Applied Nanoscience
https://doi.org/10.1007/s13204-021-02174-y

ORIGINAL ARTICLE

Secure data storage and retrieval system using hybridization of orthogonal knowledge swarm optimization and oblique cryptography algorithm in cloud

N. Madhusudhana Reddy[1] · G. Ramesh[2] · Srinivasa Babu Kasturi[3] · D. Sharmila[4] · G. Gopichand[5] · L. Thomas Robinson[6]

Received: 11 September 2021 / Accepted: 9 October 2021

Abstract
Distributed computing provides extensive storage capacity for customers to carry out their applications with no investment in infrastructure. As a result, many companies do their trade in the Public Space. For an instance to process the initial information set, many mediator information sets will be used for information exhaustive applications. However, protecting the protection of the intermediate information set is a difficult job. To solve this problem, numerous algorithms are implemented in the literature for retrieval problems. As a result, in my previous study, the optimal privacy protection of cloud-based data search was proposed using an oppositional cuckoo search and an ElGamal encryption algorithm. However, the downside is ElGamal, and the ciphertext is twice as long as the plain text. In addition, this algorithm is slower and necessary for randomness. To overcome the problem in this work, we propose the Optimum oblique Cryptography (OOCC) Algorithm for Encryption. In this, we primarily choose the equivalent node starting with and create the transitional dataset and apply the Opposition Cuckoo Search (OCS) algorithm. We choose confidential material from the intermediate information. We then encrypt sensitive data using the OECC algorithm. We now use an algorithm for orthogonal wisdom element optimization (OLPSO) for input generation. The information can be stored securely in the cloud after encoding; we recover the query dependent statistics securely from the cloud; performance of proposed effort on a variety of procedures, such as data transfer rate, encryption time, memory usage, and information thrashing.

Keywords Cloud service provider · Privacy-preserving · Encryption · Retrieval · Elliptical cryptography algorithm · Orthogonal learning · And storage system

Introduction

Cloud computing is the major and popular innovations both in IT companies and in R&D (Chengpeng 2011). This cloud computing (Xun 2012) ensures the representation of extensive computational management across the network and the introduction of compensate as use model. This cloud infrastructure will allow greater administration based on virtualized computing and storage technologies through next-generation data centers. Users are capable to way in cloud information and software wherever in the world on a compensate as use go financial method. In comparison, cloud computing (Armbrust et al. 2010) is used for computing possessions which are offered for system service. The name is derived beginning with the traditional utilize of a cloud produced representation as a concept for the composite transportation used in the

✉ G. Ramesh
ramesh680@gmail.com

1 Department of CSE, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, AP, India

2 Department of CSE, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, Telangana, India

3 Department of CSE, Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, Telangana, India

4 Department of Computer Application, Government Arts and Science College, Kanyakumari, Tamil Nadu, India

5 School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India

6 Department of Computer Science, Nanjil Catholic College of Arts and Science, Kaliyakkavilai, Kanyakumari, Tamil Nadu, India

Published online: 06 February 2022

organization representations (Bellare and Mihir 2000). Cloud Computing uses three different service models (Armbrust et al. 2010; Mather et al. 2009), named "Cloud Computing" as Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS). Cloud Computing classifies four operation representations are hybrid cloud, private cloud, open cloud, and Community Cloud.

All participants in cloud computing retail cuffs will gain from this new industry mock-up as they know how to focus on its own core business and growing its costs (Zhang et al. 2011). As a consequence, many individuals or businesses have brought their enterprise to cloud computing environments. Cloud computing causes challenges and countless chances at the same time. Security is built to be a crucial barrier to cloud computing on its path to success (Hassan and Qusay 2011). The security problems of the cloud computing approach are immense and very dynamic. The positioning of data in cloud computing security is a key factor in cloud computing security (Mell et al. 2011). One of the unique properties for cloud computing is location transparency, which is a security vulnerability at the same time without knowing the correct location of data storage, and the provision of a data protection act for certain countries may be severely affected and violated. The privacy of cloud users is therefore a critical threat in a cloud computing environment (Haghighat et al. 2015).

