https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

An Analytical approach for optimal secured data storage on cloud server for online education platform

R. Soundhara Raja Pandian[1]*, Christopher Columbus[2]

[1*]Research Scholar, Department of Computer Science and Engineering,
PSN College of Engineering and Technology, India
[2]Department of Computer Science and Engineering,
PSN College of Engineering and Technology, India

R. Soundhara Raja Pandian[1*], [1*]scholar.soundharrajapandian@gmail.com

Abstract: Cloud computing is becoming increasingly popular in the IT business because of its higher performance, widespread access, cheap cost, and other benefits. It is also a pay-as-you-go approach; hence, anyone can access cloud data from anywhere, and it is employed in education platforms for online classes due to its ease of use. However, many educational institutions hesitate to use the cloud educational platform due to security and privacy issues. Hence in this study, the performance analysis of various cryptographic algorithms such as Elliptic Curve Cryptography (ECC), Advanced encryption standard (AES), Two Fish, Blowfish, Data Encryption Standard (DES), Triple Data Encryption Standard (TDES) and role-based access control (RBAC) was analyzed and compared with each other in a view to ensuring the protection of cloud data storage used for educational purpose in the NPTEL database. Encryption time, decryption time, and retrieval time with different data sizes were used as performance evaluation factors to figure out the best End-To-End Encryption security in a network system. Moreover, an ElGamal SBO with Delta Competitive NN Cryptography has been proposed in which ElGamal Stag beetle optimization performs ElGamal encryption with the generation of an optimized key with low execution time, thereby allowing only authorized users to access the educational data in the cloud and the data transmission has been secured using Delta Competitive NN that minimizes vulnerable attacks while controlling the decryption activity. Results showed that the proposed ElGamal SBO with Delta Competitive NN Cryptography performs better than all other techniques in terms of retrieval time, encryption time, communication cost, computational overhead and decryption time and hence when applied in a security scenario, it can improve the encryption effectiveness.

Keywords: Cloud Computing, Security Issues, Triple Data Encryption Standard, Authentication, Data Storage.

1. Introduction

Computers play an important role in education, business and industry. In a conventional setting, high-end technology is rarely presented in a way that meets the demands of academics [Irgashevich, Dadamuxamedov Alimjon (2020)]. Businesses desire

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

to exchange students who are well-educated and qualified [Al-Malah, et al. (2021)]. In India, the educational standard is not uniform [Sondhara Raja Pandian R and Christopher Columbus C (2020)] in educational systems0. Many prestigious institutions offer outstanding laboratory and computing facilities, including the Indian Institute of Science (IISc), Indian Institute of Technologies (IITs), and the National Institute of Technologies (NITs). They may be contributing to 5% of educational institutions in India. The other 95% of educational institutions do not have equivalent facilities to those above for providing adequate technology-based skills [Mulauzi, et al. (2019)]. E-learning is motivated through which the reach of quality teachers can be extended and make them available to the outside world by using Information and Communication Technology (ICT). Online-based e-learning educational platforms like Massive Online Open Course (MOOC) providers have been pursuing various strategies to popularize them, and each country is slowly trying to integrate them into their curriculum through various policy initiatives.

The National Program on Technology Enhanced Learning (NPTEL) [Soundhara Raja Pandian R, et al. (2011)] is an initiative of India's leading science and technology institutes to provide access to quality higher education in India and worldwide. Using NPTEL, Students may listen to all renowned professors' lessons from top schools via virtual classrooms set up at any time and from any location. Many educational industries move their classes online because of insufficient staff, funds and unexpected natural disasters or some pandemic situations like Covid-19. Now a day's Government of India's educational projects like NPTEL, SWAYAM and the Online Degree Programme by IIT Madras are providing online education platforms for all area students. In recent years they have organized complete course packages by providing certificates by IITs. Students can access online video lectures or stored video lectures, frequent interval assignments during course time and final online examinations for certifications [Pandian, Soundhara Raja R and Kasiapillai Kasiviswanathan S (2011)]. The teaching materials and other related NPTEL/SWAYAM servers are connected on a mirror configuration and need better security encryption techniques for securing NPTEL contents available on CLOUD servers, like question Papers, assignments, quizzes and students' databases from hackers. In this paper, we are discussing the cloud security data process.

The Internet Engineering Task Force (IETF) created the lightweight Constrained Application Protocol (CoAP) [Bhattacharjya, et al. (2020)] because certain computers are unable to connect efficiently owing to a lack of resources. As an Internet of Things (IoT) application layer protocol, CoAP is being viewed as a replacement for Hypertext Transfer Protocol (HTTP) [Alhaidari, Fahd A and Ebtesam Alqahtani J (2020)]. This protocol was designed with low overhead, simplicity and multicast to support restricted devices [Suwannapong, et al. (2019)]. Furthermore, there are numerous limited devices in buildings and automobiles; Internet Protocol version 6 (IPv6) is utilized for IoT deployment because it provides a larger address space, allowing more devices to connect to the internet [Jia, et al. (2019)]. CoAP is a protocol that could connect energy-constrained devices to the internet. Although Internet Protocol (IP) networking delivers new resources and benefits in our daily lives, security is still an issue that must be handled [Khan, et al. (2019)]. Creating a robust security policy has proven to be a difficult and error-prone process [Hirschi, Lucca, and Jean-Yves Marion.]. As a result, when researchers were worried about IoT security, they designed lightweight versions and ported them to restricted applications, resulting in a situation where security falls behind. Despite this, the uniform Constrained Application Protocol (CoAP) fully supports the application's specifications

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

[Biswal, et al. (2019)]. Many studies have been conducted on IoT security methods, which may be vulnerable to various security threats compromising the network's functionalities and services [Chaabouni, et al. (2019)].

According to some statistics, technical data doubles every two years. On the other hand, school and college curricula have not advanced quickly enough, thereby preventing development. Hence, there is a need to deliver high-quality services at a reasonable cost by utilizing cloud infrastructure [Barakabitze, et al. (2019), Farhan, et al. (2019)]. This would go a long way toward addressing the problem of Educational Institution's financial constraints. It has several well-known benefits, including quick cloud management platform upgrades.

On the other hand, security is a big concern in the cloud. In addition, the cloud stores student records, exam questions, response sheets, and student reviews [Widjaja, et al. (2019)]. The data listed above are classified as confidential. These data may be stolen due to cloud protection problems.

From the issues mentioned above, it is clear that efficient, secure authentication is required to solve the problems. So in this study, we have examined different methods for secure authentication in the cloud to resolve the above complications. The contribution of the paper analyses various secure authentication techniques to sort out the above-mentioned issues. Different cryptography techniques are compared and discussed in this paper and the best technique is preferred for this project based on technical metrics of retrieval time, Encryption time and Decryption time

The remainder of this paper is arranged as follows: Section 2 presents an overview of the various cryptographic approaches. Section 3 outlines constructing an enhanced methodology as a Secure Communication approach. Section 4 gives a benchmarking examination of the enhanced methodology. Section 5 finally presents concluding comments.

2. Literature survey

Security is essential for data storage and other data communication process to prevent unwanted access from unknown persons. To overcome the security issues, various cryptography algorithms are developed. In this section, some techniques are discussed, and their corresponding research works are analyzed. The first section described the Elliptic Curve Cryptography.

2.1 Elliptic Curve Cryptography (ECC)

ECC stands for Elliptic Curve Cryptography which is a form of public-key cryptography. In [Kumari, et al. (2019)] ECC based user authentication scheme for communication security was analyzed. Elliptic Curve Cryptography is a public-key cryptography technique based on elliptic curves over finite fields. The Elliptic Curve Discrete Logarithm issue is a well-known NP-Hard problem, and the ECC is based on it. The equation defines an elliptic curve.

$$y^2 + xy = x^3 + ax + b \quad (1)$$

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

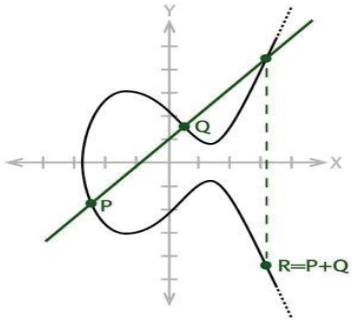


Figure 1: Elliptical curve showing function R=P+Q

The elliptical curve showing function R=P+Q in explained in above figure 1. It consists of three phases. The details of the three phases are given below,

- Set up Phase
- Extraction phase
- Mutual authentication and session key phase

2.1.1 Set up Phase

Here PKG (Public Key Generator) inputs a key parameter. Then the PKG takes the steps such as selecting the arbitrary generator, selecting and setting the public key PK = Mg, and Choosing the collision-free one-way function. Publish the system parameters where M keeps the secret. In this phase, 2 persons were considered; for example, person 1 and person 2 take extraction as follows

Person 1 will submit the identity to the PKG. Then it will check for the validation of the submitted ID. If it gets succeeded, then PKG generates a random number. Then a computational process takes place for the random number. With the help of that random number, PKG will generate the partial private key and deliver it to person 1 via the secure communication channel. On receiving this partial private key person 1 will check for the condition in that key available. Then person 1 sets his/her public key. For person 2 the same procedure repeats as in person 1.

2.1.2. Mutual Authentication and session key phase

In this phase, people 1 and 2 mutually authenticate and establish a session key. Once the key is established, they can communicate over a public communication channel. After that, security analysis was also done under this ECC-based user authentication scheme. The security investigations were done for known key secrecy, known session-specific temporary information Attack, Man in the middle attack, Replay attack, PKG towards secrecy, Passive attack, and key freshness.

ECC has generally based on prime fields or the Galois field's binary extension. It is extremely difficult to break the ECC cryptosystem because it is difficult to identify a relationship between the points P and Q on the Elliptic curve. This research

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

uses ECC for Encryption, key creation, and Decryption. Point P (x, y) selection is critical in building a more secure and dependable encryption method. In [Khan, et al. (2019)] two-tiered methods were used for data security in the cloud. The first step is to divide the data into small bits, and the second is to use random safe curves for Encryption. ECC can help optimize memory space and minimize computational complexity, resulting in lower energy usage for smart devices. The literature works in which ECC technique is utilized is summarized below.

For fog enabled IoT environments, Verma et al [Verma, et al. (2021)] suggested an anonymous mutual authentication technique based on ECC. With the support of a trusted third-party (TTP) centralized authentication protocol, the proposed protocol enables device privacy and mutual authentication between IoT devices and fog nodes. The suggested authentication protocol's security analysis reveals that it is resistant to cryptographic attacks. Milani et al [Milani, et al. (2021)] demonstrated that the devices use elliptic-curve cryptography to safely negotiate fresh keys regularly. The suggested mechanism's security features are tested against a specific attack. According to the analysis, the novel safe rejoin mechanism ensures computational key secrecy, (ii) decisional key secrecy, and (iii) forward and backward key independence for both root keys, thereby addressing the LoRaWAN security vulnerabilities. Rashid et al [Rashid, et al. (2021)] discussed the Point Multiplication (PM) architecture of Elliptic-Curve Cryptography (ECC) over GF (2163) with an emphasis on hardware resource optimization and latency at the same time in their paper. Adopting a bit-serial (traditional schoolbook) multiplication approach reduces hardware resources. Similarly, utilising pipeline registers, latency is minimized by reducing a vital path. For data encryption, Aldabbagh et al [Aldabbagh, et al. (2021)] devised a hybrid optimum elliptic curve cryptography (HOECC) technique that combines public and private keys. The suggested method employs an adaptive tunicate slime-mold (ATS) algorithm to obtain the best key value. As a result, data uploaded to the cloud system is protected by strong authentication, data integrity, and secrecy. Qazi et al [Qazi, et al. (2021)] explored security challenges in WSNs and so subjected node-to-node communication to provide authentication and data encryption in a novel method, with the help of the Elliptic Curve Digital Signature (ECDSA) cryptographic scheme, the proposed scheme not only provides security for the node-to-node communication network, but it also hoards memory space on nodes by providing an appropriate mechanism for measuring key generation time, count of hello messages, and packet size.

