997 it was considered as national level. It consists of 56-key length which will be handled by 64-bit applications.

3.4 Encryption Standard Blowfish

The encryption standard which became very popular after using it for web applications. This is a freely available algorithm developed by Bruce Schneier. The popularity of the algorithm increases gradually because of its performance and maintenance and its key length. The Blowfish known as block cipher having 64-bit and it is suggested as a substitute DES. For this standard to permits are required because of its effectiveness. In consists of 4 S-boxes and a P-array which are available in table operators. The main content of this standard is it a Feistel block cipher. It will completely depend on its rounds. To meet the basic principles of DES it uses P function. So, it delivers the encrypted data with better speed and low energy to run the applications. The 32-bit chips use this algorithm because it is fast. The Blowfish algorithm consists of a lookup table, XOR and addition.

IV. PROPOSED TECHNIQUE

The Blowfish cryptography standard was developed by Bruce Schneier. He makes this algorithm open source because it avoids all the attacks. There is no mark on the Blowfish standard to date. The algorithm will use the changing key length. The length of the key varies from 32-bit to 448-bit which is not available in any other algorithms. Without negotiating the security standards, he built this algorithm. This standard is designed for encoding and decoding the data with high speed in the application performance and energy-saving with implacable security for the data. There is F-function which consists of blocks, S-boxes, XOR, and addition. The subkeys are used as P-arrays for each round in the encryption and decryption process. This diagram will show the flow of data.

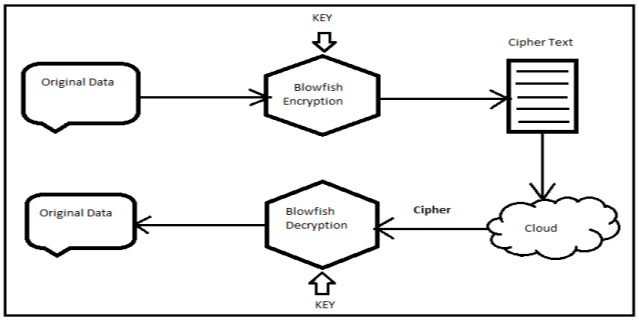

Fig. 2. Architecture.

This process is a different feature from the permutation function undertaken in DES.The encrypted data which is encoded before transfer to cloud will be converted to byte arrays and then it will convert to hex decimal code and will forward to cloud.

4.1 Data Encryption

In data encryption there are to two inputs one is original data and key of length which is based on the standard of the encryption. In this algorithm (Blowfish) the data will divide into two blocks that consists of 32-bit each based on block cipher.

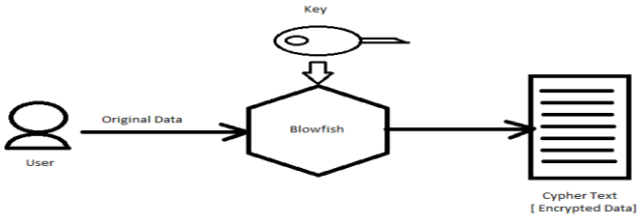

Fig .3.Data Encryption.

These two blocks are sub divided into four blocks that consists of four 8-bit blocks each. Later, it will loop 16 rounds and gives two blocks each of 32-bit. Here P-arrays holds keys for each round. It will be subjected to subkeys in each round for XOR and addition operations and it will be combined to get 64-bit cipher text. Here F function is used in encryption.

Algorithm (Blowfish)

Divide X in two 32-bit splits X_l and X_r.

Each 32-bit split will be loop for 16 rounds using subkey P_i.

For (i = 1 to 16)

$X_l = X_l\ P_i$

X_r= F (X_l) XOR X_r

Swap X_l and X_r

X_r= X_rXOR P_{17}

X_r= X_l XOR P_{18}

Join these 32-bit X_l and X_r using addition operation.

Output X (64-bit data block: ciphertext)

Decoding processes is identical to encoding standard, except for that sub keys P_1, P_2... P_{18} is being used in the opposite sequence.

4.2 Data Decryption

Here the cipher text also called as encrypted data is divided into two blocks of each 32-bit. Every block goes on as same process in the encryption standard in the Blowfish algorithm. But the process will start from subkey P_{18} to end of all rounds. It meets the post processing block to decrypt the cipher text into two 32-bit block. Finally, these two blocks are combined to get original text or decrypted data.

Note: We will use same key for both encryption and decryption to encrypt and decode data respectively.