However, privacy issues and security will bring regarding during holding transitional information sets are indicated here (Adams et al. 2009). At risk of being compromised is the incidence of midway information sets cargo space increases the assault exterior, so that the creative information confidentiality may be verified. The midway information set store room may be unmanageable, and can be accessed and divided by other applications and the original data owner, considering an opponent to congregate & take a chance the confidential information to the creative information set, auxiliary contributing to extensive financial defeat. With the occurrence of cloud services, more and more sensitive data are being centrally into the cloud servers, photos, company financial information, government documents, and called as emails, personal health records, private videos, etc. (Hussein et al. 2016). To defend combat unsolicited accesses and data privacy, sensitive information has to be encrypted previous to sending data to another (Cloud Security Alliance 2017) to afford back-to-back data privacy pledge to beyond and cloud. Nevertheless, real fact operation is creating by data encryption of an extremely stimulating mission rendered that there will be enormous outsourced in sequence records. In cloud computing, Data owners become progressively outsource sensitive information in encrypted form from neighboring strategy to the public cloud for supplementary flexibility and economic savings (Tari et al. 2015). At many encryption algorithms are available such as ECC, AES, and Round robin etc.

The main aim of the projected approach is to secure the in order storage and improvement scheme by combining orthogonal element group optimization and an elliptical cryptography algorithm for the cloud. We can also use Elgamal Encryption Mechanism for Secure data storage in cloud. ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message. This cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know g^{a} and g^{k}, it is extremely difficult to compute g^{ak}. Here, we primarily produce a framework midway information set and find the matching node in the cloud using the OCS algorithm. Then, we find out all about sensitive information and non-sensitive information in the data analysis. We then encrypt the sensitive encryption using the Optimal ECC algorithm. In ECC, we use the OLPSO algorithm for the key generation process. We just encrypts critical data to reduce the expense of encryption and memory use in this article. Finally, we are going to retrieve the question relevant info.

The key purpose of proposed work is as follows:

- The projected model encrypts confidential data on the server part and provides protected encrypted information to the inspection supplier.
- During the inquiry scan, the customer must get back the top-n documents that are appropriate to the inquiry.
- The designed system offers multiuser authentication by registering with the manager
- Conserve confidentiality of encrypted information using a mixture of OLPSO and ECC.

The remaining sections are as follow: In the section "Related works", a brief overview of some of the literature on the security of privacy in intermediate dataset techniques is presented. The section "Back ground of the proposed research" addresses the background of the study. In the section "Proposed secure data retrieval system", a detailed overview of the projected approach is given. In the section "Results and discussion", the discussion on investigational outcome and routine assessment is given. Finally, in the section "Conclusion", the conclusion is illustrated.

Related works

A lot of researchers have residential stable data revival in a cloud surroundings. A number of the explore work are verified at this point. A cost-effective approach to storage and privacy preservation in the cloud environment was discovered by Ramachandran et al. (2014). The subscription model is expanded by Cloud computing, where Consumers pay purely for their use of resources. Numerous applications are now used in cloud computing. These have a large number of important midway outcomes for hypothetical applications. Whereas it is not a money-making approach to store up all intermediate information. Simultaneously, the multiple intermediates can be referred to by adversaries which outcomes in the stealing of knowledge. In the same way, encrypting any aspect of the intermediate results would increase the user's cost of computing. Providing a gainful solution for storage and isolation for outcome measures is the main support of the framework.

Ciphertext Policy characteristic-dependent Encryption is a capable technique for dealing with this safety Problem, for which the information owner can set up a control organization for encoding Information. Decryption is conceivable when client's impossibility of missing properties fulfills the entry control tree. In view of the quality of the clients, private keys for the clients will be made. Another viewpoint to be included in this framework is the main problem that a single external expert may interpret an encrypted data that may contain confidential data. To conquer this problem, Saikeerthana and Umamakeswari (2015) explained the encryption policy attribute of safe data storage and data retrieval. In this situation, the key generation for clients will be issued by a specific key age expert and the standard of clients will be supervised by the property management specialist. Along these lines, none of the experts can decipher the mystery data of the knowledge holder.