Although it has various advantages it also faces some limitations. This technique, while simple and straightforward to use, has a number of downsides, some of which are stated below:

- Both parties must agree on the use of a shared secret key.
- If a user has n communication partners, he or she must save n secret keys, one for each.
- Because the secret key is shared, the authenticity of the origin or receipt cannot be proven.
- Managing the symmetric keys becomes difficult.

As a result, ECC is suggested for smart devices. Until quantum computers become accessible on the market, using ECC in cloud computing is more dependable and efficient. A quantum computer can break the elliptic curve cryptosystem. Hence it created the necessity for the development of other security algorithms.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

2.2. Blowfish Algorithm (BA)

To strengthen the security Blowfish Algorithm has been developed. The data retention and Encryption with the symmetric block cipher technique Blowfish are utilized. This is an open and unpatented algorithm that is available for all users free of charge. The variable-length key is 32 bit to 448 bit and makes it perfect for data prevention. The blowfish (BA) algorithm is used for the encryption procedure. BA is the algorithm for symmetric key Encryption. The key length is 32 to 448 parts of the 64-bit block. P-arrays are completely available here as well as four 32-bit S-boxes. The 8-bit information with 32-bit yield is recognized in the S-boxes. The Encryption of the information requires the 16-round Feistel scheme, each with a key ward mix and a key ward switch. All tasks imply those of the XOR and the 32-bit word enhancements in the blowfish system.

2.2.1. Encryption

Encryption means the assignment of the basic text to the complicated ciphertext. The 64-bit data is utilized for the time-making technique and divided into the left half (LH) and the right half (RH) for the epoch-making technique into 2 32-bit bisects. The XOR work is done by the principal 32-bit remainder of the original matrix and the P- array, and the result is a feature (F). The XOR task is then performed for the other half smoothly, followed by 32% for the right half. This follows the ensuing operation. The rest of the circle is expanded to the 16th round.

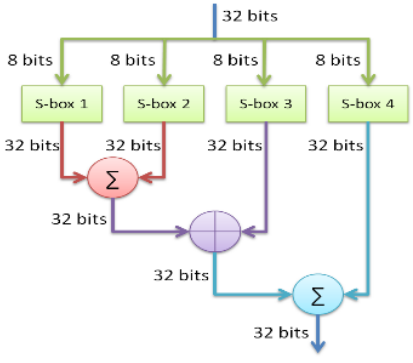


Figure 2: Working procedure of F function.

2.2.2. Process of the F function

The F functions use four 32-bit S-boxes, each with 256 files. In the new blowfish approach, the remaining 32-bit halves are separated into four eight-bit rows comprising m, n, o, and p. Figure 2 depicts the F function's operating principle. The formula for employing the left half's F(LH) feature is described in the following Equation (6). The first two S boxes perform the mod function with mod232 and then XOR with b3 S-box. b4 S-box also performs mod232 and then added to b3 S-box.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

$$F(L_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,o}) + \_ S_{b4,p} \bmod 2^{32} \quad (2)$$

F(LH) is the feature of the left half

b1, b2, b3, b4 are the 4 32-bit S-boxes

2.2.3. Decryption

The Decryption of the blowfish approach is the same as the encryption method, even if the P-array is employed to eliminate it. The productivity of the blowfish approach accumulates the cloud folder, which is used as the second segment's input. The folder goes through the Encryption work and is uploaded to the cloud with the help of the communal and personal keys. The key creation procedure of the blowfish encryption technique generates a safe key that can be used for decoding and encoding. Blowfish is a symmetric block cipher that may be used to securely safeguard data, and it uses the same key for both Decryption and Encryption. The following are some of the advantages of employing the blowfish encryption method: (1) large data blocks may be handled; (2) effective algorithm; (4) scalable key from 32 bits to 256 least bits; and (5) simple operations. It reduces encryption time and increases throughput. Various research works on the technique are discussed as below.

Selvi et al [Selvi M and Ramakrishnan B (2021)] established a trust-based secured broadcasting mechanism that ensures the metrics such as security, privacy, integrity, trust etc. The main goal of this study is to reduce latency and provide highly dependable, secure, and efficient vehicle communication. A separate table holds vehicle position, location, speed, and other traffic information. Various densities are used to form a network. Based on the estimated specific gateway, a path is generated for message broadcasting between source and destination. Gangi reddy et al [Gangireddy, et al. (2021)] created a novel cyber security model that allows optimal key selection. The secret information is clustered using the k-medoid clustering algorithm. It is based on the distance between data points. Blowfish encryption encrypts the data and stores it on the cloud. Improved dragonfly algorithm is utilized to improve accuracy. Muhammed et al [Muhammed, et al. (2020)] suggested a set of techniques to give a high level of security for cloud data, proving the Blowfish Symmetric Algorithm as cryptography and Text Steganography as a cover medium, both of which have shown to be effective. With the help of multi-stage authentication (MSA) and an optimized blowfish algorithm (OBA), Shyla et al [Shyla S and Sujatha SS (2022)] devised an efficient secure data retrieval. MSA, data security, and data retrieval are the three elements that make up the proposed system. Initially, cloud users employ a multi-authentication technique to register their information on the cloud. Following the registration process, the data is encrypted using OBA. The key value is appropriately selected using a binary crow search algorithm to boost the system's security. Dinesh et al [Dinesh E and Ramesh SM (2021)] suggested a secure cloud data transaction using the blowfish algorithm. The proposed approach first checks the user's authentication to increase the system's security. After the authentication process, the uploaded data is initially separated using a pattern-matching algorithm. After that, BA is used to encrypt the separated data. Finally, the data is encrypted and saved in the cloud at the most appropriate location.

In the blowfish algorithm for each user authentication, they are provided with a unique key. So that increase in the user increases the key data, which complicates the key management. However, in the blowfish algorithm, the authentic mechanism

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

has just a few applications, and to overcome the drawback of the Blowfish algorithm, two fish algorithm has been developed. It is explained in the next section of the article.

2.3. Two Fish Algorithm

A twofish algorithm has been developed to use the authentic mechanism in all applications. The Two fish features a symmetrical block cipher Feistel structure. Effective for hardware embedding and programs operating on tiny CPUs. Optimizing encryption speed, key setup, and code size allows users to balance performance. Two fish is available without a license, is unpatented, and can be downloaded for free. Double-fish Encryption is used at 128, 192, and 256 bits. The encryption technique has 16 loops and a block size of 128 bits. The rounding property of two fish is seen in Figure 3.

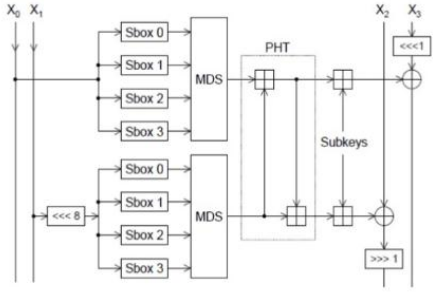


Figure 3: Rounding Function of Two fish algorithm

In this round feature, it encrypts data. This round feature encrypts data 16 times and then displays the final ciphertext after round 16. In the diagram above, On the left-hand side, X0 and X1 function by co-versioning one input to a Maximum Distance Separable (MDS) matrix with 8 bits of one input after the rotation. Four-byte S-boxes plus a linear mixing step consist of the g function. The results are complemented by a Pseudo-Hadamard Transform (PHT) for the two g functions (Pseudo-Hadamard Transform). Two other keywords will be added later. The left-hand result is XORed, with the right-hand result rotating slightly. Right and left have been replaced for the following round. After 16 encryption rounds, the last exchange will return, and the real encrypted text and ciphertext will be created with four more XORized keywords.

The encryption method used in the two fish approach includes 16 loops and a block size of 128 bits. After round 16, this round feature encrypts data 16 times and shows the final ciphertext. The last exchange is reversed after 16 rounds of Encryption, with four extra XORized keywords forming the real encrypted text and the ciphertext. The recent works with two fish algorithms are discussed.

From a public cloud storage perspective, Ramesh et al [Jayasankar TRM, et al. (2021)] deployed the Two fish technique to safeguard IoT health data in health systems. Based on these role-based access controls, the suggested system considerably aided in efficient medical data storage in IoT applications and enabled secure medical data stored in the cloud. A clustering

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

approach is also implemented to shorten the time it takes to retrieve important medical data. Santoso [Santoso KI, et al. (2020)] and colleagues used two cryptographic algorithms, AES (Advanced Encryption Standard) and Two fish, using a 256-bit key obtained via the SHA 256 HASH function. The data uploaded or downloaded in the Cloud system was more secure thanks to this new technique. Pushpa et al [Pushpa B (2020)] proposed a hybrid encryption technique that combined the Blowfish and Two Fish algorithms. The presented model starts with the Encryption of secrecy data and then hides the result by using a cover image and 2D-DWT-1L or 2D-DWT-2L. Color graphics are used as cover images to hide a variety of text sizes. Kareem et al [Kareem, et al. (2020)] presented a new security-enhancing variant of the Two fish method. During the 16 rounds of the typical Feistel Encryption technique, two additional control keys are used. Instead of using only one key for regulating varying bit sizes of the blocks (either 1 or 2, or 4 or 8 bits), the suggested approach uses three keys in the encryption and decryption procedures. Maata et al [Maata, et al. (2020)] showed the Encryption and Decryption of several large datasets and compared the outcomes in terms of message size and processing time. App store, interactions train, border crossing, PP users, PP recipes, raw recipes, and raw interactions are among the seven huge data files loaded in a Java NetBeans two fish algorithm software for simulation reasons.

From the survey, it is clear that the twofish encryption technique is likewise safe; however, it has insufficient encryption speed.

2.4. Advanced Encryption Standard Algorithm (AES)

AES is block encryption with a 128-bit block length. It has three key lengths: 128, 192, and 256 bits. AES with a key length of 512 bits is used in this segment. In Encryption, 10 rounds of encoding are required for the 521-bit key. Except for the final round in each event, the rest of the rounds are the same. The state array is a 4 x 4 matrix of bytes generated by a 512-bit input module. With a 512-bit input volume and a 512-bit address, the new AES-512 algorithm is resistant to encryption inspection with acceptable area increments. AES-512 is ideal for applications that need high protection and efficiency while having a small footprint. The various transition states run on what is known as intermediate results; the state is essentially a rectangular sequence of bytes. Before any round-based encryption encoding, the first four terms in the input level table are XOR. Consider figure 4(a), which shows the original data, and figure 4(b), which shows the main (b).

