Turkish Journal of Computer and Mathematics Education Vol.12 No. 1S (2021), 459- 464

Research Article

Optimize Cryptography Algorithm for Efficient Data Security on Cloud Computing

Dr.M.Buvana, Dr.K.Muthumayil[2], Dr.M.Rajinikannan[3]& Dr.Jayasankar[4]

[1]Associate professor, Dept of CSE, PSNACET

[2]Professor, Dept.of IT, PSNACET

[3]Professor, Dept.of Computer Applications, PSNACET

[4]Asst prof, Dept of ECE, University College of Engineering, BIT Campus, Trichy

Email: [1]buvana@psnacet.edu.in,[2]muthumayil@psnacet.edu.in, [3]rajinikannan@psnacet.edu.in

[4]jayasankar27681@gmail.com

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Services in the cloud environment are distributed between all servers and users. Cloud providers have problems with file protection as security is a major problem when processing and transferring information, as the original data type can be viewed, misused and lost. In the cloud computing world, cloud protection is a major concern. A variety of research projects are planned to safeguard the cloud climate. Cryptography is used to address the security problem and to achieve the CIA (confidentiality, honesty and disponibility). The most effective technique for ensuring high data transfer and storage protection is cryptography. There are certain drawbacks in traditional symmetric and asymmetrics. We will introduce a new technique of hybrid data protection and confidentiality to solve this issue. We use the ECC and Blowfish to build a hybrid algorithm in this article. The hybrid scheme output is compared to the current hybrid technique and demonstrates the high safety and confidentiality of the patient data in the proposed method. The hybrid encryption is used to remove both symmetrical and asymmetrical drawbacks.

Keywords: Blowfish, Elliptic curve, cryptography, Cloud environment, CIA property, Data Security,

1. Introduction

Cryphotography, i.e. correspondence, overcome the involvement or control of the opponents or third parties, e.g. avoid information leakage to unauthorized parties, is the method of constructing and analyzing protocols for safe exchanging of information[1]. As far as information security is concerned, it covers a range of areas, e.g. data integrity, validation and privacy. Cript algorithms are built around assumptions of computational hardness, e.g. with numerological definition, which makes it impossible for an unauthorized party to crack such algorithms in practice. These algorithms/schemes are called computer-proof, since in principle, while they are breakable, they cannot be broken by known functional means. In theoretical developments, such as the integer factorization Algorithms and earlier computing knowledge[2], these algorithms/schemes were to be continually developed.

Many of the previously submitted cryptosystems are public key numerical cryptosystems requiring a significant amount of computer power and often involve a very time-consuming, complex method for secret channel generation. Several other principles and approaches have investigated these limitations. Among them, the idea could be used to build a hidden key for neural networks and several could provide a potential solution for a critical problem from the key exchange[3].

More widely, encryption is concerned with developing and evaluating protocols that prohibit third parties or the public from reading private messages. The algorithms used for that method are called cryptographic algorithms or ciphers, which can be classified into the two basic kinds based on the keys used as a symmetric key and asymmetrical key algorithm (altering data from readable type to safe shape). The most ancient and encryption approach used for encrypting and decrypting data is symmetric encryption (DES, RC2, RC4, Blowfish, RC5 RC6 or AES). Sender and recipient share the key, which is a big problem, as an attacker can scan the important conversation channel to decrypt the data[4]. You need a safe channel between the sender and the recipient to transform the secret key. In contrast, asymmetric encryption, public and private, for plain text ciphering. Any public body can send a message with a public key, but it keeps a private key secret and can decode the message [5].