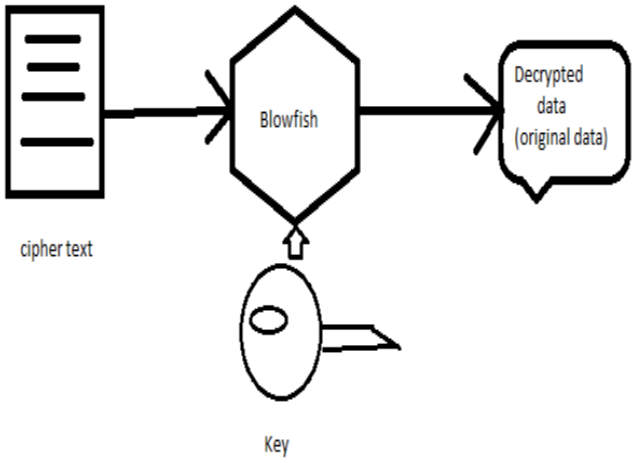

Fig. 4. Data Decryption.

Values	A	B	C	D	E
Length of the key	Module dependent.	56bits	168 bits, 112 bits	128, 192, 256	32-448
Rounds	1	16	48	10-128, 12-192, 14-256 bit key	16
Block size	Variable	64bit	64bit	128bit	64
Speed	Slow	Slow	Very slow	Fast	Fast

A. RSA – This is a public key cryptosystem which is also known as first public key cryptosystem. It uses to keys one is public key and another is private key.

B. DES – This is a private key cryptosystem which is used to encode and decode data. It is implemented by Feistel block cipher.

C. Triple DES – This is asymmetric key block cipher.

D. AES - This is abbrevated as Advanced encryption Standard which is also known as symmectric key cryptosystem. This uses only a single key for both encrption and decrption which is known as private key.

E. BF – This is called as symmetric key cryptosystem which is also commonly known as private key encryption. It also uses same key for both encoding and decoding.

Tables: Comparison of Different Encryptions.

4.3 Performance

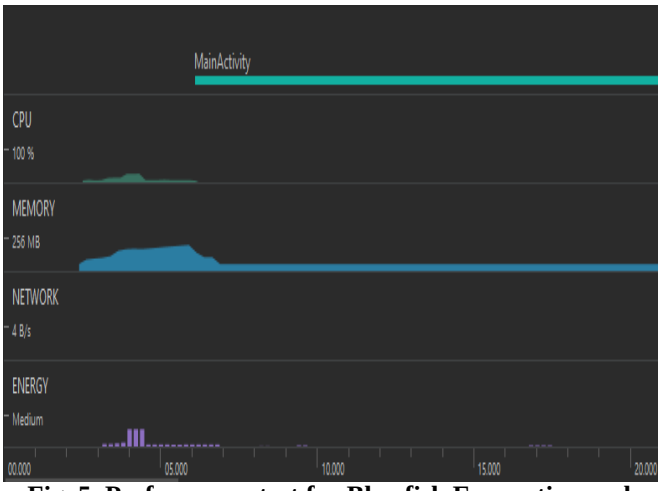

Fig. 5. Performance test for Blowfish Encryption and Decryption.

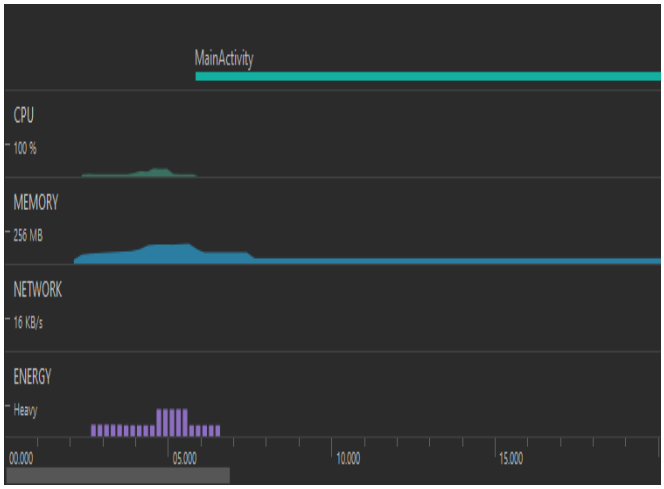

Fig. 6. Performance test for AES Encryption and Decryption.

The comparison between AES and Blowfish based on encryption and decryption using android application

1. The CPU usage is 100% for both AES and Blowfish algorithms.
2. The memory usage is 256MB/156MB for both AES and Blowfish algorithms.
3. The Network using in AES is 16KB/s and in Blowfish 4B/s.
4. The Energy usage in AES is HIGH and in Blowfish it's MEDIUM.

