International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.019

Improvement of Cloud Security Efficiency by Reducing Data Size and Computational Time Using ECDH, AES, BlowFish & PSO Algorithm

Rakesh Dogra
Department of Computer Science and Engineering
Deshbhagat University, Mandi Gobindgarh, Punjab, India

Anupam Sharma
Assistant Professor, Department of Computer Science and Engineering
Deshbhagat University, Mandi Gobindgarh, Punjab, India

Abstract- Cloud security is an important area of research as the number of individuals and companies storing data remotely in the cloud is exponentially increasing. This research tries to improve the security efficiency of cloud storage through the reduction of computation time and encrypted data size through the use of Elliptical Curve Diffie Hellman and Blowfish algorithms. Particle Swarm Optimization might be applied during the actual experiments. Experimental results will be evaluated to compare and contrast the results with the same experiment using RSA algorithm to find out the relative improvement in performance.

Keywords – Cloud Security, Blowfish, ECDH, Data Slicing

I. INTRODUCTION

Cloud computing is recognized as on-demand computing, which is considered as internet-based computing in which the user shares processing resources and computers data and other devices on interest [1]. It provides the ability to users and enterprises for storing and processing information in third party data centers through the use of dynamically flexible services and on interest, hardware and software virtualization over the internet [2]. Despite thits rising popularity, many times due to lack of direct control on external data, users are averse to accepting cloud services [3]. In a cloud, provider shared platform by various users having probability that information belonging to distinct clients resides on similar data server [4]. There have been many attempts to overcome the various security and privacy issues in cloud computing and studies about current issues and problems.

Ahmed & Hossain [5] observed that security is one of the prime factors and unless individuals and organizations are assured that their data is confidential and safe, it will act as a bottleneck for full scale adoption of such services. Barron et al [6] studied several real world cases which involved security breaches in the cloud computing services. Several attacks on big cloud provider services were studied including cases of wrapping signature attack, SYN flooding, social engineering and so forth. The trend of slicing the data before storing it on the cloud has also been popular recently. Li et al [7] suggested a new approach whereby the data is stored in a distributed fashion in the cloud. Normally even if no outsider has access to the data, the cloud service provider has the data within their reach. This can be a cause for concern in case of very sensitive data and tends to decrease the inclination to use cloud services. [8] Manjula et al [8] proposed a methodology to improve security of cloud data by dividing the data into smaller parts, and storing those parts in different servers. This way if any hacker or the cloud service provider wants to read the data, they will only have a partial view which would be encrypted as well. So the data will not make any sense and there would be an absence of the knowledge of the context of the data, hence it is much safer than simply encrypting the data and storing at one place.

Many authors suggested an approach of using a mixture of different algorithms to improve cloud security and negate the shortcomings of each individual algorithm by following this hybrid approach. Mamatha & Kanchan [9] proposed a method of hybrid encryption which uses a combination of AES and DES algorithms to encrypt data. This renders the data less vulnerable to attacks by increasing the cryptography security. The additional use of Diffie-Hellman key exchange. Kamboj & Bansal [10] propose a three step mechanism which helps to improve cloud data storage security. The three steps consist of RSA, MD5 and AES. RSA homomorphic encryption was used at the client end to encrypt data before transmission to the cloud, while MD5 hashing along with AES was used at the cloud server side.

Patil & Kulkarni [11] developed a new algorithm for data encryption which was a combination of the popular asymmetric encryption algorithms namely RSA and El-gamal. Chintawar et al [12] have proposed that the use of elliptical curve cryptography instead of the conventional techniques is the future of encryption especially in cases of cloud computing. This is due to the fact that the overhead in case of techniques like ECC is much less than those in the current algorithms in use, such as the RSA.

Hong et al [13] proposed the use of elliptic curve cryptography by using it for homorphic encryption of data to be stored on a cloud server. The GPS data in China related to sensitive seismic information was used to demonstrate that this scheme works better than the RSA and Paillier method which has been traditionally used for such encryption. This increase of performance is achieved by reducing the computation cost and communication time with the help of the proposed algorithm.

II. Proposed Algorithms

A. ECDH Algorithm

Taking further the experiments done previously as described in the introductory section above, the authors propose a combination of Elliptic Curve Diffie Hellman (ECDH), Blowfish (BF) and Particle Swarm Optimization (PSO) algorithms to try and improve the cloud security efficiency in terms of reduced computational time and reduced data size.

ECDH is a key generation mechanism which generates keys used for encryption and decryption. The actual encryption is then carried out using another algorithm, Blowfish in this case, to encrypt the data.

The mechanism of key generation is shown below. Let there be two persons Alice and Bob who want to communicate secretly over a public channel which Eve the hacker wants to listen.