E0,0	*E0,1*	*E0,2*	*E0,3*
E1,0	*E1,1*	*E1,2*	*E1,3*
E2,0	*E2,1*	*E2,2*	*E2,3*
E3,0	*E3,1*	*E3,2*	*E3,3*

(a)

K0,0	*K0,1*	*K0,2*	*K0,3*
K1,0	*K1,1*	*K1,2*	*K1,3*
K2,0	*K2,1*	*K2,2*	*K2,3*
K3,0	*K3,1*	*K3,2*	*K3,3*

(b)

Figure 4: Sample values (a) input value and (b) key value

2.4.1. Encryption

There are four major rounds in the encryption process: sub bytes, swap rows, mix columns and add round key.

(a) Sub-bytes Operation

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

Sub Bytes is a byte alternative that does not work directly; instead, it works independently on each byte in the state. Reversed toggle table (S-box).

(b) Shift Row Operation

Based on the row code, the Shift Row function rotates each row of the state to the left in rotation, which is illustrated in figure 5.

- 1st row to 0th positions to the left
- 2ndrow to 1st position to the left
- 3rd row to 2nd positions to the left
- 4th row to 3rd positions to the left

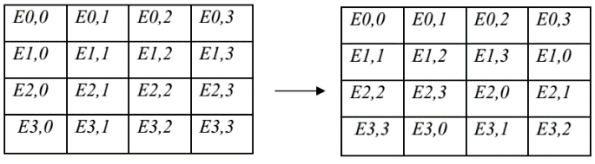


Figure 5: Shift row operation

(c)Mix-Column Operation

The mix-column transformation is performed column by column, with each column being treated as a four-term polynomial. This phase's goal is to ensure that pieces are distributed evenly through several rounds. This is accomplished by multiplying each column separately. In a fixed matrix, each value in the column is multiplied by the value of each row.

(d)Add Round Key

Add the round key and use bitwise XOR to apply it to the condition is explained in the below figure 6. Using the main stand, you will get the round key from the cyber key.

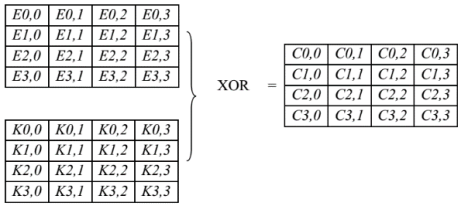


Figure 6: Add round key operation

2.4.2. Decryption

For the decryption process, the reverse encryption function is utilized. The default reverse circuit contains the following

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

functions in this sequence: Inv Mix column, shift arrays, and Inv-sub-bytes add circular key. The encrypted data is encrypted from this procedure.

With a 512-bit input volume and a 512-bit address, the new AES-512 algorithm is resistant to encryption inspection with acceptable area increments. AES-512 is an excellent choice for applications that require great security and efficiency while maintaining a modest footprint. Sub bytes, swap rows, mix columns, and add round keys are the four primary rounds in the encryption process. The reverse encryption function is used in the decryption process. It enhances picture pixel assortment and multifarious detecting information. The research works which involve the AES technique are discussed below.

Teng et al [Teng, et al. (2020)] devised a modified advanced encryption standard for data security in cloud computing by integrating random disturbance information to increase data security, resulting in improved column mix operation and key choreography in AES [Irgashevich, Dadamuxamedov Alimjon (2020)]. Awan et al [Awan, et al. (2020)] presented a framework with significant aspects such as improved security and data privacy for the owner. The double round key feature changed the 128 AES method to enhance the encryption process' speed to 1000 blocks per second. However, a single round key with 800 blocks per second has been used in the past. Less power usage, better load balancing, and improved network trust and resource management were all part of the suggested algorithm. Wang et al [Wang, et al. (2020)] proposed a new image retrieval approach based on random mapping characteristics and the bag-of-words model, which is a ciphertext image retrieval method. The cloud server generates random templates after encrypting the image with Advanced Encryption Standard and block permutation and then extracts the local features. The visual word is formed by clustering all local features using the k-means algorithm. As the feature vector for each image, the histogram of encrypted visual words is built in this manner. The distance between feature vectors on the cloud server determines image similarity. By recognizing security as a critical problem, Hidayat et al [Hidayat, et al. (2020)] designed an encryption-based system to protect data transit. The authors presented a method for improving system security during data transfer to prevent data theft by unauthorized individuals. The Advanced Encryption Standard (AES) was designed to secure data transmission and storage in cloud computing to prevent an attack by an unauthorized person. Mohammed et al [Mohammed, et al. (2019)] produced numerous degrees of multi-coding levels utilising multiple methods to achieve additional confidentiality using DNA encryption and then adding a higher level of confidentiality by adding Advanced Encryption Standard (AES) and loading it into cloud storage. The proposed strategy was implemented with many analyses using Mat lab software (R2014a).

According to the analyses, the AES algorithm has a convincing level of security, efficiency, complexity, and speed. The issue faced in this AES technology is that the Encryption occurs in several rounds. In every round, they encrypted in the same way. To further increase the security a DES Algorithm has been developed and described in the next section.

2.5. Data Encryption Standard (DES)

Encryption and Decryption are the two steps of the DES algorithm. The DES takes 64-bit plain text and converts it to a 64-bit cipher text during the encryption process. DES takes 64-bit ciphertext and converts it to 64-bit plain text in Decryption. A 56-bit cipher key is used here for Encryption and Decryption. Figure 7 depicts the DES block cipher.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

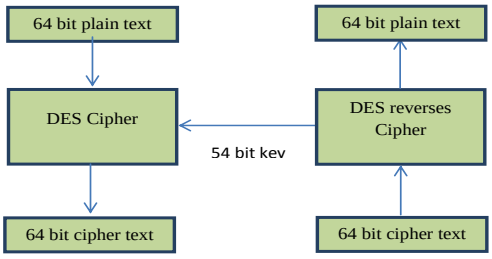


Figure 7: DES block cipher diagram

2.5.1. Encryption process

The encryption mechanism consists of sixteen round circuits and two permutations (B-boxes) with the first and last permutations. A 48-bit circuit key is created from a cyber key for each circuit. Figure 8 depicts the general form of DES.

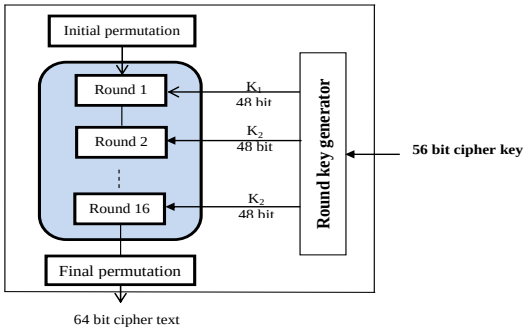


Figure 8: General structure of DES

2.5.2. DES function

DES function is the most important part of the DES algorithm. The DES feature employs a 48-bit key to create a 32-bit output (RI-1). The stages crucial for this debate in the DES algorithm are listed below. A 64-bit plain text module is provided for the Initial Conversion Phase (IP). Two parts of ordered volumes are obtained following permutation, such as Left Flat Text (LFT) and Right Flat Text (RFT). Each LFT and RFT will then be encrypted in 16 rounds. The most important size is 56 bits. Each of these has its key. Then, the 48-bit auxiliary key obtained from the 56-bit key is used for each circuit. Using expansion permutation RFT is then enlarged from 32 to 48 bits. The 48-bit key is Exclusive ORed (XOR) with the RFT, which moves the result to the following level. 32-bits are generated based on S-box replacement from 48-bits. The 32 bits are then allowed with the permutation of the P-Box. The outcome of P-Box is a 32-bit long XOR with LFT. The output sizes are then changed and the pre-output is created for the 32-bit LFT and the 32-bit RFT. The output of the original permutation is extracted in the opposite direction. The ciphertext with 64-bit results from the last permutation. Finally, in this step, secure data are gathered.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

Various researchers used DES algorithm as a part of their work, in which a few are discussed below.
According to Jayasarathi, M., et al [Jayasarathi M, et al. (2019)], the efficiency of cloud storage in the suggested system was achieved by offering flexible data segmentation with an additional authorization process among the three participating parties client, server, and a Third-Party Auditor, (TPA). Because the DES algorithm is an identity-based data storage technique, it can withstand collusion attacks. In their paper, Chen et al [Chen, et al. (2019)] used deep pipeline and full expansion technology to build the AES encryption algorithm on FPGA to increase the encryption speed of massive amounts of data. In their study, Su et al [Su, et al. (2019)] optimized the Advanced Encryption Standard (AES) and developed the data encryption standard DESI (Data Encryption Standard in IoT) for use in the Internet of Things. According to the findings, DESI is more secure and thus suited for encrypting data in the IoT environment. In their work for protecting information of student value data, Ikhwan et al [Ikhwan, et al. (2021)] developed a system that uses a cryptographic algorithm to secure the data. In this case, the method employed is the Data Encryption Standard (DES) algorithm to secure student value data. DES is an asymmetrical cryptographic technique with a 64-bit key size that is also categorized as a cypher block. DES uses a 56-bit internal key to convert plaintext into a cipher text of the same size, 64 bits. Saračević [Saračević, et al. (2020)] developed a new data encryption technology that is ideal for IoT applications. The cryptosystem is based on the use of a Catalan object (as a cryptographic key) to offer Encryption using non-crossing or non-nested combinatorial structures. This article's experimental section compares the suggested encryption method with the Catalan numbers and data encryption standard (DES) algorithm, which is carried out with machine learning-based identification of the encryption method using cipher text only.
Despite the advantages of DES algorithm, there are security issues. To speed up the Encryption, a new method such as Triple Data Encryption Standard has been developed that has been explained in the next section.

2.6. Triple Data Encryption Standard

The Triple Data Encryption Algorithm (TDEA or Triple DEA), often known as Triple DES (3DES or TDES), is a symmetric-key block cipher that applies the DES encryption algorithm to every other data block three times. Triple DES (3DES), a modified variant of DES, employs the same method to provide more secure Encryption. The key size of 56 bits in the original DES encryption was typically sufficient at its inception, but the availability of rising computer power made brute-force assaults possible. Some of the literature related to triple data encryption is mentioned below.
Sadawarti et al [Sadawarti, Kanav (2021)] investigated the security aspects of cloud computing using an encryption technique, and a Cuckoo Search (CS) optimized Feed Forward and Back Propagation Neural Network (FFBPNN). Rivest–Shamir–Adleman (RSA) is used in conjunction with Advanced Encryption Standard (AES) and Triple Data Encryption Standard (TDES) to improve the security of stored data (TDES). Vuppala et al [Vuppala, et al. (2020)] presented the FORTIS algorithm for sub-key generation and investigated its strength against side-channel power attacks using the Chip Whisperer R -Lite and Artix FPGA as target boards. The number of glitches that represent leakage power has been reduced by about 53.3 percent, and the power traces of the key schedule algorithm show that all of the instructions are similar, making it difficult to determine which operation is being performed, and the probability of guessing entropy has been reduced in 86.6 percent of cases. Raheja

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

et al [Raheja, et al. (2021)] developed a one-time padding key and used an encryption method in authentication mode to achieve encryption and authentication. A water cycle optimization technique provides a completely random one-time padding key, and the ECG data is encrypted using the Triple Data Encryption Standard (3DES) algorithm. To strengthen security, Selvarani et al [Selvarani P, et al. (2019)], using the Cross over mutation technique, the feature value of the fingerprint and iris is extracted and fed into a hybrid Genetic Algorithm and Particle Swarm Optimization algorithm to identify the optimal solution.