Deep learning gained lots of interest and productively linked in a number of fields, such as image processing, PC security, bioinformatics, image processing, entertainment, and so on. Then again, deep learning typically has a huge amount of preparation data that a sole proprietor could not provide. It is necessary for customers to stock up their information in an external cloud as the volume of information becomes overwhelming. Data are typically put away in an encoded form because of the confidentiality of the data. They have to deal with two difficulties in applying deep learning to available information sets own by different owners of cloud information: (i) The information is scrambled with diverse keys and they must be protected, counting moderate performance; and (ii) the information owner(s) should hold the computational costs and communication costs of the information negligible.

Consequently, the search for encrypted cloud papers using explanation words was explained by Keerthiga et al. (2015). Security enables a solution for safe ranked explanation words investigate over encrypted ambiguous information to be used in the information search scheme. Instead of submitting indifferent outcomes and additional ensuring the correctness of folder revival, prepared investigate significantly industrial methodology usability by enabling seek out consequence significance position.

The numerical determination method, i.e., the benefit in value from the retrieval of information, was explored to create a stable investigate catalog. Multiple information reserve map techniques have been maintained to better defend these critical achieve data. The approach has been enhanced to increase the value of active growth. The framework also provided verification of the findings of the investigation. One-to-many order preserving mapping approaches have also been improved in a reversible manner. Review of similarity technique was worn to recognize the query consequences for the cloud information storeroom.

Furthermore, the Safe and Interactive Multiindexes grade investigate systems over Encrypted Cloud information was described by Xia et al. (2015). Specifically, in the directory building and inquiry creation, the vector break method and the commonly used TF IDF reproduction were combined. They create an individual method, Tree dependent directory organization, and a "moderate Depth-first Search" algorithm to offer an accurate search for multi-keywords. To encrypt indexes and question vectors, the Safe *k-N* algorithm was used. Accurate calculation of the score between encrypted indexes and query vectors is thus ensured. Phantom words for blinding search results have been applied to the index vector to avoid mathematical attacks.

Ren et al. (2016) clarified a stable search for cloud storage enhancement with homomorphic indexing. This paper uses an exclusive or homomorphism encryption scheme to help protected keywords search scrambled information for distributed storage. In the first place, this plan describes another knowledge insurance policy by encoding the catchphrase and fastening the method conducting XOR process together an irregular piece sequence for every gathering to ensure contact design spillage; in the second place, the homomorphic assessment input empowers the search assessment to be ascertained on request, and then evacuates the dependence of input storage on cloud. This plan also reduces the spread of knowledge to the specialized co-op on the ground that the homomorphism-key system is more critical than that key stockpiling on cloud.

Background of the proposed research

We will first describe the algorithm worn in this work. Later part will discusses about the projected Scheme.

Particle swarm optimization

The universal Optimization Approach is a Particle Swarm Optimization (PSO) algorithm (Parameswari et al. 2021; Ramesh 2020a); global optimization is a group intellect (Ramesh 2020b) algorithm that simulates swarm behaviors such as bird flock and angle training. It is a population-based iterative learning algorithm that assigns certain typical features to other evolutionary computing algorithms (Ramesh 2020c).

On the other hand, PSO is searching for a most favorable for every element flying to adjust its flying trajectory and the search space, enabling its unique most excellent understanding its neighborhood, rather than from beginning to end particles undergoing genetic operations such as collection, crossover, and transformation (Ramesh 2020d). Thanks for its elevated degree of competence and ease of idea, PSO has proved to be an extensively accepted optimization method which is effectively useful to a lot of real-time troubles. In ordinary PSO, every entity in the group is considered as an element in the Swarm. As a particle in a D directional investigate break, & verified by 3 tuple $\{X_i, V_i, P_i\}$. $X_i = (x_{i1}, x_{i2}, ..., x_{iD})$ and $V_i = (v_{i1}, v_{i2}, ..., v_{iD})$ depicted the location and speed of the particle i, correspondingly. $P_i = (p_{i1}, p_{i2}, ..., p_{iD})$ signifies the personal best (p best) of element i. $G = (g_1, g_2, ..., g_D)$. To depict the universal greatest which was, the maximum situation follow by whole collection? The worth of every constituent in the vector V_i can be blocked the choice of $[-v_{\max}, v_{\max}]$ to manage the need less roving of constituent part exterior the seek out freedom and shown in one reference (Adams et al. 2009)