- First of all Alice and Bob agree upon a common generator point on an elliptic curve, which is denoted by G
- Both of them choose their own private keys P_A and P_B which they keep to themselves.
- They generate their public keys H_A and H_B using their private keys and the common Generator Point G as follows

$$H_A = P_A G \text{ and}$$

$$H_B = P_B G$$

- They both exchange their public keys over the unsecured medium and then use it to generate a common shared key using the formula

$$S_A = P_A H_B = P_A P_B G \text{ and}$$

$$S_B = P_B H_A = P_A P_B G$$

Hence it can be seen that now both Alice and Bob have same secret key without actually exchanging it over the unsecured medium. Eve cannot decipher this key despite knowing the shared Generator point and the public keys because it is not possible to reverse the process which is known as the discrete logarithmic problem.

A Flowchart of this process is shown below.

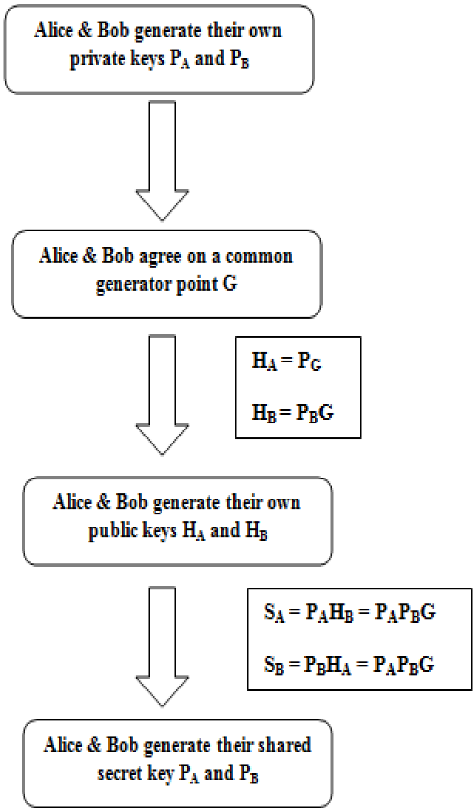
Alice & Bob generate their own private keys P_A and P_B
Alice & Bob agree on a common generator point G
$H_A = P_G$
$H_B = P_BG$
Alice & Bob generate their own public keys H_A and H_B
$S_A = P_AH_B = P_AP_BG$
$S_B = P_BH_A = P_AP_BG$
Alice & Bob generate their shared secret key P_A and P_B

Figure 1. Key Generation using ECDH

B. BlowFish & AES Algorithm

After generation of the key securely using ECDH, the next step is to encrypt the data using Blowfish Algorithm. It is a symmetric block cipher algorithm where the block size is 64 bits or 8 bytes, while the key size varies from 4 to 56 bytes. The algorithm works in 16 rounds as explained in figure 2 below. The journey from a plaintext block to cipher text block goes through 16 rounds involving block splitting into two equal parts, XOR operation and swapping.

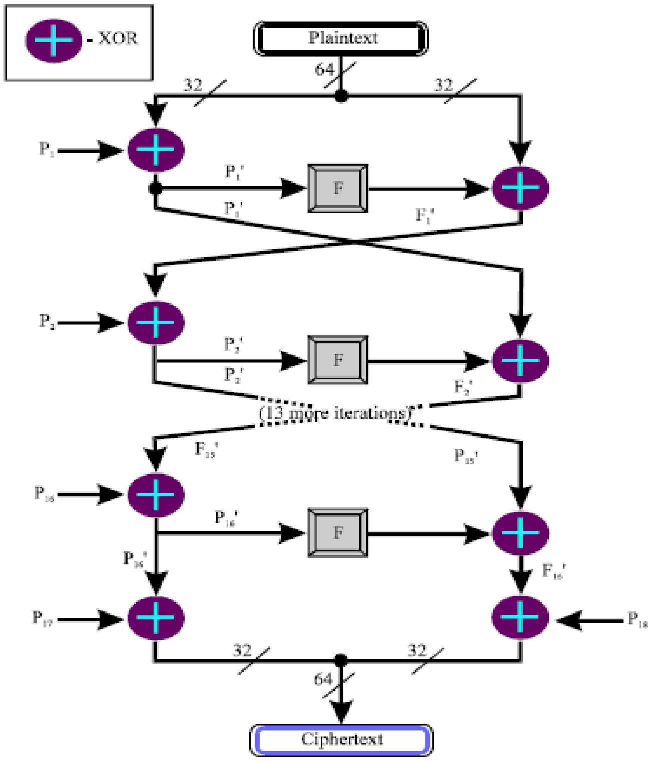

Figure 2. Blowfish Algorithm [14]

The second algorithm in this case is the AES which is the popular advanced encryption standard and used to encrypt the data along with Blowfish algorithm.

C. Particle Swarm Optimization Algorithm

Particle swarm optimization is an algorithm based on the behavior of groups of birds or fish and is a meta heuristic approach towards problem solving. Such an approach is used when the solution is complex and there is only a probability of the solution being found and no surety.

