Novel Approach of Cryptography by Hybridization of ECC and Diffie-Hellman with Blowfish Method in Cloud Environment

Tanmaya Mahandru
M.Tech Scholar, CSE Department
Doaba Institute of Engg. & Technology, Kharar

Ramanjot Kaur
Assistant Professor, CSE Department
Doaba Institute of Engg.&Technology, Kharar

ABSTRACT

Cloud computing is an emerging field in information technology field. It is growing very fast and provides the effective services to the users in every field. Cloud stores the data in huge amount on it and it is the main issue to handle the data with proper security. For providing the security to the cloud data many techniques are used by different service providers. In this paper we proposed the Hybrid Blow Fish algorithm combined with AES. Both the algorithms are encryption algorithm which provides the security to the user at sender end as well as receiver end.

Keywords

Cloud Security, Blowfish Algorithm, AES, ECDH.

1. INTRODUCTION

Cloud computing is a term which provides the services over the internet. These services related to the software platform and services. Cloud also provides the infrastructure to the user to develop the applications on it. Cloud provides the storage space to the user to store the data online and access this data anywhere at any time. A cloud provides the platform, infrastructure, function and software at a single click. Cloud provides the hostage of the resources on it for flexible data interchange and communication process. According to the services provides by the cloud it is differentiated into three types that are public, private and hybrid.

From the consumer's perspective, they want their data to be safe as well as time and storage saving. So, in accordance to achieve this, we proposed a hybrid approach of using ECDH with Blowfish Algorithm.
ECDH is a fusion of Elliptic Curve Cryptography with Diffie-Hellman algorithm mainly used for elliptic curves. It is a protocol used for key agreement which makes it more than an encryption algorithm. ECDH means to define how keys must be generated and exchanged between parties; irrespective of the encryption scheme to be used. With the help of this technique, it is possible to exchange the data over an insecure channel as the intruder can intercept the data but will not be able to decode.

For encryption and decryption of the data, we chose the Blowfish algorithm for our research. Blowfish algorithm is categorized as a symmetric algorithm for encryption and decryption of the data. It is considered as fast in comparison with existing algorithms like AES, DES, 3DES, etc. Blowfish algorithm encrypts a block of 64 bits of data with the help of keys of length ranging from 32 bits to 448 bits making it compact and fast.

In this research, we used blowfish algorithm with AES algorithm to encrypt the AES encrypted slices parallel using Blowfish algorithm. After the encryption has been performed, the data has been securely uploaded on the cloud server by using ECDH technique. The main aim of this research is to decrease the time and storage utilization; also ensuring the data security.

2. LITERATURE REVIEW

Cloud computing provides the on-demand services related to hardware, software and data services. The author discussed the various models of cloud computing and security issues related to that model. Intelligent cryptographic approach is used to provide the security to the data. In this method files are divided and stores separately in cloud servers [1]. Content based image retrieval system is used to support the encryption method without any loss of the information. KNN algorithm is used to provide the secure cypher text [2]. Data security and integrity is maintained by using the combination of the encryption algorithm RSA and MD5 hashing algorithm. RSA encrypt file before uploading on the clod and after that MD5 starts its working [3, 4]. The author proposed a method which is based on ID in encryption process. Diffie Hell Man method is used with Elliptical curve method for providing the security to the data over cloud [7, 8]

A summary is given on cloud computing. The summary consists of reliability, availability and security issues and its solution. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry but still they have some issues that exist with the wide spread implementation of cloud computing. The origin of issues is from data sortation remotely from customer's location etc.

3. PROPOSED WORK

In this section we describe the proposed work methodology and flow chart. This work performed by using the AES (Advanced Encryption Standard) and Blow Fish algorithm.

Algorithm
Step 1: Give input in the form of text file by data set. Step 2: Combine the key generated by ECDH (Elliptic curve and Deffi Hell Men method). Step 3: When key generation is completed encryption algorithm is started which is hybrid with AES and

Blow Fish.

- First we encrypt by AES algorithm.
- Then make the slices and these slices optimized by Meta- Heuristic algorithm.
- Apply Blowfish on these slices parallel.