1. 2 Literature Survey

Kamara and Lauter[6] have put forward a public cloud protection model that uses primitives for data integrity verification. The advantages of the cloud storage such as reliability, availability, efficient recovery and data sharing were addressed in this paper, combining the latest and non primitives for safe cloud storage. In [7], there has been introduced a hybrid encryption scheme using both RSA and Blowfish. In that they have used the Field

Programmable Gate Array with a mathematical methodology (FPGA). Due to its low cost and high degree of security, this strategy is very effective. However, the main problem is the key size (448 bits).
In order to secure cloud file storage, Maitri and Verma [8] proposed to use the hybrid cryptographic techniques. Steganography with LSB was used, by which the encryption key for key information integrity is protected in an image header. An revolutionary hybrid cryptography technique for health records was built in [9]. This helps them to improve patient data protection and avoid false needs by using Blowfish and improved RSA algorithms. Wang et al., [10] implemented a new system for encrypting information and for sending encrypted data to another consumer. The private key is used for decryption. To look for encrypted data using symmetric and asymmetric searchable encryption. Wang et al. have designed and consumer should have previous knowledge of encrypted data using security encryption techniques. In [11], he introduced a lightweight data hybrid (AES-RSA) technology. It cannot however be extended to multimedia data because it offers protection only for lightweight data.
The use of both the symmetric and Asymmetric-key (RSA), to provide strong protection, was suggested by Karthiket al., [12]. The effect of this method was better safety. The time needed for data collection is also earlier than the previous process. In the XaaS architecture, Rahmani et al. [13] have projected a new cloud service system. Cloud Encryption as a Service was suggested by the authors, which reduces the security risk of encryption for service providers and strengthen customer safety.

2. 3 Privacy and Security Requirements of Data Sharing in the Cloud

Data shared in the cloud worth noting in this context are privacy and security criteria. The fulfillment of these cloud infrastructure criteria will lead to a large number of users taking cloud technology into account and accepting it.
Data privacy: Unauthorized users can not access data at any time. Data confidentiality: In transportation, rest and backup media, the data should remain confidential. Links to data should be granted only to approved users.
User cancelation: If the access rights to data are removed from the user, the user should not at any time be entitled to access the data. The revocation of users should ideally not influence the performance of other approved community users.
Scalable and efficient: Because the numbers of cloud users are very high and at times volatile as the users come and go, reliability and scalability need to be managed.
Entities collusion: When it comes to cloud data sharing methodologies, it is essential that they cannot access any data without permission from their data owner, even though certain entities collude.

3. 4 Proposed Method

Hybrid encryption blends public key encryption and symmetrical key encoding. Hybrid algorithms are elliptical (public key) and Blowfish algorithms. Elliptical curve encryption (symmetric key cryptography). Cryptography of the elliptical curve (public encryption key) based on Elliptically curved theory to create more rapid, smaller and more accurate cryptographic keys. A elliptical curve has an advantage of smaller chip sizes, less fuel, speed increases, etc. Blowfish is a free, accessible and efficient symmetric encryption algorithm used in a number of items, such as secure email encryptions, backup software, or password against hackers and cyber-crimen. Based on the limited sum of rounds, Blowfish is a very effective and relatively easy block-chipher (encryption tool). In this section we describe the fundamental functions of cryptography algorithms in Elliptic curve and Blowfish.