$$v_{id}(t+1) = \omega\, v_{id}(t) + c_1 r_1[x_{id}(t) - p_{id}(t)] + c_2 r_2[x_{id}(t) - g_d(t)], \quad (1)$$

wherever $i = 1, 2, \ldots, M$ suggests the numeral of element and the dimension of elements is $d = 1, 2, ..., D.r_1$ and r_2 are evenly assigned arbitrary numeral whose variety is [0, 1]. c_1 and c_2 are knowledge factor [0.1]. ω is the inertia load [0.1] to stay away as of the unrestricted expansion of particle's rapidity.

The element flies in the direction of an original location according to (2), and every worth of the original location (Haghighat et al. 2015) be supposed not go ahead of the choice of [min X, max X]

$$x_{id}(t+1) = x_{id}(t) + v_{id}(t+1). \quad (2)$$

At the commencement, the place and quickness of every element in the swarm are started randomly. After that, each element is directed by finest element and its own flying practice (pbest), i.e., modified by (1) and (1) (2). This process is recurring in anticipation of a discontinue standard established by the consumer is achieved.

Algorithm 3.1: Determination of fitness function

Step 1: Initialize the location and quickness of every element at random.

Step 2: Determine fitness values of every element; The pbest of every element be its existing position; let gbest be the finest lone of every element.

Step 3: revise the swiftness and situation of every element using (1) and (2).

Phase 4: The fitness significance of every element is determined.

Step 5: Pbest modernize. For every element, if its latest situation fitness value is better than that of its pbest, next alternate the latest location with its pbest.

Step 6: Revise gbest. If the robustness charge of its latest location is better to that of the gbest for each particle, then substitute the gbest with gbest.

Step 7: If the end customary is fulfilled, then result gbest and its strength worth; or else, Proceed to Step 3.

OLPSO

With an effective and promising exemplary approach, the OL strategy will guide the particles in better direction. The OL strategy uses PSO for every topological structure. For example, provide a 3-dimensional Sphere function with [0, 0, and 0] as the global minimum point. Presuming that the current position is = [2, 5, 2], its best personal position is = [0, 2, 5] and the best position of its neighborhood is = [6, 1, 2]. The revised quickness of T = [2, − 7, 1] allows for (Ramesh 2021), and thus, the latest location is = [4, − 4, 3], followed to new location with a charge worth of 29 that is lower compared to Xi and Pi. For consequence, the observation from and within this century does not support the particle. On the other hand, vectors in their structures and definitely acquire good knowledge.

For e.g., if we can decide the two vectors' good dimensions, we preserve and unite them to shape a new supervision vector of = [0, 0, and 1] from which the first coordinate 0 originates.P_i even as the 2nd and the 3rd harmonize 1 and 0 move toward as of P_n. Afforded the management of P_o, the improved quickness roll away to be $V_i = P_o + X_i$ = [1,