The best solution value can be used as a key in the Triple Data Encryption Standard Algorithm to encrypt and decrypt data. Finally, utilizing the cloud simulator in the Working Platform of Net Beans in Java, encrypted data can be saved in the cloud. Abdullah and his colleagues [Abdullah, et al. (2019)] devised a method for encrypting and decrypting communications transmitted and received via the SMS service. The 3DES (Triple Data Encryption Standard) algorithm was used to create the software. The 3DES algorithm is a symmetric key encryption method that uses a flow algorithm (block cipher). Without having to create a whole new block cipher algorithm, Triple DES makes it relatively simple to increase the key size of DES to protect against such attacks. Hence TDES has the advantage of proven dependability and a larger key length that avoids many attacks and can be used to minimize the amount of time it takes to complete a task. However, it was vulnerable to man-in-the-middle attacks due to its low file size.

2.7. Role-Based Access Control

Authentication is currently done on two or three layers to provide access to everyone inside the system. Authorization, on the other hand, is permission to use machine tools until the user identity has been verified. Normally, authorization follows authorization on any device that grants the system administrator rights. Role-Based Access Control (RBAC) is a computer system architecture that grants users restricted access depending on privileges once they have completed the required authentication. This paradigm runs on a system that concentrates on user functions and permissions. The below diagram depicts the Role-based Access Control Definition Rules. Figure 9 depicts the basic principles employed in the RBAC model followed by some related studies.

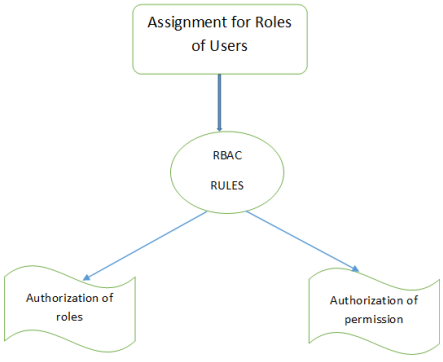


Figure 9: Rules in RBAC model

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

Xu et al [Xu, et al. (2021)] offer an RBAC (RBAC1 model, which is a deeper access control model) strategy for ciphertext in cloud storage using a combined identity-based cryptosystem (IBC) and role-based access control (RBAC) model. Also provide formal definitions for our scheme and a full explanation of four tuples used to describe access control, hybrid Encryption, and write-time re-encryption strategies, all of which are intended to improve system performance. Badsha et al [Badsha, et al. (2020)] used a blockchain-based privacy-preserving cybersecurity information sharing using proxy re-encryption and attribute-based Encryption (BloCyNfo-Share), where the organization can achieve fine-grain access control by delegating which organizations can have access to its cybersecurity information. In a cloud context, Sultan et al [Sultan, et al. (2021)] applied the Role-Based Encryption (RBE) approach. This work makes several contributions. To begin, it introduces a keyword search scheme that allows only authorized users with appropriately assigned responsibilities to delegate keyword-based data search capabilities over encrypted data to cloud providers without revealing any sensitive data. Anilkumar et al [Anilkumar, et al. (2021)] compared Amazon cloud, Microsoft Azure, and OpenStack cloud in a real-world setting. A framework called Predicate Based Access Control (PBAC) is developed to provide fine-grained access control to Swift storage. Predicates that are part of an object are accessible. Su et al [Su, et al. (2019)] created a new cipher text access control strategy (PreBAC) based on proxy re-encryption (PRE) technology. It will be suited for the secure protection of data and information privacy, since the methods offered have shown the security of our scheme.

Even though RBAC's core reference models perform better in terms of authentication and access control, the ordinary ones have few flaws. However, because RBAC reference models allow for several users to fulfill a role, there are no restrictions for restricting the number of users for the same job. Users cannot obtain distinct accesses based on criteria within one role, even when rights are given to functions. Although it has many advantages over the previously mentioned techniques, it also faces some disadvantages. When a user has many complicated roles, the application becomes unsupported. Membership, role inheritance, and the necessity for personalized advantages make administration in big systems somewhat unwieldy. RBAC does not have a method of detecting the relationship between users and using that knowledge to make policy decisions.

Table 1: Analysis of Various techniques with merits and demerits

S. No	Techniques	Merits	Demerits
1	Elliptical curve cryptography	Enhances CPU and memory performance while lowering power consumption	It increases the size of the encrypted message.
2	Advanced encryption standard algorithm	Improves image pixel assortment and diverse detecting information	More steganography compress shrink security is required

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

3	Data encryption standard	Cloud storage services are provided	It is vulnerable to attacks using linear cryptanalysis
4	Triple data encryption standard	Improves the cost performance trade off and is the best match in a variety of critical applications	vulnerable to man in the middle attacks due to its low file size
5	Blow fish	Encryption time and throughput are improved	Each pair of users has distinct requirements. Therefore, key management becomes more difficult as the number of users increases.
6	Two fish	Run in littler processor and insert in equipment. It is an unlicensed and openly accessible algorithm	It has insufficient encryption speed
7	Role based access control	RBAC's core reference models perform better in terms of authentication and access control	No restrictions restricting the number of users for the same job

Table 1 summarizes the analyzed techniques such as ECC, AES, DES, TDES, Blowfish, Two Fish, and Role-Based Access Control. It also gives the Significance (i.e.) the advantages and challenges faced by utilizing the techniques mentioned above in cloud computing.

In this section various existing techniques used in secured Encryption have been analyzed. Encryption, Decryption processes using those techniques were also discussed, along with the drawbacks. To overcome the drawbacks mentioned above a novel technique called the Enhanced Role-Based Access Control technique is proposed and is discussed in the next section.

2.8. Enhanced authentication methods

From the above section, the merits and drawbacks of various algorithms has been proposed. The recent research works deal with the improvement in such algorithms to overcome the drawbacks they possess. Hence various enhanced authentication techniques have been introduced concerning different application platforms.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

3. Proposed ElGamal SBO with Delta Competitive NN Cryptography

Cloud consumers face challenges regarding privacy and protection while transmitting and storing data in cloud servers. Users in a distributed cloud system have no proper access control of their remote data when it is sent to a cloud server. Also, the existing techniques to secure cloud transmission and storage are vulnerable to attacks due to no restriction in providing access and enlarged encryption message size with improper key management, increasing the computational time and leakage of educational data. To solve this problem, a novel **ElGamal SBO with Delta Competitive NN Cryptography** is introduced in which two-phase operation takes place. In the first phase of operation, the ElGamal educational data encryption has been performed with appropriate multiplicative operator and generator order selection to produce encrypted educational data. Then, the incorporated Stag beetle optimization scheme in the encryption algorithm selects the suitable optimized secured key with proper key management. Thus, access is provided only to the authorized student with the key credentials to log in to the educational data in the cloud server. Thus, reduces the encryption time and computational complexity using an Encryption scheme with an optimization process. Then, to prevent educational data leakage and vulnerable attacks during the transmission of educational data to cloud storage and user, Delta Competitive NN based secure data transmission has been used in which the decryption process is controlled to prevent the leakage of data and vulnerable attacks using Delta competitive rule thereby reject and block malicious login request.

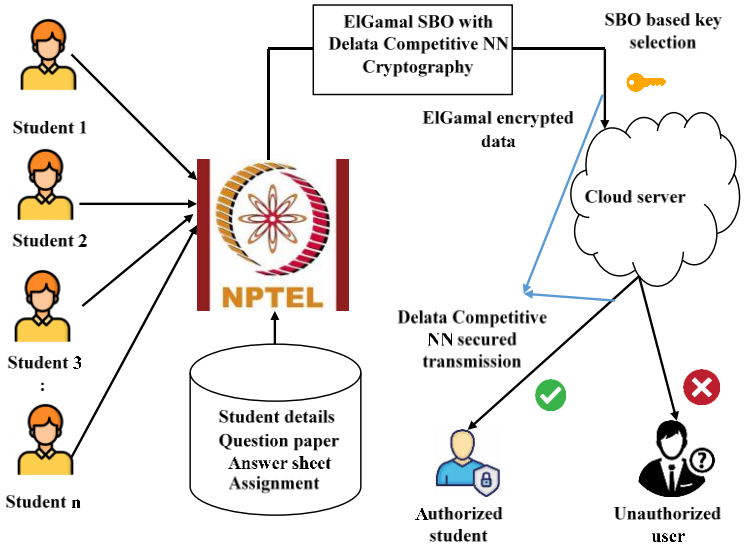


Figure 10: System model of proposed ElGamal SBO with Delta Competitive NN Cryptography

Figure 10 depicts the system architecture of the proposed ElGamal SBO with Delta Competitive NN Cryptography. The student data such as student details, courses, assignments and question papers in NPTEL database has been encrypted with proper key management using ElGamal SBO scheme, and the educational data transmission to the cloud server and access to authorized and unauthorized users were controlled using Delta Competitive NN secure data transmission thereby enhance security in

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

cloud storage without data leakage and vulnerable attack.

3.1 ElGamal Stag beetle optimization based encryption scheme

ElGamal encryption has been performed on NPTEL database with educational data. For performing Encryption, initially public parameters have been anticipated with the selection of two prime numbers u and v using SBO. Then a multiplicative group has been selected based on random assumption. Using the prime numbers, multiplicative group and generator, the keys have been generated and optimally selected using Stag beetle optimization algorithm. Based on these optimal keys, the Encryption of educational data in NPTEL database has been performed. The authorized student with an optimal secret key can only access the educational data by decrypting the encrypted data. The process in ElGamal Stag beetle optimization based encryption scheme has been expressed in algorithm 1.

Algorithm 1: ElGamal Stag beetle optimization based encryption scheme

Input: Educational data from NPTEL database

Output: Encrypted educational data

Initialize public parameters

Take two large prime numbers u and v such that $\frac{u}{v} - 1$ using SBO

Select multiplicative group K of order m with generator N

/* u, v and N are publically known parameters *

Choose value of public key randomly as $Pu_K \in Y_Q^*$

Calculate private key as $Pv_K = N^{Pu_K}$

Select optimized public and private key using Stag beetle optimization

Perform Encryption using optimized keys as $E_C(Edu) = (u, v)$

/* Edu is educational data, $u = N^{Y_Q}$, $v = Edu P_{v_K}^{Y_Q}$ chosen based on randomly selected public key*/

Decrypt $E_C(Edu)$ using optimized secret key and is expressed as $Edu = v.u^{-Pu_K}$

End

Initially, two prime numbers u and v have been selected to generate the key as shown in algorithm 1. The optimized key is a larger secret key that cannot be cracked by modern computers. This ensures effective key management, which increases the security of login activity by fortifying the key creation process. The movement of individual stag beetle based on independent local searching behavior is given in eqn (1) as

$$X_{is}^{T+1} = X_{is}^{T} + \lambda S_{is}^{T} + (1 - \lambda)\mu_{is}^{T} \quad (1)$$

where, μ_{is}^{T} is the position of beetle, S_{is}^{T} is the speed of stag beetle and T is the current number of iteration.