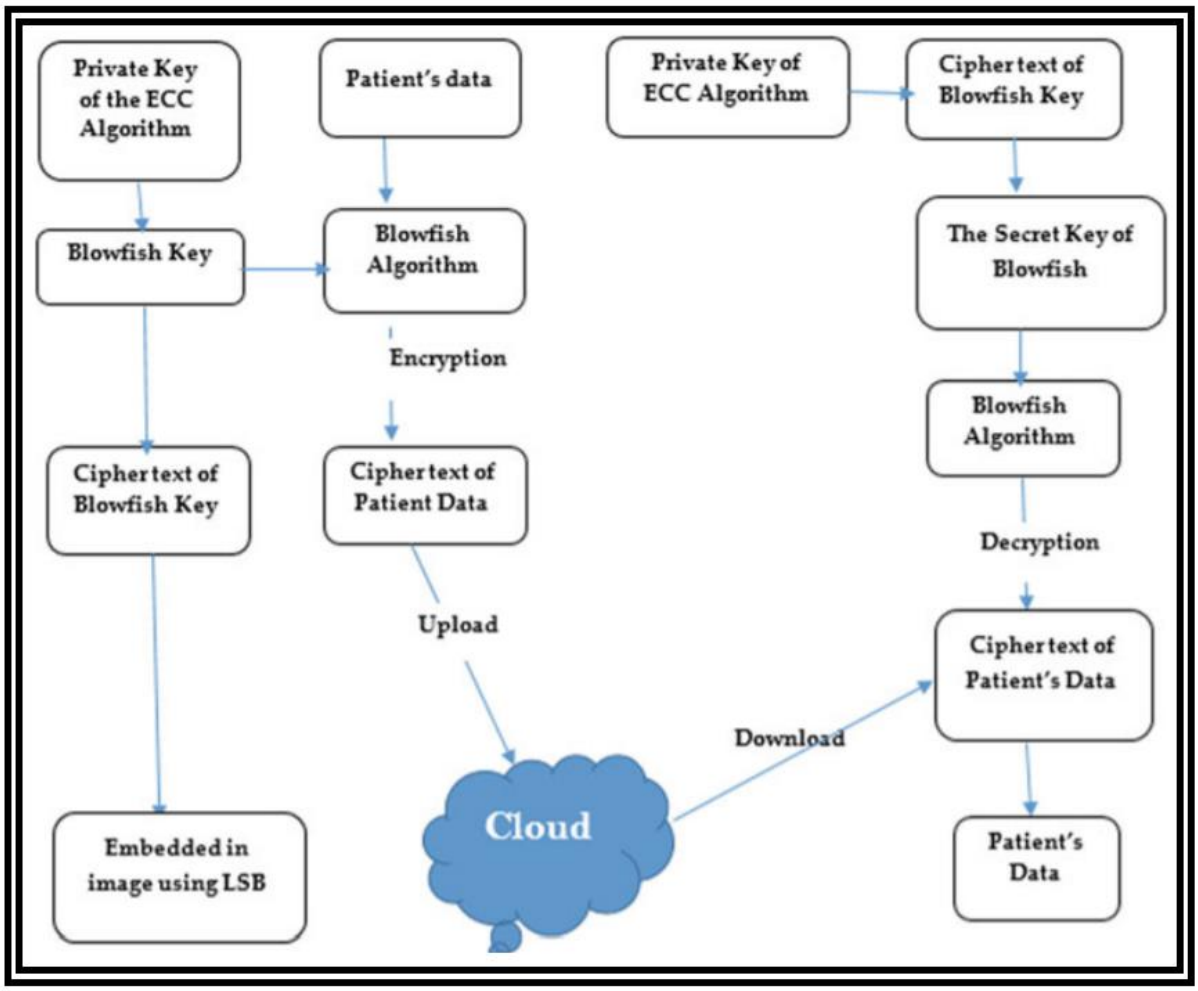

Figure 1: The cryptography architecture

4.1 Elliptic Curve Cryptographic Algorithm

The elliptic curve encryption (ECC) for smaller key size, large speed and low memory consumption has selected public key-related systems, digital encoding, bitcoin services and others to instantiate. The established reputations of the ECC are focused on its discreet logarithm algorithmic problem (DLP). The elliptic curve in the FP prime finite region is about the point cloud defined in the following equation

$$y2 = x3 + ax + b \bmod p \quad (1)$$

4.2 Blowfish Algorithm

Blowfish is a Fiesta network symmetrical block chip which is composed of 16 rounds of functional decryption and iterative encoding. The block size used is 64 bit and the dimension of the key will vary from 448 to 448. Cipher Blowfish uses 18 sub-arrays of 32 bit generally known as P-boxes, and 4 extra boxes of 32 bit with 256 entries, respectively.