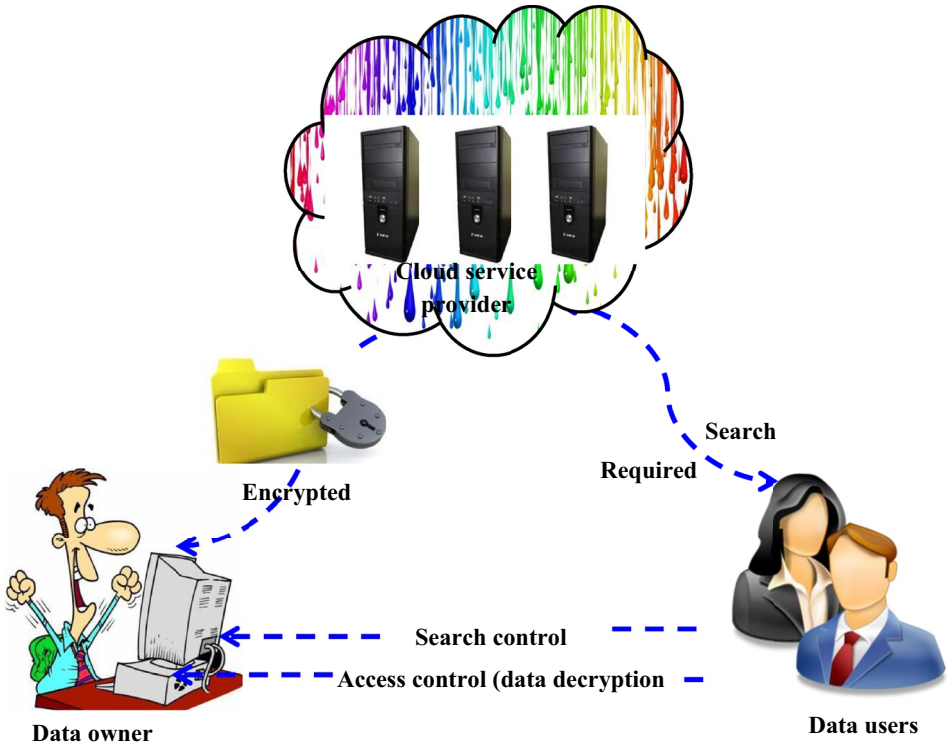

Fig. 1 Retrieval system in cloud

1, 0] − [4, 6, 3] = [− 3, − 5, − 3]; hence, the latest location is $X_i = X_i + V_i$ = [1, 1, 0], consequential for novel and superior location with a price $f(X) = 1$ which develops the element flutter closer on the way to the comprehensive optimum [1, 1, 0].

System model

The quest scenario and recovery of encrypted information in the cloud is illustrated in Fig. 1. The structure consists basically of 3 individuals, for example the data owner (DO), the data user (DU), & the cloud service provider (CSP). The data owner has collected a dataset D, however, with different details. The data owner has compiled a D dataset with various information forms. It is difficult to handle large datasets; the data owner thus generates a middle data set. DO then distinguishes the relevant data from the non-sensitive data collection.

The confidential data selected would then be encrypted with the encryption algorithm. In the cloud service provider are also stored the encrypted files (CSP).All sensible files stored on the CSP in encrypted formats after the above processes have been completed. It can be decrypted only by the DU. The CSP or a third party should not have information leakage. Typically, the DU can retrieve CSP files relevant to the query. First of all, a DU will submit the CSP query. Here, the DU information is sent to the DO by the CSP. The DO will enquire for user id and signature when the authentication success is achieved; the DO sends the decryption key toward DU and CSP forwards the question linked top-n-encrypted file to DU. If user identity is not authenticated, the application is ignored.

Proposed secure data retrieval system

The major purpose of the projected work is to safeguard data storage & to recover data from the cloud over many stages. Confidentiality is one of the greatest challenges to the cloud, as cloud consumers can accumulate a vast quantity of production data in the cloud. This occurrence has contributed to the development of various organizations or alliances in the cloud. However, due to privacy protection issues, many potential clients are still hesitant to take advantage of the club. We provide cloud storage data with confidentiality in this job. The paper consists of 4 phases such as (i) transitional records set generation, (ii) finest join collection support on OCS selection, (iii) finest ECC dependent encryption, and (iv) reservation-based information revival and selecting sensitive data. The general diagram for the proposed scheme to privacy conservation is shown in Fig. 2.

