SN Computer Science (2024) 5:98
https://doi.org/10.1007/s42979-023-02419-3

ORIGINAL RESEARCH

Adaptive Artificial Bee Colony Algorithm-Based Enhancement of Data Security in Cloud Computing

J. Sai Geetha[1]

Received: 8 March 2023 / Accepted: 15 October 2023

Abstract

Nowadays, the usage of network has been increased due to cloud computing. It is used in many applications because of its salient features such as reduced cost, hassle-free usage without the requirement of client–server model. The networked resources of cloud computing environment support the data storage in remote server. It has been used in more applications particularly in resource utilization and data sharing. The fundamental functions of security and user authentication must be improved for cloud computing to operate more efficiently. The above tasks should be achieved through the Artificial Bee Colony with split encryption process and biometric authentication. The biometric authentication is utilized to improve the user authentication in public cloud environment. In addition, the method of split encryption process in Artificial Bee Colony algorithm helps to improve the data security. The proposed methodology, namely biometric-based split encryption (BSE) accomplishes two main goals: (i) enhancement of security and (ii) user authentication. The split encryption process with ABC algorithm is applied to the sensitive data and also combined with the finger impression of the authenticated user. To prevent unwanted access to encrypted data, the resulting data and the biometric authentication should be kept distinct in the cloud storage area and verified before decrypting the original data. The execution time, which includes encryption and decryption, as well as memory usage, are used to gauge the effectiveness of the biometric-based split encryption (BSE). The results of BSE algorithm are compared with the emperor penguin optimization (EPO) with Elliptic curve cryptography.

Keywords Cryptography · Biometric authentication · Artificial bee colony algorithm · Cloud computing · Data storage · Data retrieval · Confidentiality

Introduction

One of the most recent technologies is cloud computing, which has superior features and services and a high capacity while connecting through numerous traditional online computing methods. It is used in different applications, namely science, medical, defence, etc. It consists of collection of resources and also services to manage specific needs such as data storage/recovery, analysis of big data and maintain backups. The ownership of data storage and services related to the cloud servers. The main usage of cloud computing provides free data storage spaces to store huge volume of highly sensitive data. In cloud environment, the data sharing techniques are more user friendly when compared with other kinds of sharing techniques [1]. Most of the end users are moving towards the services of cloud computing because of its services with an on-demand nature.

There are several threats associated with the cloud infrastructure such as scalability, operational control and security. Both privacy concerns and data security are the important issues related to internal and external attacks. Because most of the organizations maintain their highly sensitive and vital data in cloud storage. Because cloud computing services are shared, it is challenging to verify data security in a cloud environment and to restrict unwanted access to or use of data. The special systems and protocols have been designed to establish secured connection between the cloud service providers and end users. The conventional methods are not suitable to solve the security problem in cloud environment.

This article is part of the topical collection "Industrial IoT and Cyber-Physical Systems" guest edited by Arun K Somani, Seeram Ramakrishnan, Anil Chaudhary and Mehul Mahrishi.

✉ J. Sai Geetha
saigeetha.it@bhc.edu.in

[1] Department of Information Technology, Bishop Heber College, Tiruchirappalli, Tamil Nadu, India

Published online: 13 December 2023

Among various techniques applied towards enhancement of cloud data security, cryptography is the most effective mechanism. It is necessary to transfer the data securely that are understandable only by the intended and authorized recipient which is to be achieved by translating plain text into cipher text.

The Private key cryptography method is more suitable for strong data in cloud storage [2]. Both encryption and decryption process are using the similar key and the secret key known only to the owner of the data. The key of Symmetric key cryptography is essential for improving data security. The way to improve the randomness of the key is by generating the random number using any random number generation techniques or optimization algorithm.

Recently, many security algorithms introduced for the security of cloud data. However, they are lagging in primary security parameters associated with performance of cryptographic process such as encryption and decryption time, memory utilization, execution speed, delay of network and less power consumption. Hence, it is necessary to design an algorithm which can satisfy the needs of CSP and also the cloud users. The cloud service provider (CSP) has full responsibility of secured data storage and retrieval. The cloud user tries to enhance the communication security and also provided access control mechanism by authorized user. A novel security algorithm is to be proposed to fulfil the data security parameter.