Step 4: Upload the data on cloud when encryption is completed.

- First encrypted data will send to cloud let. Cloud let scheduled by broker.
- Broker scheduled data storage on virtual machine.

Step 5: After encrypt data storage start decryption process

- First download the data from cloud by client.
- Then client key which generate in 2 step decrypt the data.

Step 6: Calculate the time and storage after decryption

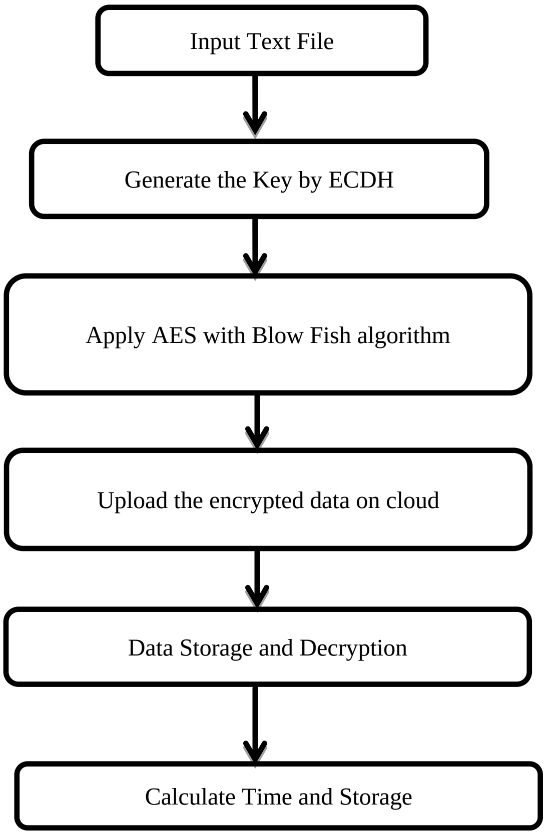
Input Text File
Generate the Key by ECDH
Apply AES with Blow Fish algorithm
Upload the encrypted data on cloud
Data Storage and Decryption
Calculate Time and Storage

Figure1.1 Flow chart of the proposed methodology

A. AES: stands for advanced encryption standard are an encryption algorithm developed by the NIST to provide the security of the data on the cloud environment. It works on the block cipher method on 128 bits data size. AES performs the four major functions that are defined below.

1) Sub Bytes
2) Shift Rows
3) Mix columns
4) Add Key

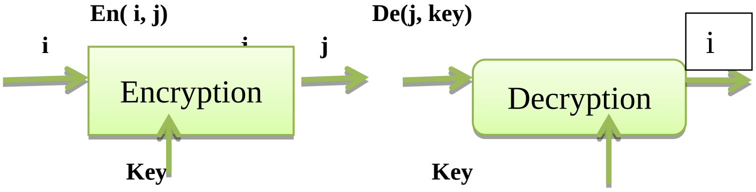

Figure 1.2 Working of AES

Here,

En: define the Encryption function for symmetric block cipher.

i: plain text message of size 128 bits.

Key: Key of size 28 bits it is same for both encryption and decryption.

De: Decryption function for symmetric block.

Figure 1.2 shows the working of the AES algorithm. In this I is the plain text message of size 128 bits given as input for the encryption with the key. Encryption function En(i,j) is applied on the text and gives the encrypted output. On the receiver end decryption function is applied to get the original text by De(j, key). The Key is common for encryption and decryption.

B. Blow Fish Algorithm: It is an security algorithm which works on the block of the text of 6 Bits. This algorithm is very fast and compact in cloud system. It works in the two parts that are following:

1) Key Expansion
2) Data Encryption

Key expansion: It divides the key into the sub keys because it works on the large number of sub keys. Keys are generated before the encryption and decryption process.

The k- array consists of 18 and 32 bit sub-keys:

K1, k2, k3……, k18.

Data Encryption: In this process 32 data is divided into the right and left 16 bit data and XOR operation is applied on it and then swapping process is done on left and right part.