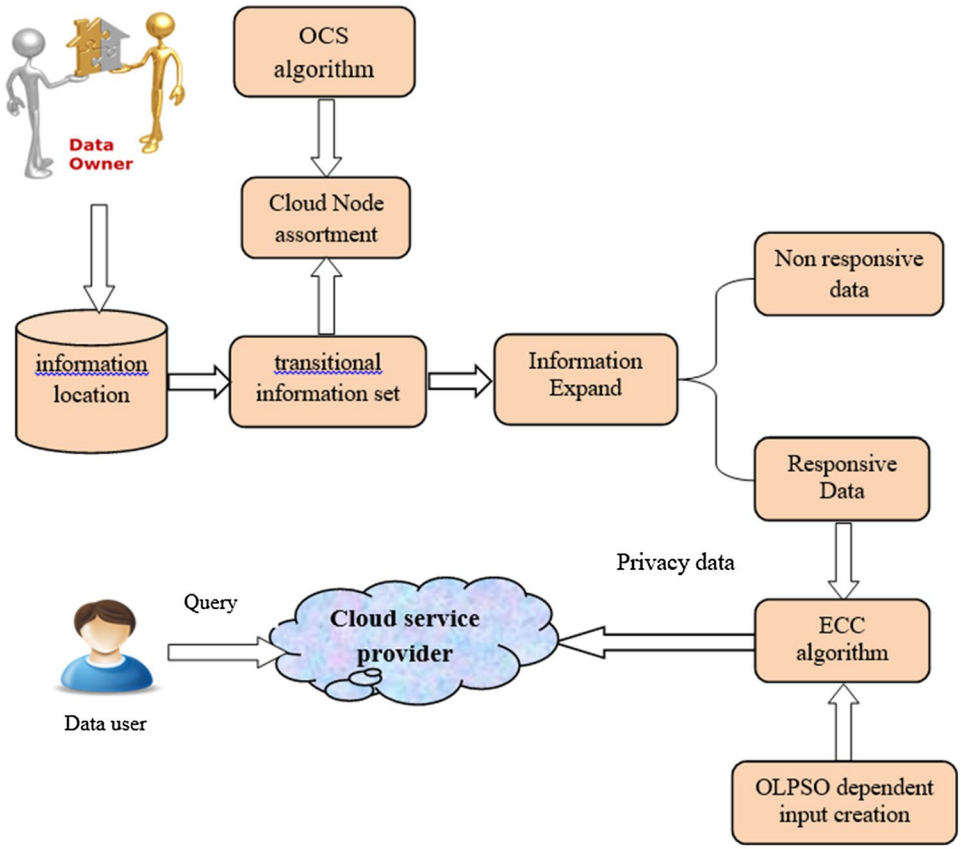

Fig. 2 Projected methodology

Optimal node selection based on OCS module

Cloud computing is a combination of a wide range of technologies to provide an IT service business model. Customers will save on their IT technology investment; many businesses integrate all their business into the cloud. At the same time, many consumers do not use cloud services, since they are concerned about safety and privacy, because privacy issues and intermediate data sets are very relevant in the cloud. Take into consideration the input dataset with N attributes and S record number. We are splitting the original data set into many intermediate data sets that have been generated for the purpose of privacy. The intermediate dataset is then stored in the corresponding CSP node. There are numerous descriptors in of node here. One of the important issues is fixing the intermediate dataset in the corresponding node. Therefore, with OCS algorithm, we optimally pick the node. The most significant characteristic of transitional information is that it would be generated if we are aware of its origin. Information from effort flows are a type of essential metadata in which the addiction connecting information sets are documented. The data origin is particularly important, since some intermediate datasets were deleted after performance, but scientists often had to create them for re-use or re-analysis. The source of data is used for management in our research of intermediate data sets and we take it for granted that the data recorded are used to create relationships in data sets generation.

Responsive information selection based on information gain module

We assess the insensitive information and receptive information toward the after the intermediate information set is selected. It is neither competent nor cost-effective for encrypting all the transitional information sets, and instance consuming. In this paper, we therefore only encrypt confidential data that can reduce the cost of maintaining privacy compared to previous approaches; it is useful for cloud users. We use the information gain formulation to pick the sensitive data before encryption.

The information expand *IG* is considered established on Eq. (3)

$$\mathrm{IG} = \mathrm{Entropy}\ \ (\mathrm{parent}) - \left[\mathrm{average\ entropy}\ \ (\mathrm{children})\right]. \tag{3}$$

We fix an entry charge after the information process and break the information into responsive and non-responsive data. Afterward, the confidential information is chosen for encryption. Find a basic example of knowledge gain in computing. Process step by step.