This paper organized with different sections. To begin with, the next section consists of the existing algorithms related to security enhancement in cloud computing. The subsequent section describes the working principles of BSE algorithm. The description and also the application of optimization algorithm ABC is also included in this section. The penultimate section provides the analysis of the performance through various parameters between the proposed and existing algorithms. The final section concludes the advantages and future enhancement of the proposed model.

Related Work

Nowadays, cloud computing services are used in different applications such as Science, Medical and so on. Many technologies are available to enhance the data storage security in the cloud environment. In this section, some of the existing methodologies are being reviewed.

Rajendra Patil et al. introduced a new model for monitoring the network traffic and intrusion detecting system, namely Hypervisor Level Distributed Network security (HLDSN). The Random forest algorithm is used to detect the network traffic in cloud data storage and also generates intrusion alert message which helps to identify a distributed attack [3]. Mohamed Saidur Rahman et.al. have proposed a framework for preserving privacy service selection using Homomorphic Encryption method for enhancing the QoS values and also minimize the cost of computation through the parallel execution of Map Reduce model [4].

Najd Almoysheer proposed a multilevel cryptographic schema, which includes Blowfish and Elliptic Curve Cryptography. The original message is encrypted using Blowfish algorithm with the help of the key generated by the ECC. The proposed method prevents unauthorized users to access sensitive data in Public cloud [5]. Yibin Li et.al., presented Security Aware Efficient Distributed Storage (SA-EDS) model to prevent the direct access of partial data by cloud operators. In this method, the content of file is to split and store them in distributed severs of cloud. It also reduces the execution time using decomposed form of data packets [6].

P. Chinnasamy et.al. introduced a hybrid approach which included the asymmetric key algorithms such as Elliptic curve and Blowfish. The proposed method rectifies the issues related to data security. It provides more data security with high-speed data storage and retrieval in cloud computing. JKR Sastry et.al., introduced the new methodology to create multiple instances of DBMs located in multiple servers. However, it provides more security using double encryption with different keys and algorithms, which is to be applied by both the user, and CSP to ensure complete security [7]. Hence, the new model should be proposed to satisfy the requirements of security and also the privacy of the cloud users.

To secure cloud storage and control data dynamics, Sundar et.al (2022) introduced a novel model known as the Enhanced Cloud Security Model by utilizing Quantum Key Distribution Protocol (ECSM-QKDP). Quantum key cryptography is used. The first step makes use of BB84 QKDP, while the second phase frames Secure Authentication Protocol around distance boundaries and secure keys that are produced using Hierarchical Attribute-Set-based Encryption [8]. Using the model, the secured keys are sent to the LU via a reliable route.

To build a many-to-one mapping relationship between the key and the chaotic beginning value, conceal the original key of the cloud encryption system, and increase the security and randomness of the key system. Zhenlong Man et al. presented a new bidirectional activation (BA) neural network [9]. The M-semitensor product diffusion and a dynamic index scrambling-based encryption system for medical images are then suggested.

The current developments include Homomorphic encryption, Differential privacy, Zero Knowledge proof, Block chain and Multifactor Authentication, among other techniques related to confidentiality and authentication. The algorithm that is proposed in this paper allows

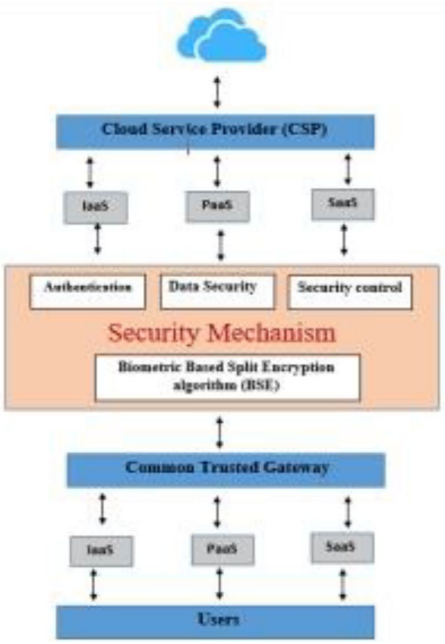

Fig. 1 Cloud security model for secured storage

both biometric authentication and split encryption for confidentiality.