The speed of stag beetle is calculated using eqn (2) as

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

$$S_{is}^{T+1} = WS_{is}^{T} + g_1 R_1\left(U_{is}^{T} - P_{is}^{T}\right) + g_2 R_2\left(U_{is}^{T} - P_{is}^{T}\right) \quad (2)$$

where, W is the weight, g_1, g_2 are the optimistic constants and R_1, R_2 are the arbitrary functions in the range $(0,1)$

The weight function is calculated as shown in eqn (3) as

$$W = \frac{W_{max} - W_{min}}{t} \times T \quad (3)$$

where T and t denotes current and maximum number of iterations, W_{max}, W_{min} represents maximum and minimum value of W

The mathematical representation of incremental function for weight is represented as

$$\xi_{is}^{T+1} = \delta^{t} * S_{is}^{T} * \text{sign}\left(f\left(P_{R_1 s}^{T}\right) - f\left(P_{R_2 s}^{T}\right)\right) \quad (4)$$

Expand the update solution to a high dimension in eqn (4). Here, δ is the step size. The eqn (5) and (6) represents the public and private key selection updating function.

$$X_{R_1 s}^{T+1} = X_{R_1 s}^{T} + S_{is}^{T} * {}^{D}/_{2} \quad (5)$$

$$X_{R_2 s}^{T+1} = X_{R_2 s}^{T} - S_{is}^{T} * {}^{D}/_{2} \quad (6)$$

Hence using these equations, optimal key values are selected and which is used for encrypting and decrypting the educational data. Thereby strengthening the encryption process with optimum selection of key values and making the access secure by using the optimized key as the login credentials. Then to further protect the data transmission and storage in the cloud server, Delta Competitive NN-based secure data transmission is introduced, which is explained in the next subsection.

3.2 Delta Competitive NN based secure data transmission approach

Delta Competitive Neural Network based secure data transmission approach has been used to secure the transmission of educational data to users by managing the decryption activity. Delta Competitive Neural Network's input layer gets user requests from both authorized and unauthorized users, optimized keys and encrypted data. Then, the hidden layers with Delta competitive rule based mechanism identify the authorized user by updating the weights and reducing the cost function using the delta rule. Also, the authorized users are allowed to access the decrypted educational data, whereas the unauthorized users are blocked and rejected from accessing the educational data using the competitive rule. The process in Delta Competitive NN based secure data transmission approach is shown in figure 11.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

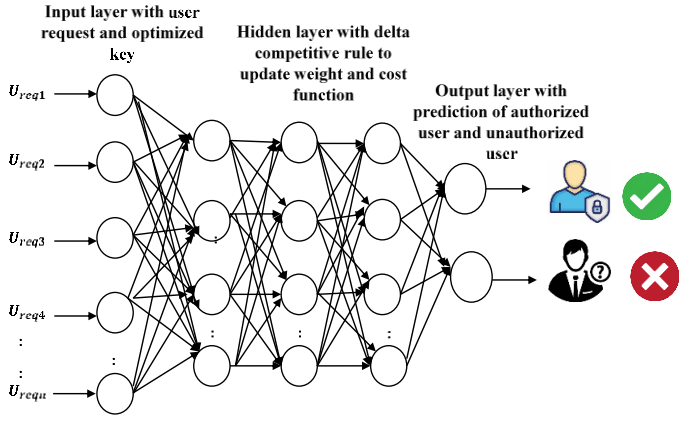


Figure 11: Architecture of Delta Competitive NN based secure data transmission approach

In the learning phase of Delta Competitive NN based secure data transmission approach, the input features, including user requests U_{req1}, U_{req2} ....U_{reqn} from n number of users and optimized key $X_{R_s}^{T+1}$ with assumed initial weights are initialized. The weights are updated using delta rule as ΔW, and the updation is also intended to reduce the cost function as the objective with reduced mean square error is given by,

$$Cost(\Delta W, U_{reqn}, X_{R_s}^{T+1}) = \frac{1}{2}\left(H_F U_{reqn} - X_{R_s}^{T+1}\right)^2 \quad (7)$$

In eqn (7), a hypothesis function H_F has been added to determine the authorized user. Then, the overall cost function is calculated as:

$$C(\Delta W) = \frac{1}{n}\left(C(\Delta W: U_{reqn}, X_{R_s}^{T+1}) + \frac{\alpha}{2}\right) \sum_{m=1}^{M} \sum_{a=1}^{N_l} \sum_{b=1}^{N_l+1} \Delta W_{ab} \quad (8)$$

From equation (8), N_l, $N_l + 1$ signifies number of requests in lth layer, M denotes depth of network and ΔW_{ab} indicates weight of edges a in layer $m - 1$ and b in layer m respectively. The algorithm for Delta Competitive NN based secure data transmission approach is explained as follows:

Algorithm 2: Delta Competitive NN based secure data transmission

---

Input: U_{req1}, U_{req2} ....U_{reqn}, $X_{R_s}^{T+1}$, $E_C(Edu)$

Output: Secured educational data transmission

Begin

for users with request, optimized key and encrypted data

Calculate $Cost(\Delta W, U_{reqn}, X_{R_s}^{T+1})$ using eqn (7)

Measure $C(\Delta W)$ using eqn (8)

if $(C(\Delta W) \geq 0)$, then

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

Proceed with secured transmission
Provide access to authorized user
Else
Do not proceed
Reject and block access to unauthorized users
End if
End for
End

Hence, the secured data transmission in the delta competitive neural network model has been explained in algorithm 2 in which the condition for data transmission and blockage has been provided using measured cost function without error due to the adoption of delta competitive rule.

3.3 Security Model

The goal of the security model is to protect the privacy of educational data from NPTEL database in the cloud server. This data in the cloud server should be secured effectively during storage and transmission. Also, this educational data should not be available to unauthorize malicious users. Hence, a security model has been created in this research and its security mechanism has been explained as follows:

Key management: In the key management phase, the public and private keys are initially generated from two large prime numbers provided by SBO approach. Then, to further manage the key generation process and to enhance the security of login access, an optimized secret key has been selected using SBO, thereby effectively managing the access credentials with the secure generation of larger keys that are unbreakable by modern computers. Thus, the key management phase makes the cloud environment secure by strengthening the key credentials required for login access.

Secured Storage: To enhance the security during the storage of educational data in cloud server, the educational data has been encrypted using ElGamal encryption, and this encryption process has been strengthened by using the optimized secret key in the encryption process thereby this security model provides enhanced security while storing the data to cloud server with minimum encryption time and computational overhead.

Secured Transmission: The educational data transmission security in the cloud environment has been provided using Delta Competitive NN based secure data transmission in the security model. Thus, only authorized users get access to decrypted educational data transmission by controlling the Decryption in cloud server based on user request and optimized key.

4.Results and Discussions

This section compares and contrasts various analytical techniques. Student content, question papers, and answer sheets make

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

up the dataset to validate the performance. In this case, Cloud Simulator is written in Python. Three metrics are used to evaluate the output of the various methods: encryption time, decryption time, and retrieval time.

4.1. System Specification

The suggested system has been implemented in Python to demonstrate competent power utility. The system specifications are (i) Windows 7 operating system (ii) Intel Core i5 processor with 8 GB RAM (iii) Dataset: NPTEL dataset (iv) Platform: Python

4.2. Performance Metrics

The techniques as mentioned earlier are evaluated for their performances and the results are discussed in this section with the following metrics.

4.2.1. Retrieval Time

The time it takes to retrieve/access the data is called the data retrieval time.

$$\text{retrieval time}(T) = \frac{\text{data size (DS)}}{\text{speed (S)}}$$

Where:
DS refers to the size of the data used to perform the process
S refers to the speed of the operation

4.2.2. Encryption Time

The encryption time is when it takes an encryption algorithm to convert plaintext into cipher text. The encryption scheme's throughput is determined using encryption time. It refers to the speed with which data is encrypted.

$$\text{encryption time}(T) = \frac{\text{data size (DS)}}{\text{speed (S)}}$$

Where:
DS refers to the size of the data used to perform the process
S refers to the speed of the operation

4.2.3. Decryption Time

Decryption time is the time it takes to convert encrypted data to its original type. In most cases, it's a reversal of the encryption method. Since Decryption involves a hidden key or password, it decodes the encrypted information such that only an approved person can decrypt the details.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

$$\text{decryption time (T)} = \frac{\text{data size (DS)}}{\text{speed (S)}}$$

Where:

DS refers to the size of the data used to perform the process

S refers to the speed of the operation

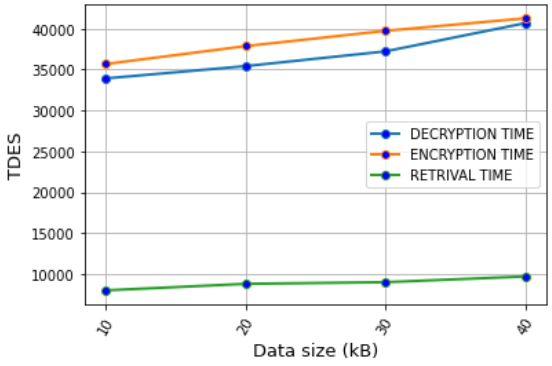


Figure 12: Performance of TDES

The analysis of various techniques is depicted in figure.12. The graph denotes the performance of the TDES in terms of encryption time, decryption time and retrieval time. It shows that the decryption time for data 10 kB is 33914 ms. For transferring 40 kB data, the value is found to be 40672 ms. Similarly, the values of encryption time obtained for decryption time and retrieval time are 35674ms and 8000 ms for 10 kB data, respectively and 41263 and 9700 ms for transferring 40kB data, respectively.

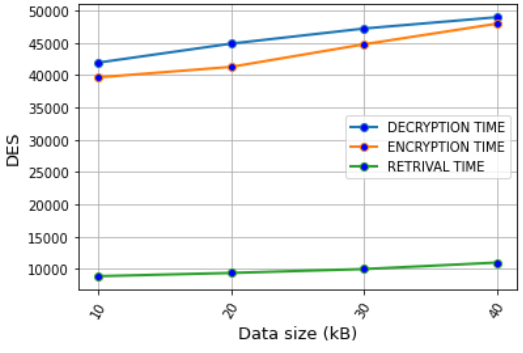


Figure 13: Performance of DES

Figure 13 shows the performance of DES algorithm. The corresponding encryption time, decryption time and retrieval time obtained are 39645, 41928 and 8900 for 10 kB data respectively and for 40kB the values obtained are 47942,48942 and 11000 ms respectively for transferring 40 kB data.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

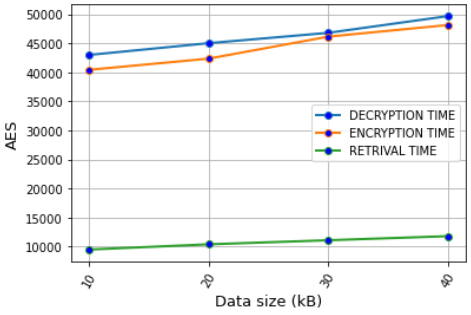


Figure 14: Performance of AES

The graph shows the plot of time vs data size for AES method was explained in figure 14. The encryption time is 40435 ms and 48143 ms. The values obtained for decryption time is 42977 and 49675 for transferring 10 kB and 40 kB data respectively. Maximum retrieval time obtained is 11800 ms.