There are two phases: The first extension is the key and the other encryption is data. Key in the key expansion process is transformed into several sub keys and encryption occurs in the 16-round network data encryption step. Each round involves an essential permutation and a main- and data-based substitution.

4. 5 System Model

The cloud is the primary storage medium for the encryption of patient data using the Blowfish algorithm and the encryption of the key using the Elliptic curve public key. The chip text and the Blowfish key are stored in the cloud of all patient data. The elliptic curve cryptography private key is used for decrypting the Blowfish key and the decrypted Blowfish key is obtained. The Blowfish algorithm uses the Blowfish decrypted key to decrypt patient information. Here, the patient data for store and collection of the cloud data using hybrid algorithms are taken into account. The process is described below and explained,

5.1 Upload Process

If it's a script or plain text, the client may specify the route or data to be encrypted directly. A symmetric key is automatically created based on the key size called a key. Claintext P can be encoded with blowfish to obtain text in cipher C. By the Elliptic Curve method of encrypting the secret key of Blowfish is authentic and the key is secured The key is encrypted.

5.2 Download Function

Ciphertext C is obtained by the user from the cloud. Ciphertext key decryption is used using the elliptic cryptography algorithm. In order to receive plaintext P, the Blowfish procedure decrypts transferred cipher text information C. Deployment The operating system used is Windows 10 at the front end to execute the proposed process, since the system is free and platform-independent. For the purpose of storage the most widely used database is SQLite Data security efficiency Hybrid cryptographic change and key and data replacement.

5. 6 Result and Analysis

In this diagram, the parameters taken into consideration are time to compare the efficiency of the hybrid algorithm (elliptic curve and blowfish) (seconds).

Table 1: The encryption time analysis

Data	Blowfish	AES	DES	Proposed scheme
1	4.99	4.00	3.99	1.50
5	4.11	4.29	3.01	1.30
7	4.98	4.01	4.01	1.42
10	5.01	4.87	4.39	2.55

The efficacy of the elliptical curve (Elliptical curve and Blowfish) is shown in Figure 2 and Table 1 to compare parameters taken into account are time (seconds) along the x-axis and data (record) (MB) over the y-axis and time is compared.