Proposed Model for Cloud Security

Nowadays, the usage of cloud computing is increased due to its special feature such as anyone can access their data from anywhere through any devices with internet facility. The objective of this model is for enhancing the data security and authentication in cloud environment. The split encryption-based ABC (Artificial Bee Colony) algorithm is also utilized for enhancing the data security [10].

In addition, the biometric method is combined with proposed cloud security model for the purpose of authentication [11]. The proposed model is designed for satisfying two main objectives such as data security and authentication.

Initially, the cloud user needs to provide the sensitive data and also to register their finger print for the purpose of authentication. The data are taken as the input of split encryption process. The secret key (K) of encryption process is generated using optimization algorithm called ABC. In split encryption process, the given Plain text is applied into the split function. The result of split function is XOR with the secret key (K). Finally, the fingerprint is combined with the cipher text produced by XOR operation which can be stored into the cloud storage. This process is reversed in data retrieval from the cloud storage after the verification of biometric authentication. It is illustrated in Fig. 1.

All the data storage and retrieval can be done through the CSP (Cloud Service Provider). It has the responsibility to perform the biometric authentication. The finger impression of the authenticated person is collected and maintained at the time of data storage. The verification of biometric implemented at the time of data accessing from the cloud storage area. Before starting the process of data accession from the cloud storage, the CSP compares the thumb impression of the cloud user with the image of finger impression given at the time of data storage. If the match is found, the user is authenticated person and allowed to access the data from cloud storage. If the match is not found, the user is declared as unauthenticated user and not allowed to access the data.

The proposed model supports the following quality parameters:

- Confidentiality—split encryption and decryption process using the key generated by ABC algorithm.
- Authentication—biometric based authentication using finger print.

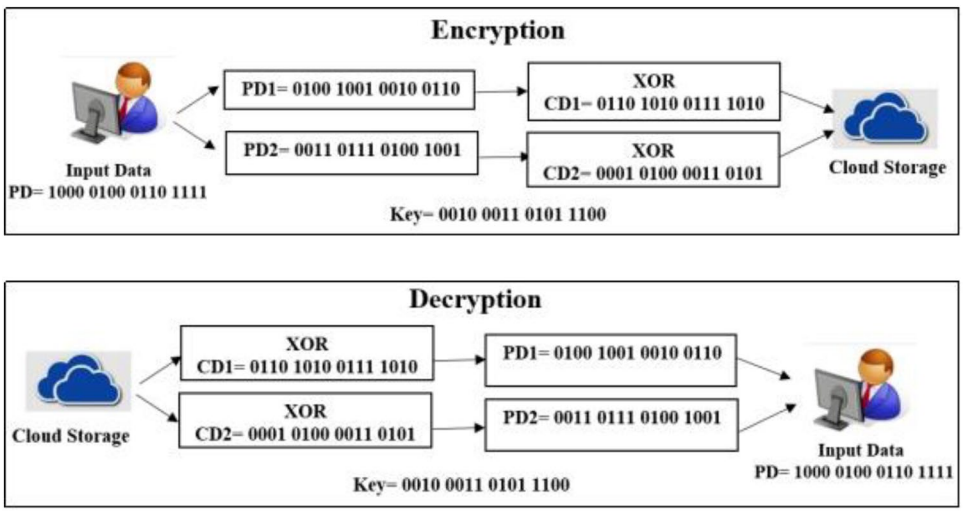

Fig. 2 Split encryption and decryption process

Algorithm: Data Encryption

Input: Plain text (PD)

Output: Cipher text with the image of finger print (CDI)

Step 1: Read plain text (PD)

Step2: Process of generating Secret Key(K) with the help of ABC algorithm

Step3: Split Data Encryption

(i) Decompose the Data into '2' blocks

PD1 and PD2 which satisfy the (PD=PD1+PD2)

(ii) CD1=PD1 xor K

CD2=PD2 xor K

Step4: Read the image of finger impression (FImg) of the user

Step5: Hide CD1 and CD2 into the image of finger impression (CDI)

Step6: The result CDI sends to the cloud Storage.