Based on Key Size:

For AES 256 key size which is that the highest key size in AES the network speed 12.2kb/s with CPU and Network light. For Blowfish 448 highest key size during this encryption, the Energy used for performance is medium at the initial its network speed is 12.4KB/s with CPU light and Energy light state. It reaches Medium CPU with Light Network on reference to the cloud.

So overall performance is more in the Blowfish for 128 key sizes.

Sending Data to the Cloud:

The input data will be sent to cloud-based email and password authentication. By default, login credentials will be taken to send data to the cloud. The login data will be verified using the same email and password. Initially, the data will be converted into byte arrays. The key will be generated automatically by using byte arrays which will be on the users' side. The key generator will generate a key based on symmetric key by its instance using the Blowfish algorithm. Later it will be randomly generated by using Secure Random using "SHA1PRNG". The key start will be sed seed by using generates key. The key generation uses the key size by default 128-bit key. Then the key will convert data into encoded bytes. Later, the encoded bytes will be sent to encrypted functionality which is in byte array format. The cloud accepts only the string format. So, the byte arrays will be converted to a string format and it will be pushed to the cloud(firebase) using credentials.

encrypted Data = encrypt (key, message. get Bytes ()).

Data Retrieval:

Data retrieval is the reversal of the encoding technique. Where the string data which is available in the cloud will be retrieved by using Auth of the cloud whole node data will be read. Later, it will be converted to byte arrays. By using the same key which is used to encode data and encrypted data from the cloud will be sent to decrypt data function which will generate byte arrays of the original data.

decrypted Data = decrypt (key, encrypted Data).

The original data byte arrays will be converted to the original text.

V. RESULT

In this work, mock the data processing section of encoding and decoding using Android software. The message/text has been considered as input to the Blowfish algorithm. On behalf of that a key which is also used as input for the encryption. Result shows the original text, encrypted data, and the decrypted data.

The encrypted data by using this algorithm will be sent to cloud. We are going to check that the decoded data is identical to the original data. The receiver will get the information without loss of data what sender was sent to him/her.

Fig. 7. Main

After 16 rounds the data is encoded and sent to the cloud. The encrypted, data have byte arrays as seen in the diagram. After decryption, the data in byte arrays will be shown as decrypted data. And finally, the Decrypted text also called the original text will be displayed as same as given plain text.

Fig. 8. Display

The data in the cloud(firebase) will be saved in an encrypted format. So, the data saved in the cloud will be secured that will not visible to others.

Fig. 9. Cloud data

VI. CONCLUSIONS

The data encryption gives performance of 4 bits per cycle. We can restrict the output as well as input based on the limitation of the bits. The performance can be checked by using all the deceives to fulfill the encryption or decryption standard. Thanks to key length that it is variable from 32 to 448. Because of the key where it won't change for encryption and decryption it creates strong and secure communication between applications. We use Blowfish algorithm It is quicker than data encryption standard. The Blowfish is used frequently because of

1. It is taking less time to execute.
2. It uses low memory.
3. It uses lesser energy while executing the application.
4. It has negotiable key length so that the data is more secured.

For this simulation every key length has been considered in the encryption and decryption process.

REFERENCES

1. Ketu File white papers, "Symmetric vs Asymmetric Encryption", a division of Midwest Research Corporation.
2. Tingyuan Nie and Teng Zhang, "A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009
3. Ozturk, I. Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004.
4. Bruce Schneier. The Blowfish Encryption Algorithm Retrieved October 25, 2008, http:// www. schneier.com/ blowfish.html.
5. Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).
6. Nadeem, Aamer; "A Performance Comparison of Data Encryption Algorithms", IEEE 2005.
7. Narendra Singh Yadav; "Analysis of modified Blowfish Algorithm in different cases with various parameters ", IEEE 2015.
8. "Blowfish—One Year Later", Dr. Dobb's Journal, September 1995.

AUTHORS PROFILE

Unnikiran Jaladhi is pursuing his Master of Technology in computer science and engineering at Koneru Lakshmaiah Education Foundation (Deemed to be university), Vaddeswaram, Guntur, Andhra Pradesh, MCA – PVPSIT, JNTU Kankinada.

Dr. P. Sai Kiran K L University Professor in Department of Computer Science and Engineering. NIRF Committee member. Cloud Computing Research Group Head Professor In-Charge for Coding. Editor for KLU Newsletter 4 Issues - SPOC – APSSDC. Professor In-charge for University Automation and Website. Professor In-charge for Information Center. Ph.D. – JNTU Hyderabad. MTech – SRMIST. M.C.A – Bharathidasan University.