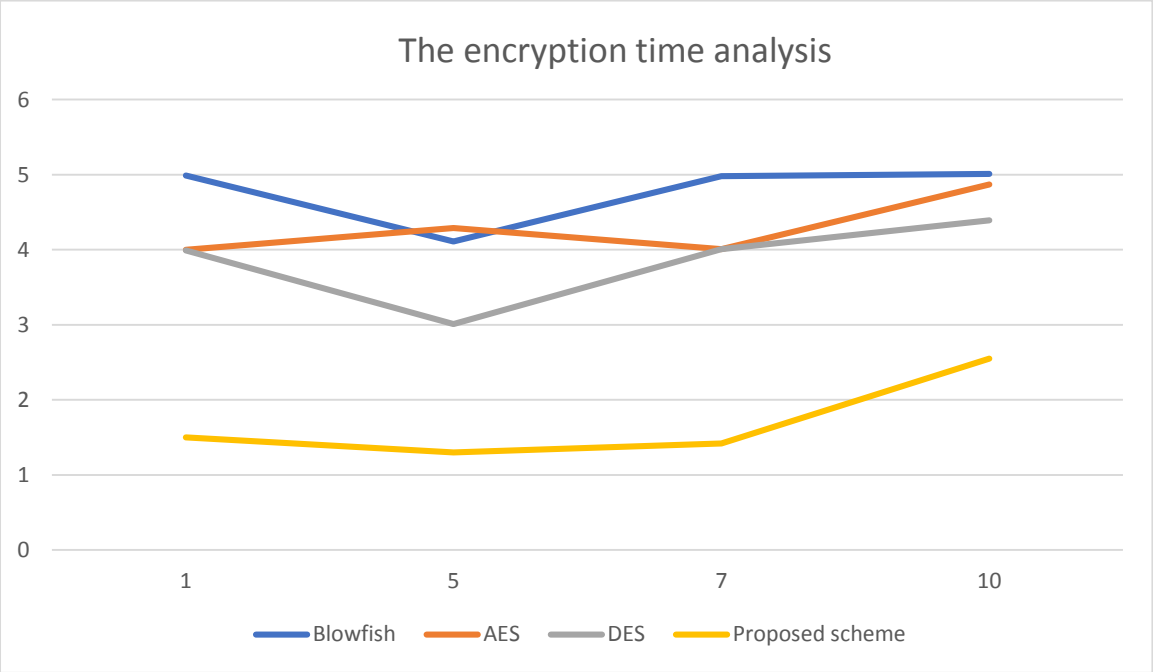

Figure 2: Graphical representation of encryption time analysis

In the Figure 3 and Table 2 shows that the algorithm (Blowfish, DES and AES) is compared with our hybrid algorithm.

Table 2: The decryption time analysis

Data	Blowfish	AES	DES	Proposed scheme
1	4.79	4.55	3.09	1.43
5	4.31	4.29	3.01	1.24
7	4.98	4.91	3.61	1.37
10	5.91	4.87	4.39	2.98

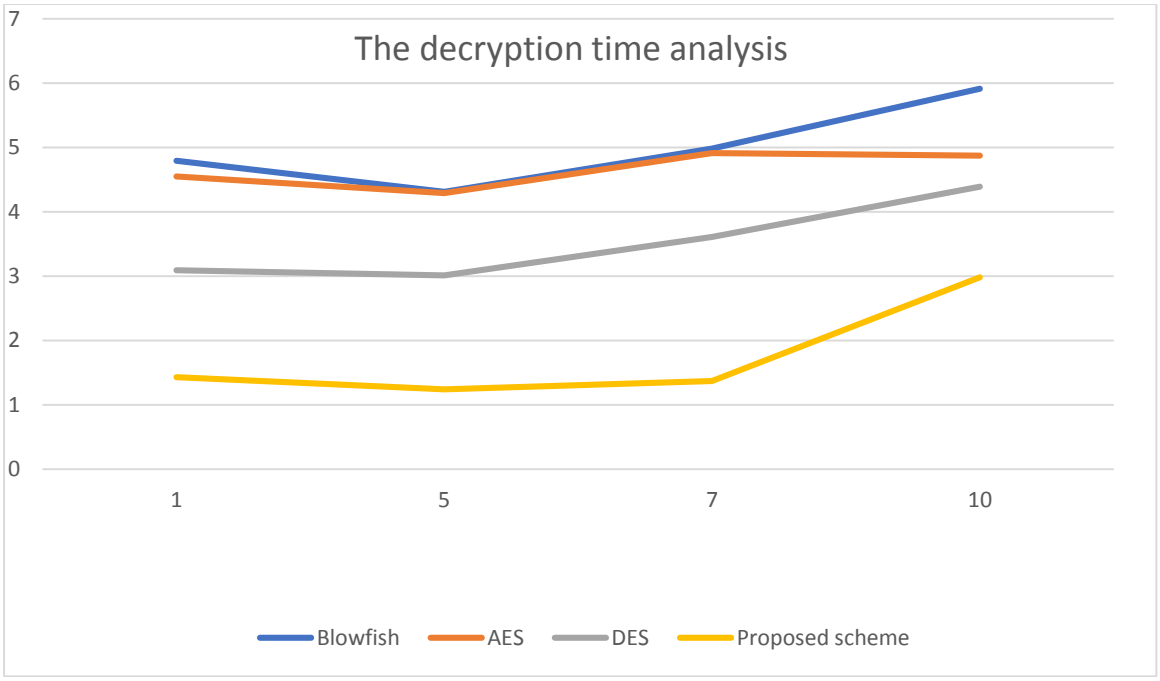

Figure 3: Graphical representation of decryption time analysis

The symmetric key cryptography is used for AES, DES and Blowfish. The key advantage of symmetric algorithms is faster performance and compact for large volumes of data. The above chart shows that our hybrid procedure is effective associated to other procedures.