//**Encryption process - Final steps by CSP**

// Split the image of finger impression (FImg) and cipher test (CD1 and CD2)

// Image stored into authentication table

Algorithm: Data Decryption

Input: Image of Finger impression (FImg) and Cipher text (CD1 and CD2)

Output: Plain text (D)

// Decryption process - Initial steps by CSP

// Read the image of finger impression (FImg) from cloud user

// verify Authentication with the help of Authentication table

// Hide CD1 and CD2 within the finger print Image (CDI)

// The result CDI send to the user of public cloud

Step1: Decompose the image of finger impression (FImg) and cipher Text (CD1 and CD2)

Step2: Read CD1 and CD2

Step2: Split Data Decryption using secret key(K)

(i) PD1=CD1 xor K

PD2=CD2 xor K

(ii) PD=PD1 +PD2, PD1 and PD2 are combined together to produce the plain Text (PD)

Step4: Retrieve and display the plain Text(PD).

Fig. 3 Data encryption and decryption using BSE algorithm

- Access control—authorized user can perform to store and retrieve their own data.

Split Encryption and Decryption Process

The sensitive plain text, PD = 1000 0100 0110 1111 is to be applied into the split function. After applying split function, the plain text PD split into two parts PD1 = 0100 1001 0010 0110 and PD2 = 0011 0111 0100 1001. The random number provided by an optimization algorithm like ABC is considered to be the secret key(k). Like symmetric key cryptography, it is used for both encryption and decryption processes. The split plain text is XOR with the secret key value K = 0010 0011 0101 1100 generated by ABC.

CD1 = PD1 XOR K

CD2 = PD2 XOR K

The resultant cipher data (CD1 and CD2) are embedded with the finger print image of cloud user and stored into the cloud storage.

The same secret key K is used for both the cryptographic process such as encryption and decryption like symmetric key cryptography. In split decryption process, the extracted data from the cloud storage is XOR with the same secret key K = 0010 0011 0101 1100. The sum of the result of XOR operation is equivalent to our plain text R = 1100 1000 0011 1100. This process is described in Fig. 2.

Optimization Algorithm

Artificial Bee Colony algorithm (ABC) is an optimization algorithm which is developed based on the behavior of honey bees. It has been applied to resolve the several complex problems. The method of key generation is the essential part of security mechanisms [12]. For the purpose of security enhancement, ABC algorithm is used for key generation process. Based on the unpredictability of the key values, the security of an asymmetric algorithm can be evaluated. Public and private keys are generated using highly random values produced by the ABC algorithm. It will contribute in strengthening the proposed BSE (biometric-based split encryption algorithm) algorithm's security. The general description of ABC mentioned in this section.

The three types of bee such as employed, scout, and observer bee which are essential to the operation of the ABC algorithm. Half of the colony was occupied by the hired bees, and the other half was made up of spectator bees. A worker bee is responsible for utilizing the nectar sources and ensuring the quality of the food supply sites they are utilizing. When a worker bee communicated knowledge about a food source, the observer bees stayed within the hive. Scouts look for food at random locations based on internal drive or potential outside cues.by the scouts depend on the internal motivation or possible external clues.

Finding a nearby food supply is described by Eq. (1) in ABC

Algorithm 1 Psecudo code of Artificial Bee Colony Algorithm

```
Initial location of Food
Calculate the Amount of nectar
Repeat
Determine the chosen food sources around the neighbours by the employee bees
  Repeat
    Determine a neighbour of the selected food source through the onlooker
     Compute the amount of Nectar
     Selection process
    Until covered all the onlookers distributed
Remember the Location
Find the abandoned food
Find new positions for the unrestricted sources of food
New location considers as Random number
Until All criteria for terminating the process are satisfied
Finalize the positions of food
```

$$\upsilon_{ij} = X_{ij} + \Phi_{ij}\left(X_{ij} - X_{kj}\right). \tag{1}$$

A food source ti is determined by altering one of xi's parameters within the vicinity of each food source site represented by Xi, such as X1, X2, X3, etc. In Eq. (1), k is a randomly chosen index that must be different from i while j is a random integer in the range [1, D]. ϕij is a real number with uniform distribution [13, 14].

After calculating the value of vi within the boundaries, a fitness value for a minimization problem can be assigned to the solution by Eq. (2).

$$\text{Fitness}_i = \begin{cases} \dfrac{1}{1+f_i} & \text{if } f_i \geq 0 \\ 1 + \text{abs}\left(f_i\right) & \text{if } f_i < 0 \end{cases} \tag{2}$$

The algorithm steps of ABC illustrated in Fig. 3.