The main technique consists of considering all the possible solutions as particles which have to be optimized for the best possible solution. The algorithm proceeds in steps known as generations and at the end of each generation each particle is updated using two parameters, namely the best location of the particle and the best location of the entire group. The equations governing the PSO algorithm are given as follows [15]

Eqn 1. v[] = v[] + c1 * rand() * (pbest[] - present[]) + c2 * rand() * (gbest[] - present[])

present[] = persent[] + v[] (b)

where

- v[] is particle velocity
- present[] is current particle
- gbest is global best
- pbest is particle best

III. Experiment and Results

The researcher proposes the following experimental methodology to perform the experiment involving the algorithms mentioned above following these steps

1. Input the text file by bench mark data set

2. Generate the key using ECDH
3. Encrypt with AES
4. Encrypt with Blowfish
5. Optimize using PSO simultaneously
6. Upload data to cloud
7. Retrieve from the cloud using previously generated key
8. Calculate time and storage
9. Compare with RSA to measure improvement

The tools used for the experimentation would include the following

Java Language: Java is a platform independent high level programming language which gets converted to bytecode that can be used on any architecture having the relevant Java Virtual Machine or JVM. It is one of the most popular languages used in the industry today and another reason for choosing Java is that the other tool used for this project, namely CloudSim is entire based on Java and hence both have a good compatibility

CloudSim: It is a simulation developed by CLOUDS Laboratory at University of Melbourne, Australia and is currently one of the most popular platforms to simulate cloud environment for study and academic purposes. It is a freely downloadable framework which can be used by anyone and hence is being widely used to simulate cloud environments, virtualization, data centers and so forth.

IV.CONCLUSION

The experimental results will compare with the results from a similar process using RSA algorithm as used in the base paper [13] to compare and contrast the values of computational time and data size. The results would prove whether it is beneficial to use the combination of these algorithms for improving cloud security. It must be noted that the decision to use the PSO algorithm would be taken by the authors at the time of actual experimentation. The expected outcomes for this study include

- Less storage capacity: it is expected that the storage space required by the encrypted data using this algorithm is smaller as compared to the previous work
- Less computation time: it is expected that the computation time of encryption and decryption is less than the previous work

The expected results are relevant to the field of cloud storage and security since cloud computing is becoming popular for storing data. Given the huge amounts of data which is being stored, even a slight decrease in the time and storage requirements could be beneficial for cloud service providers as well as the clients who avail the storage facility.

REFERENCES

[1] N. Kaaniche, A., Boudguiga, A., M. Laurent, “ID based cryptography for secure cloud data storage”, *in CLOUD 2013: IEEE 6th International Conference on Cloud Computing*, pp. 375-382, 2013.

[2] Kaur, “Cloud Computing and Security Issues: A Survey”, *International Journal of Computer Science Trends and Technology*, vol. 3, no. 2, pp. 168-171, 2015.

[3] M.A. Nadeem, “Cloud Computing: Security Issues and Challenges”, *Journal of Wireless Communications*, vol. 1, no. 1, pp. 10-15, 2016.

[4] Chen, H. Zhao, “Data security and privacy protection issues in cloud computing”, In *2012 International Conference on Computer Science and Electronics Engineering,* vol. 1, pp. 647-651, 2012.

[5] M. Ahmed, A. Hossain, “Cloud computing and security issues in the Cloud”, *International Journal of Network Security & Its Applications*, vol. 6, no. 1, pp. 25-36, 2014.

[6] Barron, H. Yu, J. Zhan, “Cloud Computing Security Case Studies and Research”, *Proceedings of the World Congress on Engineering*, vol. 2, no. 1. pp. 1-5, 2013.

[7] Y. Li, K. Gai, L. Qiu, M. Qiu, H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing”, *Information Sciences*, vol. 8, no. 5, pp. 1-13, 2016.

[8] S. Manjula, M.I. Devi, R. Swathiya, 2016, “Division of data in cloud environment for secure data storage”, *2016 IEEE International Conference on Computing Technologies and Intelligent Data Engineering*, pp. 265-269.

[9] M. Mamatha, P. Kanchan, “Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing”, *International Journal of Scientific and Research Publication*, vol. 5, no. 6, pp. 1-4, 2015.

[10] P. Kamboj, L. Bansal, “A Review Paper on 3 Step Mechanism Using RSA, AES and MD5 to Improve the Security in Cloud Environment”, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 7, pp. 389-392, 2016.

[11] R. Patil, V. Kulkarni, “Hybrid Cryptosystem Approach for secure communication”, *IOSR Journal of Computer Engineering*, vol. 17, no. 1, pp. 21-24, 2016.

[12] N.N. Chintawar, S.J. Gajare, S.V. Fatak, S.S. Shinde, G. Virkar, “Enhancing Cloud Data Security Using Elliptical Curve Cryptography”, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 5, no. 3, pp. 94-97, 2016

[13] M.Q. Hong, P.Y. Wang, W.B. Zhao, “Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing”, In *2016 IEEE 2nd International Conference on Big Data Security on Cloud*, pp. 152-157, 2016.

[14] Sakshat Virtual Labs 2017, “Blowfish Encryption Algorithm”, Retrieved from http://iitd.vlab.co.in/?sub=66&brch=184&sim=1147&cnt=1

[15] Z. Zhang, B. Gu, “Intrusion Detection Network Based on Fuzzy C-Means and Particle Swarm Optimization” *Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation*. Vol. 2, npp. 111-119, 2016.