6. 7 Conclusion

The proposed cryptography approach solves the protected data storage problem. The cloud's disadvantages are lack of safety and privacy. This proposed classical is developed and applied in Java, with the best symmetrical key (Blowfish) and asymmetric key techniques (ECC). For key generation, encryption and decryption processes the Blowfish and ECC algorithms are used. In order to achieve an improved degree of cloud computing security, elliptical curve cryptography (ECC) is used. ECC offers a stronger and more reliable model for the creation and implementation of a secure cloud application. We may use steganography to hide keys to resolve the key distribution. In future we can use the steganography approach to solve the main distribution and compare it with the hybrid method already in use.

References

1. Y. Cheng, X. Cao, D.M. Shila , W. Shen, B. Yin and W. Hong, ‘‘Secure key establishment for device-to-device communications”, IEEE Global Communications Conference (GLOBECOM 2014), pp. 336-340, 2014.
2. A. Nagar, K. Nandakumar and A. K. Jain, ‘‘Multibiometric cryptosystems based on feature-level fusion”, IEEE Trans. Inf. Forensics Security, volume: 7, number: 1, pp. 255-268, February, 2012
3. T.Jayasankar, R.M.Bhavadharini, N.R.Nagarajan, G.Mani, S. Ramesh, Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform”, *European Journal of Molecular & Clinical Medicine (2021),*Volume 08, Issue 01, 2021,pp.1075-1089.
4. Al-Shabi MA (2019) A survey on symmetric and asymmetric cryptography algorithms in information security. Int J Sci Res Pub 9(3). http://dx.doi.org/10.29322/IJSRP.9.03.2019.p. 8779
5. M.Anuradha, T.Jayasankar, PrakashN.B[3], Mohamed YacinSikkandar, G.R.Hemalakshmi, C.Bharatiraja,A. Sagai Francis Britto, “IoT enabled Cancer Prediction System to Enhance the Authentication and Security using Cloud Computing,” *Microprocessor and Microsystems (Elsevier 2021),* vol 80, February, (2021) .
6. Kamara S, Lauter K (2010) Cryptographic cloud storage. Lect Notes ComputSci 6054:136–149

7. Bansal VP, Singh S (205) A hybrid data encryption technique using RSA and blowfish for cloud computing on FPGAs. In: 2nd international conference on recent advances in engineering computational sciences (RAECS), Chandigarh, pp 1–5
8. Maitri PV, Verma A (2016) Secure file storage in cloud computing using hybrid cryptography algorithm. In: International conference on wireless communications, signal processing and networking (WiSPNET), Chennai, pp 1635–1638
9. Chinnasamy P, Deepalakshmi P (2018) Design of secure storage for health-care cloud using hybrid cryptography. In: 2nd international conference on inventive communication and computational technologies (ICICCT 2018). IEEE Xplore Compliant-Part number: CFP18BAC-ART; ISBN 978-1-5386-1974-2
10. Wang C, Cao N, Li J, Ren K, Lou W (2010) Secure ranked keyword search over encrypted cloud data. J ACM 43(3):431–473
11. Liang C, Ye N, Malekian R, Wang R (2016) The hybrid encryption algorithm of lightweight data in cloud storage. In: 2nd international symposium on agent, multi-agent systems and robotics (ISAMSR), Bangi, Malaysia, pp 160–166
12. Karthik, Chinnasamy, Deepalakshmi (2017) Hybrid cryptographic technique using OTP:RSA. In: 2017 IEEE international conference on intelligent techniques in control, optimization and signal processing (INCOS), Srivilliputhur, pp 1–4
13. Rahmani H, Sundararajan E, ZulkarnainMd, Ali AMZ (2013) Encryption as a service (EaaS) as a solution for cryptography in cloud. ProcediaTechnol 11:1202–1210.