Biometric-Based Split Encryption Algorithm (BSE)

The proposed method consists of two important stages:

1. Biometric authentication,
2. Split data encryption and decryption using the key generated by ABC algorithm.

This method satisfies the principles of security such as confidentiality and also authentication. The pseudo code of the proposed method is illustrated in Fig. 3.

In data storage, the given plain text(PD) is encrypted using split data encryption method with the optimal symmetric key(K) generation done by ABC algorithm [15, 16]. The resultant cipher text CD1 and CD2 is embedded with the image of finger impression of cloud user [17] to produce the CDI (Image embedded Cipher text). In data retrieval, the CDI is separated as text and image which have been verified by the CSP. Finally, the split data decryption is applied using the same symmetric key(K) to get the final plain text(PD). The working principle of BSE is illustrated in following Fig. 4.

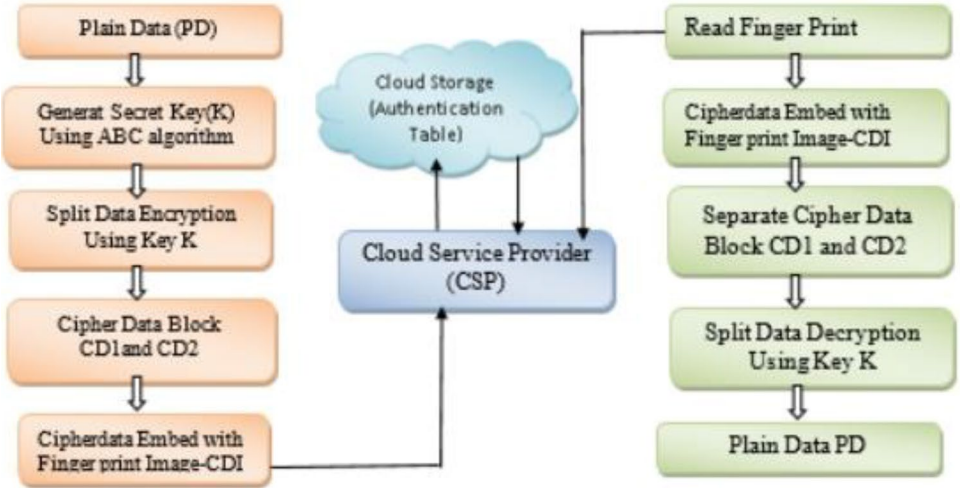

Fig. 4 Framework of BSE algorithm

In BSE, the data are being divided into two blocks PD1 and PD2. There is no restriction in data size. The number of blocks may be increased depends on the size of data.

Results and Discussion

The outcomes from the proposed model is being analyzed in this section. This algorithm is implemented by Java and analyze the performance using the PC with windows 11 operating system and 8 GB memory running with 64 bits adaptation. The total execution time and memory usage of the proposed algorithm (BSE) is measured through implementation as illustrated in Table 1.

In Table 1, whenever the data size is increased, the execution time and memory usage is also increased. The performance of the proposed algorithm is high due to symmetric key algorithm. In Symmetric cryptosystem, the size of plaintext and cipher text are same. Normally, the execution speed of symmetric key algorithm with minimum key size is better than the asymmetric key algorithm.

$$\text{Execution Time(ETi)} = \sum_{i=1}^{n} (\text{KTi, ETi, DTi}),$$

where '*i*' represents the session data $i = 1,2, \ldots n$

KT–key generation time.

ET–encryption time.

DT–decryption time.

The execution time is calculated for each data block separately and finally added together to arrive at the total execution time. The key generation time is also considered because the same key cannot be used for each session.

Table 1 Performance analysis of proposed algorithm

Data size (KB)	Memory usage (bytes)	Total execution time (ms)
10	12,752	34,283
20	23,483	45,971
30	34,795	58,312
40	26,349	80,505
50	62,078	90,212

The comparison of performance between the BSE algorithm and the existing algorithms is illustrated in Table 2 and Fig. 5.