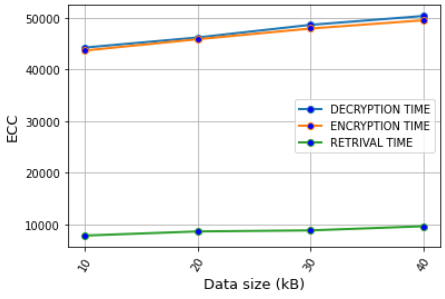


Figure 15: Performance of ECC

For ECC method in figure 15, the value for encryption time is 43675ms for 10 kB data and 49535 ms for 40 kB respectively. The decryption time is 44247 ms and 50363 ms respectively. For transferring data 10 kB and 40 kB the value obtained is 7800 and 9600 respectively.

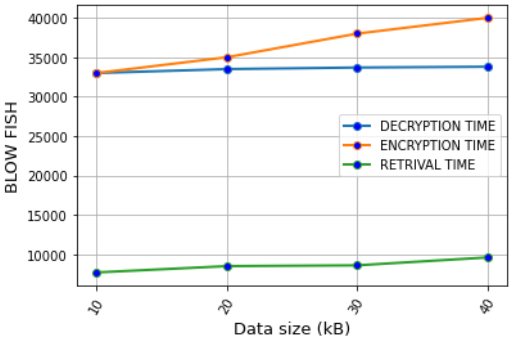


Figure 16: Performance of Blow fish

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

Figure 16 shows the performance of blow fish. The value of encryption time varies from 33000 to 40000 ms for blow fish algorithm and the decryption time range is from 33000 to 33800 ms for 10 kB and 40 kB data size respectively. The retrieval time varies from 7700 to 9600 ms respectively.

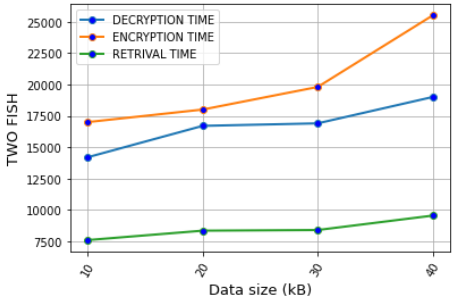


Figure 17: Performance of Two fish

Figure 17 shows the performance Two fish. For two fish method the corresponding encryption time, decryption time and retrieval time obtained are 17000, 14200 and 7600 ms respectively. The values for transferring 40 kB data are 25500, 19000 and 9550 ms respectively.

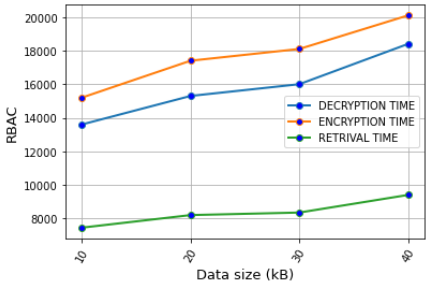


Figure 18: Performance of RBAC

Figure 18 shows the performance of RBAC. The data size foe RBAC method varies between 10 to 40 kB. The encryption time varies from 15200 tp 20100 ms. The decryption time lies between 14200 and 19000 ms and the retrieval time varies between 7450 and 9400 ms respectively.

From the above validation of techniques, the RBAC technique is superior to all other models with good range of Encryption, Decryption and retrieval time and effective data size. However, it has some drawbacks as when a user has many complicated roles, the application becomes unsupported. Hence, an improved constraint model has been proposed to expand the main RBAC concept to facilitate team collaboration and workflow management.

4.4 Performance Analysis of Proposed ElGamal SBO with Delta Competitive NN Cryptography

This section evaluates the performance of the ElGamal SBO with Delta Competitive NN Cryptography technique for various

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

parameters.

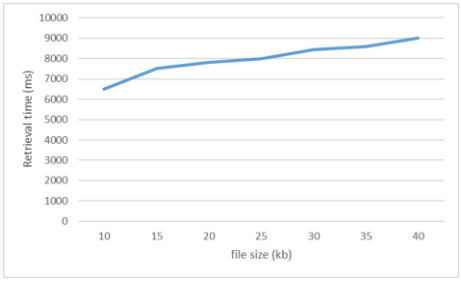


Figure 19: Performance of proposed method based on retrieval time

Figure 19 shows the efficiency of the ElGamal SBO with Delta Competitive NN Cryptography technique in terms of retrieval time. The file size is represented on the x-axis, and the retrieval time is represented on the y-axis. The proposed approach took 6450ms to retrieve the 10 kb file, 7500ms to retrieve the 20 kb file, 7800ms to retrieve the 30 kb file, and 9000ms to retrieve the 40 kb file. The retrieval time increases with the increase in file size. The retrieval time has been reduced by ElGamal SBO approach due to the selection of optimized secret key.

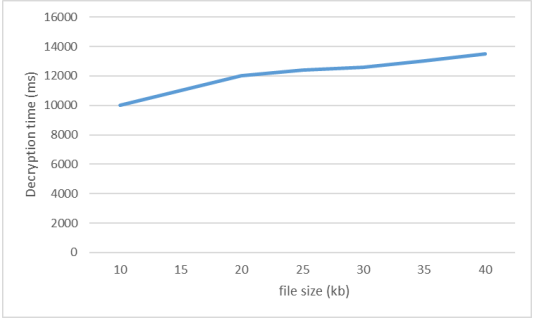


Figure 20: Performance of proposed method based on decryption time

Figure 20 shows the proposed technique's efficiency in decryption time. An effective method should be based on the shortest amount of time possible. Figure 20 shows that the proposed approach took 10000ms, 12000ms, 12600ms, and 13500ms for data sizes of 10kb, 20kb, 30kb, and 40kb. The decryption time is reduced in the proposed method due to the controlled decryption process performed by Delta Competitive NN secure transmission.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

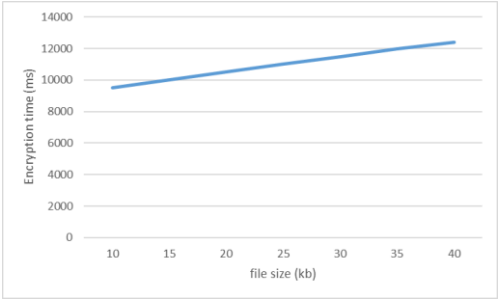


Figure 21: Performance of proposed method based on encryption time

The encryption time of proposed method is shown in Figure 21. For 10kb, 20kb, 30kb, and 40kb, the proposed technique took 9500ms, 10500ms, 11500ms, and 12400ms, respectively. The encryption time of the proposed cryptography technique has been maintained in a minimum possible range by performing ElGamal cryptography with random keys converted into optimized keys, thereby managing the encryption process to complete in sufficiently less time.

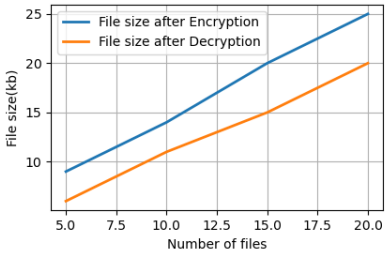


Figure 22: File size taken for the proposed method

The file size derived for the procedure is examined in Figure 22. The initial file sizes are 5 kb, 10 kb, 15 kb, and 20 kb. The file size was initially 5 kb before Encryption, but it was modified to 8 kb after Encryption. The file size is replaced by 10 kb, 15 kb, and 20 kb after encoding 13 kb, 19 kb, and 24 kb. The encrypted file is then uploaded to the server. After uploading the folder, the student must decrypt it to open it. The file's size is converted to its original size during decryption. Based on the data size above 40 kb and the transaction speed, the Encryption, retrieval, and decryption time is calculated. In the proposed method, when the data size increases, the time also increases, so if the data size is above 40 Kb, then the time of Encryption and Decryption also increases.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

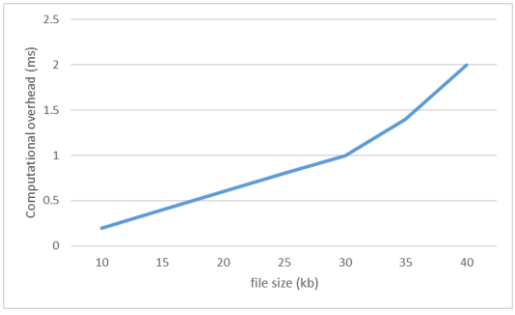


Figure 23: Computational overhead of proposed model

The computational overhead of the proposed cryptography approach is shown in figure 23. The computational overhead for file size ranges from 10 to 40 kb. From the calculation, it is noted that the computational overhead ranges between 0.2 to 2ms, which is considered as a small range for file sizes from 10kb to 40 kb. The computational overhead of proposed method has been eliminated by the selection of optimized key and neural network-based approach for the educational data transmission.

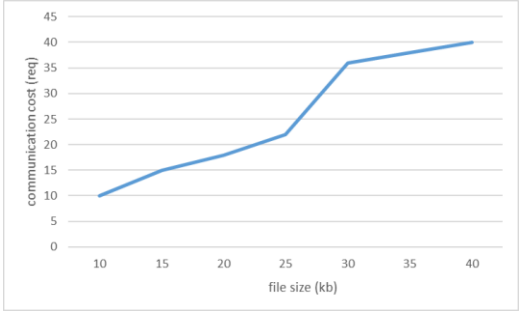


Figure 24: Communication cost of proposed method

Figure 24 depicts the communication cost of proposed ElGamal SBO with Delta Competitive NN Cryptography technique. The communication cost during data transmission to the cloud server and authorized user has been determined based on the number of user requests. When the size of file increases from 10 kb to 40 kb, the communication cost is also increase from 10 to 40 due to the increase in user request. However, the communication cost during educational data transmission has been maintained using Delta Competitive NN secured data transmission approach in which cost is reduced by delta rule.

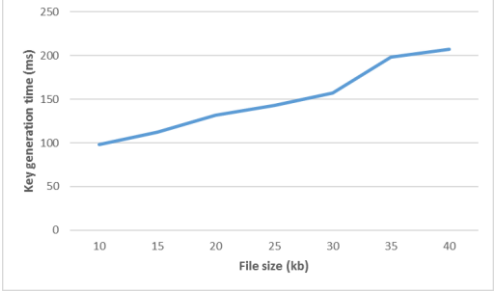


Figure 25: Key generation time

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions

The key generation time of the proposed cryptography technique is shown in figure 25. The generation time for file sizes 10 kb to 40 kb range from 98 ms to 207 ms. When the file size increases, the key generation time also increases. The key generation time has been reduced due to the Stag beetle optimization incorporated in the proposed cryptography approach with the calculation of minimized overall cost function.