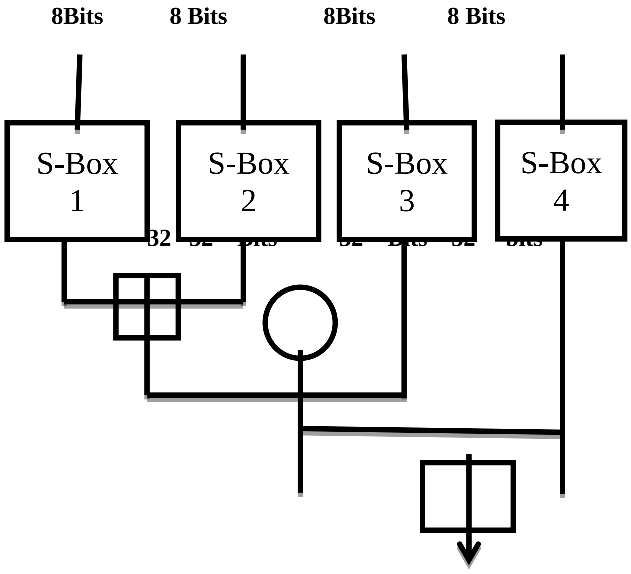

Figure 1.3 Structure of blow fish algorithm

4. RESULTS

This section of the paper shows the results of the AES and Blow fish encryption algorithm. The result evaluation is done on the basis of following parameters:-

- Input File: Show the file input for the encryption.
- Encryption Time: Total time consumes in encryption process.
- Throughput: Shows the amount of encryption file in given time.
- Encrypted File Size: Size of encrypted file.

Table 1.1 Results of the Blow fish and Existing method

Parameters	Blow Fish	RSA and MD5
I/P file Size(Mb)	0.735617	0.735617
Encryption File Size**(Mb)**	1.338909	1.338909
Encryption Time(Sec)	0.07	0.094
Throughput(Mb)	0.10508	0.06211

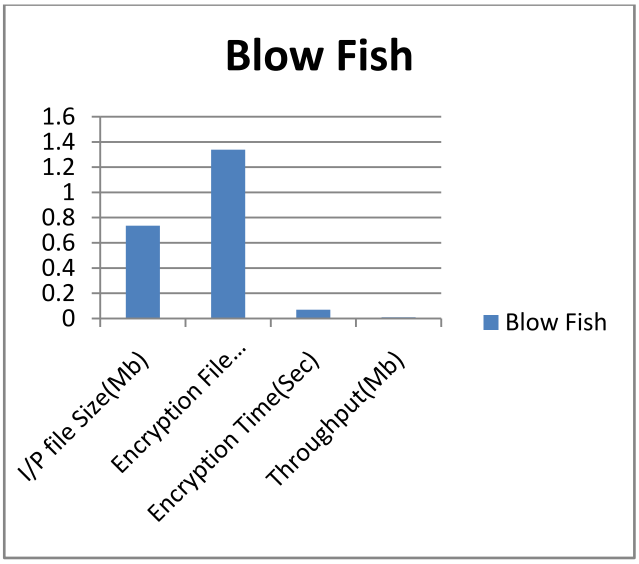

Figure 1.4 Graph of Blow Fish With all parameters.

It shows the graph of input file size, encrypted file size, encryption time and throughput of the blow fish algorithm in the graphical form.

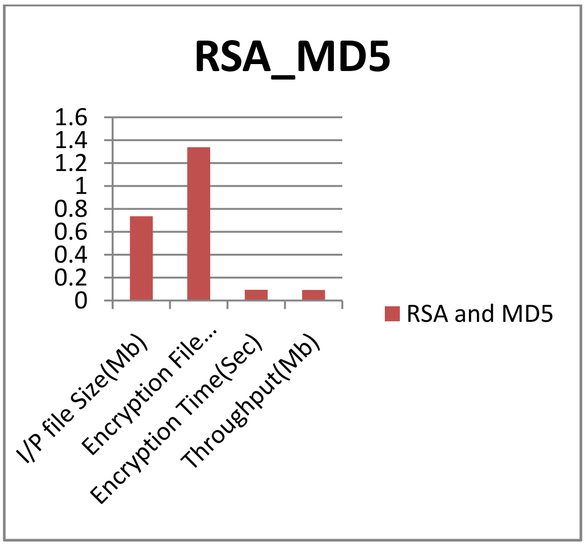

Figure 1.5 Graph of RSA_MD5 with all parameters.