In authentication-based encryption, the execution time is based on the total time needed for key generation, data encryption and decryption using Asymmetric key algorithm (RSA). It needed more execution time for Encryption and Decryption using RSA compare with other two algorithms [14]. In emperor penguin optimization (EPO) with Elliptic curve cryptography, the EPO used for generating the public key and private key of ECC. Additional time of execution involved key generation, Encryption and Decryption using Asymmetric key algorithm (ECC) [18, 19]. In the proposed

Table 2 Compare the execution time of BSE with the existing algorithm

Data size (KB)	Execution time (MS)		
	ABE	EPO with ECC	BSE
10	47,615	41,901	34,283
20	63,849	56,187	45,971
30	80,989	71,270	58,312
40	111,812	98,395	80,505
50	125,295	110,260	90,212

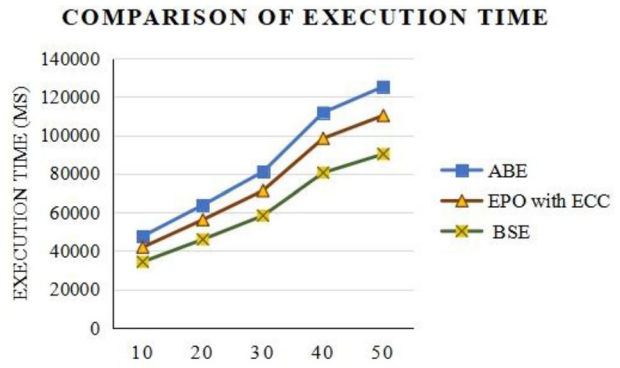

Fig. 5 Comparison of execution time

Table 3 Time comparison between BSE and existing methods for cloud data storage and retrieval

Data size (KB)	Data storage and retrieval time (ms)		
	ABE	EPO with ECC	BSE
10	51,242	41,901	40,994
20	67,800	56,187	54,240
30	85,897	71,270	68,718
40	115,004	98,395	92,003
50	128,996	110,260	103,197

model (BSE), the execution time is calculated based on Key generation using ABC algorithm, encryption and Decryption using Symmetric key method (Split Encryption process). In the comparison of above three algorithms, BSE needs minimum execution time with high level of security. The security and speed can be achieved using split encryption and decryption process using the same key which is generated by Artificial Bee Colony Algorithm.

The performance of cloud service [20] is measured by the level data security in the cloud storage, data retrieval only via authorized user and also the speed of data storage and retrieval in public cloud Hence, the time needed for data storage and retrieval using proposed algorithm is compared with the existing Algorithm and illustrated in Table 3. The graphical representation of comparison is as shown in Fig. 6.

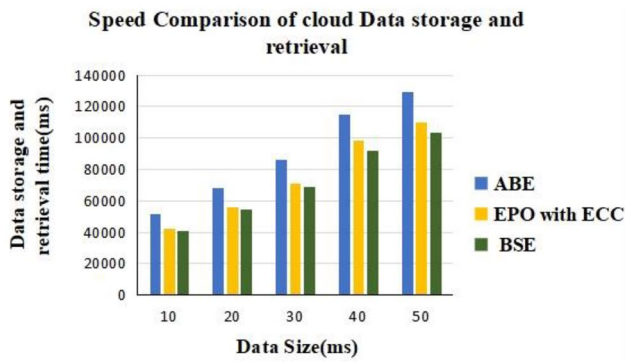

Fig. 6 Time comparison of data storage and retrieval

Conclusion

In this paper, ABC algorithm-based data security is developed in cloud environment. The level of security is enhanced with the utilization of ABC algorithm by key generation. There are two main security principles such as authentication and confidentiality are satisfied by the proposed BSE algorithm. The biometric approach is used to verify the authenticity of the user in cloud environment. The optimal key generation done using ABC algorithm and split encryption and decryption method helps to enhance the data security in cloud storage area. In general, highly protected systems require more time and memory space to provide encrypted data. The proposed method is implemented in Java and analyzed the performance using the metrics namely memory storage, encryption and decryption time. It can be used to store and retrieve the data with highly secured manner in cloud environment. It is achieved in BSE through methodologies such as the symmetric key cryptography (split Encryption and Decryption) and authentication (Biometric) The BSE algorithm is compared with the existing method ABE and EPO with ECC. Hence, it is conformed that the performance of the BSE algorithm provides better result and achieves security enhancement in Cloud computing. In future, the compression algorithm may be applied to reduce the size of image which helps to increase the data transmission speed to the cloud storage.