Security Proof: The proposed approach preserves the privacy of educational data under the hardness of solving Computational Diffie–Hellman (CDH) Problem. After complete execution of the proposed approach cloud server obtains the global count of file size as $F_{size} = \sum_{j=1}^{N} F_{size_{(i)}}$ for all files. Any malicious activity during message exchange among NPTEL database to cloud server conspires and reveals the private value of some targeted educational data. The private value of any educational data in NPTEL database cannot be revealed by such a coalition, as demonstrated in this instance. To reveal any NPTEL database's private data, an attacker has ciphertext as $E_C(Edu) = (u, v)$. An opponent's only known values for decrypting this ciphertext are the public parameters u, v and N. The value of optimized secret keys, file size and overall cost function is only known to authorized login credential users. Any set of the adversary will be able to solve the CDH challenge if they can figure out how to use the overall cost function to reveal file size and optimized secret key. The CDH puzzle is demonstrated to be challenging. As a result, the CDH issue is the same as computing the secret value, file size and optimized secret key of any cloud server with NPTEL educational data by any hostile attacker. Hence, the proposed model is highly secured due to the difficulty in extracting original educational data from encrypted educational data since the authorized secret key is not provided to the unauthorized user to solve the CDH problem.

4.5 Comparative analysis

To demonstrate the efficacy of the proposed approach, it was compared to seven other methods: DES-based data protection [Elgeldawi, et al. (2019)], TDES based data security [Elgeldawi, et al. (2019)], AES-based data security [Wani, et al. (2019)], Blow Fish-based data security [Wani, et al. (2019)], ECC-based data security [Dheepak T (2021)], RBAC-based data security [Jayasankar T, et al. (2021)] and Two Fish based data security [Jayasankar T, et al. (2021)].

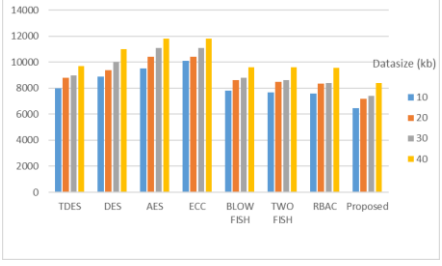


Figure 25: Comparative retrieval time-based analysis.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

723 **Table 2**: Comparative retrieval time-based analysis

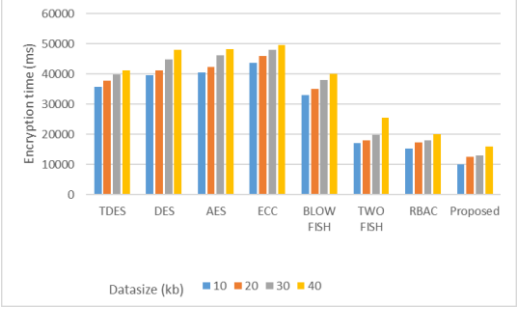
724

Data size (kB)	TDES	DES	AES	ECC	BLOW FISH	TWO FISH	RBAC	Proposed
10	8000	8900	9500	10100	7800	7700	7600	6450
20	8800	9400	10400	10400	8600	8500	8350	7200
30	9000	10000	11100	11100	8800	8600	8400	7400
40	9700	11000	11800	11800	9600	9600	9550	8400

725

726 Figure 25 shows the comparison results analyzed in terms of the retrieval time. In the analysis of Table 2, TDES Method was
727 taken for minimum data recovery of 8000 for10 Kb, which consists of 8900ms for secure data recovery from DES; 9500ms of
728 safe data recuperation based on AES; 10100ms of data recollection based on ECC; 7800ms of data recovery based on Blow
729 Fish; 7700ms of data recovery from two fish; 7600ms of RBAC data recollection; and 7450ms for data security based on
730 ERBAC Method. Because the search time was based on 2 approaches and cryptographic ways to secure cloud records, that
731 proposed method is far superior to the other seven algorithms.

732



733

734

735 **Figure 26: Comparison of encryption time**

736 **Table 3:** Comparative encryption time

Data size (kB)	TDES	DES	AES	ECC	BLOW FISH	TWO FISH	RBAC	Proposed
10	35674	39645	40435	43675	33000	17000	15200	10000
20	37864	41264	42361	45863	35000	18000	17400	12500

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022

Geoscientific Instrumentation Methods and Data Systems Discussions
Open Access
EGU

30	39732	44753	46143	47934	38000	19800	18100	13000
40	41263	47942	48143	49535	40000	25500	20100	13500

Figure 26 shows a comparative comparison focused on encryption time. When evaluating table 3, the TDES method took 42163ms to decrypt 40kb data, while DES-based Encryption took 47942ms, AES-based Encryption took 48143ms, ECC-based data encryption took 49535ms, Blowfish based data encryption took 40000ms, RBAC based data encryption took 20100ms, Two Fish based data encryption took 25500ms. The data size is increasing, while the encryption size is gradually increasing, as seen in the diagram. Encryption time is, in reality, the start of a test data algorithm before the best potential answer is discovered. This time was depicted in seconds. Encoding time was used to increase the number of files in this test, and optimum or near-optimal solutions in algorithms were subsequently identified. The proposed cryptography technique has the lowest encryption time of 13500 ms for the file size of 40 kb which is very low compared to existing techniques.

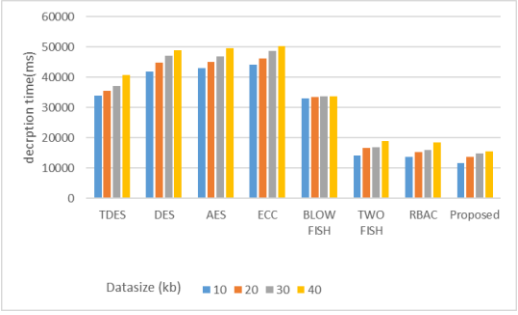


Figure 27: Decryption-based comparative analysis.

Table 4: Decryption-based comparative analysis

Data size (kB)	TDES	DES	AES	ECC	BLOW FISH	TWO FISH	RBAC	Proposed
10	33914	41928	42997	44247	33000	14200	13600	11600
20	35417	44863	45023	46198	33500	16700	15300	13600
30	37218	47194	46798	48647	33700	16900	16000	13900
40	40672	48942	49675	50363	33800	19000	18400	14000

Figure 27 shows a comparative comparison focused on decryption time. When evaluating table 4, the TDES method took 40672ms to decrypt 40kb data, while DES-based Decryption took 48942ms, AES-based Decryption took 49675ms, and ECC-based data decryption took 50363ms, Blowfish based data decryption took 33800ms, Two Fish based data decryption took 19000ms, RBAC based data decryption took 18400ms. The decryption time of the proposed cryptography technique with a neural network has been determined as 14000 ms for 40 kb file size, which is very low compared to other existing techniques.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

Thus, the performance of ElGamal SBO with Delta Competitive NN Cryptography technique is evaluated and the results are better than the DES-based data protection, AES-based data security, ECC-based data security, Blow Fish based data security, TDES based data security, RBAC based data security, and Two Fish based data security, based on encryption time, decryption time, retrieval time, size of files in Encryption and decryption time.

5. Conclusion

This study aims to figure out the ideal cryptographic technique for End-To-End Encryption security for educational purposes. For this purpose, various encryption methodologies are compared to various metrics including encryption time, decryption time, retrieval time and number of data size versus Encryption for the NPTEL cloud database and an enhanced role-based technique has been suggested. After conducting performance evaluation analysis with various cryptographic algorithms, the enhanced encryption technique outperformed the other approaches on all performance metrics and was more secure. The data decryption took 12600ms, data encryption took 11000ms and a retrieval time of 7450ms for 10 kB data size. For 40 kB size the values of encryption time, decryption time and retrieval time are 16500,16900 and 9400 respectively. Thus, the proposed ElGamal SBO with Delta Competitive NN Cryptography technique controls the complexity while managing key generation process. Also, unauthenticated users are restricted from using the network and it protects the stored data, thereby providing secured authentication. Furthermore, when used in a cloud environment, the proposed cryptography technique improves encryption effectiveness and security with retrieval time of 8400 ms, encryption time of 13000 ms, decryption time of 14000 ms, computational overhead of 2 ms and communication cost of 40 when file size is 40 kb.

References

Abdullah, Dahlan, Widia Fatimah, Ratnadewi, R., Nuning Kurniasih, Dian Rianita, Berliana Kusuma Riasti, Edi Sofian et al.: Sms Encryption Application Using 3Des (Triple Data Encryption Standard) Algorithm Based on Android. In Journal of Physics: Conference Series, IOP Publishing, 1363(1), 012077, 2019.

Aldabbagh, Ghadah, Daniyal Alghazzawi, M., Syed Hamid Hasan, Mohammed Alhaddad, Areej Malibari, and Li Cheng: Secure Data Exchange in M-Learning Platform using Adaptive Tunicate Slime-Mold-Based Hybrid Optimal Elliptic Curve Cryptography, Applied Sciences, 11(12), 5316, 2021.

Alhaidari, Fahd, A and Ebtesam Alqahtani, J.: Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey, J. Commun., 15(1), 14-30, 2020.

Al-Malah, Duha Khalid Abdul-Rahman, Ibtisam Aljazaery, A., Haider Th Salim Alrikabi, and Hussain Ali Mutar: Cloud computing and its impact on online education, In IOP Conference Series: Materials Science and Engineering. IOP Publishing, 1094(1), 012024, 2021