Figure 1.5 shows the graph of the input file size, encrypted file size, encryption time and throughput of the RSA_MD5 algorithm in the graphical form.

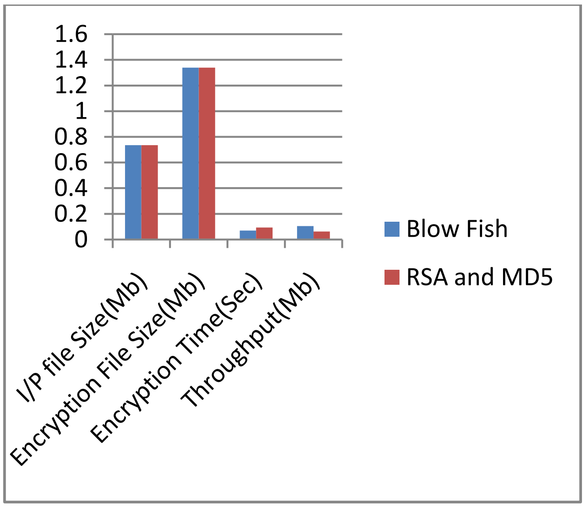

Figure 1.6 Comparative graph of Blow Fish and RSA_MD5

Figure 1.6 shows the comparison graph or blow fish and MD5. The encryption time in blow fish is less than the existing method and throughput is higher than the RSA_MD5.

5. CONCLUSION

I this paper improve the storage and time capacity by slicing of data in different parts with security constraint the combination of the encryption algorithm RSA and MD5 hashing algorithm. RSA encrypt file before uploading on the clod and after that MD5 starts its working [3, 4]. The author proposed a method which is based on ID in encryption process. Diffie Hell Man method is used with Elliptical curve method for providing the security to the data over cloud

6. REFERENCES

[1] Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences 387 (2017): 103-115.

[2] Xia, Zhihua, et al. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE Transactions on Information Forensics and Security11.11 (2016): 2594-2608.

[3] Khari, Manju, and Manoj Kumar. "Secure data transference architecture for cloud computing using cryptography algorithms." Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on. IEEE, 2016.

[4] Priyanka Ora and Dr.P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer 2015.

[5] Shakeeba S. Khan , Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, Vol. 3, Issue 1, January 2015

[6] Prof Swarnalata Bollavarapu, Bharat Gupta, 'Data Security in Cloud Computing', Volume 4, Issue 3, March 2014

[7] NesrineKaaniche,AymenBoudguiga, Maryline Laurent, "ID Based Cryptography for Secure Cloud Data Storage,"Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference

[8] NehaTirthani, GanesanR,"Data Security in Cloud Architecture Based on diffie Hellman and Elliptical Curve Cryptography," International Association for Cryptologic Research, Nov 2013.

[9] Mishra, Ankur, et al. "Cloud computing security." International Journal on Recent and Innovation Trends in Computing and Communication 1.1 (2013): 36-39.

[10] Rewagad, Prashant, and Yogita Pawar. "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013

[11] DeyanChen,Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing, " 2012 IEEE International Conference on Computer and Electronics engineering.

[12] Yu, Shucheng, Wnjing Lou, and Kui Ren. "Data security in cloud computing." Morgan Kaufmann/Elsevier, Book section 15 (2012): 389-410.

[13] Asma, Anjum, Mousmi Ajay Chaurasia, and Hala Mokhtar. "Cloud Computing Security Issues." International Journal of Application or Innovation in Engineering & Management 1.2 (2012): 141-147.

[14] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28.3 (2012): 583-592.

[15] Sudha, M., and M. Monica. "Enhanced security framework to ensure data security in cloud computing using cryptography." Advances in Computer Science and its Applications 1.1 (2012): 32-37.