Declarations

Conflict of Interest We have no conflict of interest to declare. On behalf of all co-authors, the corresponding author shall bear full responsibility for the submission.

References

1. Wu X, Jiang R, Bhargave B. On the security of data access control for multiauthority cloud storage systems. IEEE Trans Serv Comput. 2015;10(2):258–72.
2. Fursan Thabit, Abdulrazzaq HA Al-Ahdal, Suir Jagtap, "A new Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing", Global Transaction Proceedings, 2021.
3. Patil R, Dudeja H, Modi C. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. Comput Secur. 2019;85:402–22.
4. Rahman MS, Khalil I, Alabdulatif A, Yi X. Privacy preserving service selection using fully homomorphic encryption

scheme on untrusted cloud service platform. Knowl-Based Syst. 2019;180:104–15.
5. Almoysheer N, Humayun M, Abd El-Aziz A, Jhanjhi NZ. Enhancing cloud data security using multilevel encryption techniques. Turk Online J Qual Inq. 2021;12:5140–54.
6. Li Y, Gai K, Qiu L, Qiu M, Zhao H. Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf Sci. 2017;387:103–15.
7. Chinnasamy P, Padmavathi S, Swathy R, Rakesh S. Efficient data security using hybrid cryptography on cloud computing. In: Inventive communication and computational technologies. Singapore: Springer; 2021. p. 537–47.
8. Sundar K, Sasikumar S, Jayakumar C. Enhanced cloud security model using QKDP (ECSM-QKDP) for advanced data security over cloud. Quantum Inform Process. 2022. https://doi.org/10.1007/s11128-022-03452-6.
9. Man Z, Li J, Di X, Zhang R, Li X, Sun X. Research on cloud data encryption algorithm based on bidirectional activation neural network panel. Inf Sci. 2023;622:629–65.
10. Sastry JKR, Trinath Basu M. Securing multi-tenancy systems through multi DB instances and multiple databases on different physical servers. Int J Electr Comput Eng (IJECE). 2019;9(2):1385–92. https://doi.org/10.11591/ijece.v9i2.pp1385-/.
11. Jhajharia S, Mishra S, Bali S. Public key cryptography using particle swarm optimization and genetic algorithm. Int J Adv Res Comput Sci Softw Eng. 2013;3(6):832–9.
12. Mohammad OKJ, Abbas S, Horbaty E-SME, Salem A-BM. A new trend of pseudo random number generation using QKD. Int J Comput Appl. 2014;96(3):13–7.
13. F.S.A.-Mouti, M.E.Elhawary, "Overview of artificial bee colony algorithm and its applications", IEEE International Conference–System Conference, PP 1–6, 2013.
14. Geetha JS, George Amalarethinam DI. ABCRNG—swarm intelligence in public key cryptography for random number generation. Int J Fuzzy Math Arch. 2015;6(2):177–86.
15. Geetha JS. Enhance the security of data storage and retrieval in cloud computing through authentication based encryption. Int J Recent Technol Eng (IJRTE). 2019. https://doi.org/10.35940/ijrte.D9802.118419.
16. Sunanda Nalajala, Pratyusha Ch, Meghana A, Phani Meghana B, "Data Security Using Multi Prime RSA in Cloud", International Journal of Recent Technology and Engineering (IJRTE), Vol.7, Iss. 6S, 2019
17. K Sarat Chand and B Kezia Rani, "Biometric Authentication using SaaS in Cloud Computing", Int Res J Eng Technol (IRJET), Vol. 05(02), 2018
18. Mohammad Saidur R, Khalil I, Alabdulatif A, Yi X. Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform. Knowl-Based Syst. 2019;180:104–15.
19. Mohana PK, Saraswathi PV. Suppressed K-anonymity multi-factor authentication based schmidt-samoa cryptography for privacy preserved data access in cloud computing. Comput Commun. 2020;158:85–94.
20. Mageto Stephen N, Balaji NV. Enhanced data security in cloud computing: survey. Int J Eng Technol Manag Sci. 2022;6:01–6.