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

784 Anilkumar, Chunduru, and Sumathy Subramanian: A novel predicate based access control scheme for cloud environment using
785 open stack swift storage, Peer-to-Peer Networking and Applications, 14(4), 2372-2384, 2021.
786 Awan, Ijaz Ahmad, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, and Allah Ditta: Secure
787 framework enhancing AES algorithm in cloud computing, Security and Communication Networks, 2020.
788 Badsha, Shahriar, Iman Vakilinia, and Shamik Sengupta: Blocynfo-share: Blockchain based cybersecurity information sharing
789 with fine grained access control, In 2020 10th Annual Computing and Communication Workshop and Conference
790 (CCWC), IEEE, 0317-0323, 2020.
791 Barakabitze, Alcardo Alex, Anangisye William-Andey Lazaro, Neterindwa Ainea, Michael Hamza Mkwizu, Hellen Maziku,
792 Alex Xavery Matofali, Aziza Iddi, and Camillius Sanga: Transforming African education systems in science, technology,
793 engineering, and mathematics (STEM) using ICTs: Challenges and opportunities, Education Research International, 2019.
794 Bhattacharjya, Aniruddha, Xiaofeng Zhong, Jing Wang, and Xing Li: CoAP—application layer connection-less lightweight
795 protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP, In Digital twin
796 technologies and smart cities. Springer, Cham, 151-175, 2020.
797 Biswal, Amrit Kumar, and Al Mallah Obada: Analytical assessment of binary data serialization techniques in iot context
798 (evaluating protocol buffers, flat buffers, message pack, and bson for sensor nodes), 2019.
799 Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki: Network intrusion detection for
800 IoT security based on learning techniques, IEEE Communications Surveys & Tutorials, 21(3), 2671-2701, 2019.
801 Chen, Shuang, Wei Hu, and Zhenhao Li: High performance data encryption with AES implementation on FPGA. In 2019
802 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance
803 and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), IEEE, 149-153, 2019.
804 Dheepak, T.: Enhancing the Cloud Security with ECC based Key Generation Technique, Annals of the Romanian Society for
805 Cell Biology, 3874-3891, 2021.
806 Dinesh, E and Ramesh, S.M.: Security aware data transaction using optimized blowfish algorithm in cloud
807 environment, Journal of Circuits, Systems and Computers, 30(01), 2150004, 2021.
808 Elgeldawi, Enas, Maha Mahrous, and Awny Sayed: A comparative analysis of symmetric algorithms in cloud computing: A
809 survey, International Journal of Computer Applications, 975, 8887, 2019.
810 Farhan, Wejdan, Jamil Razmak, Serge Demers, and Simon Laflamme: E-learning systems versus instructional communication
811 tools: Developing and testing a new e-learning user interface from the perspectives of teachers and students, Technology
812 in Society, 59, 101192, 2019.
813 Gangireddy, Venkata Koti Reddy, Srihari Kannan, and Karthik Subburathinam: Implementation of enhanced blowfish
814 algorithm in cloud environment, Journal of Ambient Intelligence and Humanized Computing, 12(3), 3999-4005, 2021.
815 Hidayat, Taufik, and Rahutomo Mahardiko: A Systematic literature review method on aes algorithm for data sharing
816 encryption on cloud computing, International Journal of Artificial Intelligence Research, 4(1), 49-57, 2020.
817 Hirschi, Lucca, and Jean-Yves Marion: Symbolic-Model-Guided Fuzzing of Cryptographic Protocols.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

Ikhwan, Ali, Rafikha Aliana Raof, A., Phaklen Ehkan, Yasmin Yacob, and Syaifuddin, M.: Data Security Implementation using Data Encryption Standard Method for Student Values at the Faculty of Medicine, University of North Sumatra, In Journal of Physics: Conference Series. IOP Publishing, 1755(1), 012022, 2021.

Irgashevich, Dadamuxamedov Alimjon: Methods of using cloud technologies in Islamic education institutions, Methods, 7(5), 2020.

Jayasankar, T., Bhavadharini, R.M., Nagarajan, N.R., Mani, G and Ramesh, S.: Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform, European Journal of Molecular & Clinical Medicine, 8(01), 1075-1089, 2021.

Jayasankar, T.R.M., Bhavadharini, N.R., Nagarajan Mani, G and Ramesh, S.: Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform, European Journal of Molecular & Clinical Medicine, 8(01), 1075-1089, 2021.

Jayasarathi, M., Rajeshwari, S., Shiny Mercy, I and Rathika, S.K.B.: Enhanced on Data Encryption Standard for Secured Cloud Storage, Bonfring International Journal of Software Engineering and Soft Computing, 9(1), 710, 2019.

Jia, Mengda, Ali Komeily, Yueren Wang, and Ravi Srinivasan, S.: Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications, Automation in Construction, 101, 111-126, 2019.

Kareem, Suhad Muhajer, and Abdul Monem Rahma, S.: A novel approach for the development of the Twofish algorithm based on multi-level key space, Journal of Information Security and Applications, 50, 102410, 2020.

Khan, Imran Ahmad, and Rosheen Qazi: Data security in cloud computing using elliptic curve cryptography, International Journal of Computing and Communication Networks, 1(1), 46-52, 2019.

Khan, Jamil, Y and Mehmet Yuce, R.: eds. Internet of Things (IoT): systems and applications, CRC Press, 2019.

Kumari, Adesh, Yahya Abbasi, M., Vinod Kumar, and Akber Ali Khan: A secure user authentication protocol using elliptic curve cryptography, Journal of Discrete Mathematical Sciences and Cryptography, 22(4), 521-530, 2019.

Maata, Rolou Lyn, R., Ronald Cordova, S and Alrence Halibas: Performance Analysis of Twofish Cryptography Algorithm in Big Data, In Proceedings of the 2020 9th International Conference on Software and Information Engineering (ICSIE), 56-60, 2020.

Milani, Stefano, and Ioannis Chatzigiannakis: Design, analysis, and experimental evaluation of a new secure rejoin mechanism for lorawan using elliptic-curve cryptography, Journal of Sensor and Actuator Networks, 10(2), 36, 2021.

Mohammed, Nadia, and Najla Ibrahim: Implementation of new secure encryption technique for cloud computing, In 2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA), IEEE, 1-5, 2019.

Muhammed, Ishaq, Muhammad Aliyu, Iliya Musa Adamu, And Amatullah Yahaya Aliyu: Securing Cloud Data Using Blowfish Algorithm Combined With Text Steganography, 2020.

Mulauzi, Felesia, Gabriel Walubita, and Judith Pumulo: Introduction of computer education in the curriculum of Zambian primary and secondary schools: Benefits and challenges, Marvel Publishers, 2019

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

852 Pandian, Soundhara Raja, R and Kasiapillai Kasiviswanathan, S.: Effective Use of CloudComputing Concepts in Engineering
853 Colleges, In 2011 IEEE International Conference on Technology for Education, IEEE, 233-236, 2011.
854 Pushpa, B.: Hybrid data encryption algorithm for secure medical data transmission in cloud environment, In 2020 Fourth
855 international conference on computing methodologies and communication (ICCMC), 329-334, 2020.
856 Qazi, Rosheen, Kashif Naseer Qureshi, Faisal Bashir, Najam Ul Islam, Saleem Iqbal, and Arsalan Arshad: Security protocol
857 using elliptic curve cryptography algorithm for wireless sensor networks, Journal of Ambient Intelligence and Humanized
858 Computing, 12(1), 547-566, 2021.
859 Raheja, Nisha, and Amit Kumar Manocha: An Efficient Encryption-Authentication Scheme for Electrocardiogram Data using
860 the 3DES and Water Cycle Optimization Algorithm, In 2021 6th International Conference on Signal Processing,
861 Computing and Control (ISPCC), IEEE, 10-14, 2021.
862 Rashid, Muhammad, Mohammad Mazyad Hazzazi, Sikandar Zulqarnain Khan, Adel R. Alharbi, Asher Sajid, and Amer
863 Aljaedi: A Novel Low-Area Point Multiplication Architecture for Elliptic-Curve Cryptography, Electronics, 10(21), 2698,
864 2021.
865 Sadawarti, Kanav: Secure Cloud Computing Platform Advantaged by Data Encryption and CS Optimized Ffbpnns, Turkish
866 Journal of Computer and Mathematics Education (TURCOMAT), 12(12), 979-988, 2021.
867 Santoso, K.I., Muin, M.A and Mahmudi, M.A.: Implementation of AES cryptography and twofish hybrid algorithms for cloud,
868 In Journal of Physics: Conference Series, 1517(1), 012099, 2020. IOP Publishing.
869 Saračević, Muzafer, H., Saša Adamović, Z., Vladislav Miškovic, A., Mohamed Elhoseny, Nemanja Maček, D., Mahmoud
870 Mohamed Selim, and Shankar, K.: Data encryption for Internet of Things applications based on catalan objects and two
871 combinatorial structures, IEEE Transactions on Reliability, 70(2), 819-830, 2020.
872 Selvarani, P., Annamalai Suresh and Malarvizhi, N.: Secure and optimal authentication framework for cloud management
873 using HGAPSO algorithm, Cluster Computing, 22(2), 4007-4016, 2019.
874 Selvi, M and Ramakrishnan, B.: Secured Message Broadcasting in VANET using Blowfish Algorithm with Oppositional Deer
875 Hunting Optimization, International Journal of Computer Network & Information Security, 13(2), 2021.
876 Shylam S and Sujatha, S.S.: Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish
877 algorithm, Journal of Ambient Intelligence and Humanized Computing, 13(1), 151-163, 2022.
878 Sondhara Raja Pandian, R and Christopher Columbus, C.: Automatic Feedback System for Online Video Classes by using
879 Facial Expression, Tierärztliche Praxis, 40, 1773-1787, 2020.
880 Soundhara Raja Pandian, R., Thangalakshmi, S and Saravanan, S.: Virtual Learning System: A Conceptual Framework of
881 Network Optimization, In Proceedings of the International Conference on Soft Computing for Problem Solving, (SocProS
882 2011) December 20-22,789-795, 2011. Springer, India, 2012.
883 Su, Mang, and Liangchen Wang: PreBAC: a novel Access Control scheme based Proxy Re-Encryption for cloud
884 computing, KSII Transactions on Internet and Information Systems (TIIS), 13(5), 2754-2767, 2019.

https://doi.org/10.5194/gi-2022-15
Preprint. Discussion started: 22 August 2022


Geoscientific Instrumentation Methods and Data Systems Discussions

885 Su, Na, Yi Zhang, and Mingyue Li: Research on data encryption standard based on aes algorithm in internet of things
886 environment, In 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference
887 (ITNEC), IEEE, 2071-2075, 2019.
888 Sultan, Nazatul Haque, Maryline Laurent, and Vijay Varadharajan: Securing Organization's Data: A Role-Based Authorized
889 Keyword Search Scheme with Efficient Decryption, IEEE Transactions on Cloud Computing, 2021
890 Suwannapong, Chanwit, and Chatchai Khunboa: Congestion control in CoAP observe group communication, Sensors, 19(15),
891 3433, 2019.
892 Teng, Lin, Hang Li, Shoulin Yin, and Yang Sun: A Modified Advanced Encryption Standard for Data Security, Int. J. Netw.
893 Secur., 22(1), 112-117, 2020.
894 Verma, Upendra, and Diwakar Bhardwaj: Elliptic Curve Cryptography based Centralized Authentication Protocol for Fog
895 enabled Internet of Things, International Journal of Computing and Digital Systems, 10, 2021.
896 Vuppala, Akshitha, Sai Roshan, R., Shaik Nawaz, and Ravindra, J.V.R.: An efficient optimization and secured triple data
897 encryption standard using enhanced key scheduling algorithm, Procedia Computer Science, 171, 1054-1063, 2020.
898 Wang, Hua, Zhihua Xia, Jianwei Fei, and Fengjun Xiao: An AES-based secure image retrieval scheme using random mapping
899 and BOW in cloud computing, IEEE Access, 8, 61138-61147, 2020.
900 Wani, Abdul Raoof, Rana, Q.P and Nitin Pandey: Performance evaluation and analysis of advanced symmetric key
901 cryptographic algorithms for cloud computing security, In Soft Computing: Theories and Applications, Springer,
902 Singapore, 261-271, 2019.
903 Widjaja, Andree, E., Jengchung Victor Chen, Badri Munir Sukoco, and Quang-An Ha: Understanding users' willingness to
904 put their personal information on the personal cloud-based storage applications: An empirical study, Computers in Human
905 Behavior, 91, 67-185, 2019.
906 Xu, Jian, Yanbo Yu, Qingyu Meng, Qiyu Wu, and Fucai Zhou: Role-based access control model for cloud storage using
907 identity-based cryptosystem, Mobile Networks and Applications, 26(4),1475-1492, 2021.
908