In this section, each data entropy is calculated first and the information gain is then calculated.

Finally, we give the sensitive and non-sensitive information a threshold value that was calculated at the threshold. The calculation of entropy is as follows:

$$\text{Entropy} = \sum_{i} -P_i \log_2 P_i, \tag{4}$$

where, P_i is the Likelihood of set i.

Subsequently, we measure the data expand of every knowledge. Here, we compute which is most useful for processing to allocate in an afforded data set. Gaining data show us the key feature vectors of a given attribute. We use it to evaluate the categorization of ascriptions in the resolution tree node.

The in sequence grow IG is considered established is shown below (5)

$$\text{IG} = \text{Entropy (parent)} - \left[\text{average entropy (children)}\right]. \tag{5}$$

We fix a maximum charge after the information process and break the information into responsive and non-responsive data. Afterward, for the encryption method, we pick the sensitive data. Let us conceive of a simple instance of calculating the gain of knowledge. The method is illustrated below.

Phase 1 Consider the information set with the three characteristics and one of the two classes.

Step 2 If X is the finest element, this node is further separated by the best attribute (Fig. 3).

Table 1 Sample information set

X	Y	Z	C
0	0	0	X
0	0	1	X
1	1	0	Y
0	1	1	Y

Step 3 We measure the gain cost of the complete quality available to the trial information set given in Table 1. On the basis of step 2.

Step 4 We correct one threshold value after the information process, depending on the Maximum price, breaks the information into responsive or not. If the IG acquire is higher than the Maximum, the information is responsive; otherwise, the information is non-responsive. Afterward, for the encryption method, we choose the sensitive data.

Optimal elliptic curve cryptography (OECC)

After the sensitive data identification, we have to encrypt the sensitive data, so that while reducing the execution time and privacy-preserving cost. For encryption, we suggested an optimal elliptic curve cryptography (OECC) algorithm by this paper.

In the ECC algorithm proposed, the main values are optimally selected and the orthogonal learning element group optimization algorithm is useful (OLPSO). By the ECC process, the private and public keys are established, making the encrypted data safer. The general elliptic curve equation is given below

$$y^2 = x^3 + ax + b. \tag{6}$$

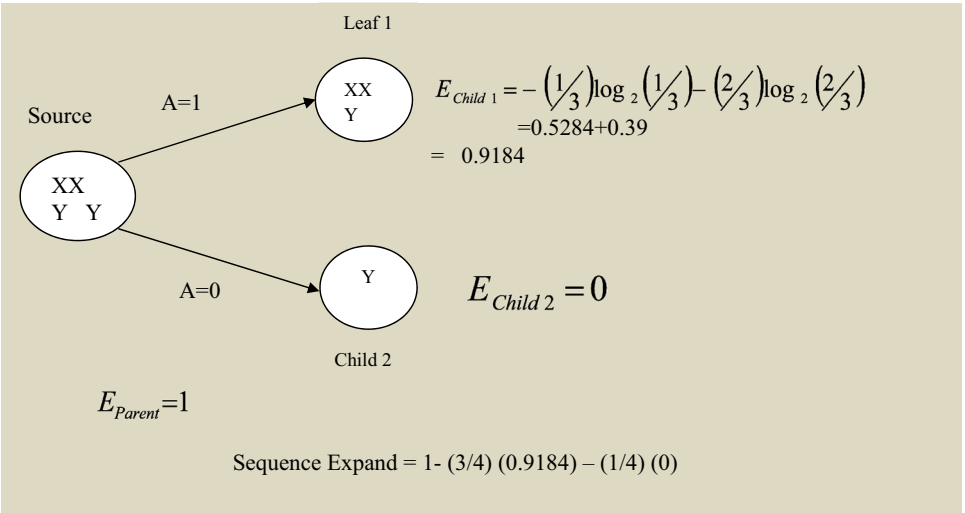

Fig. 3 Procedure of in order achievement calculation

As we need part of key generation and both community input and confidential input to be generated. The correspondent will use the recipient community key to encrypt the message and the recipient will decrypt his private key. Underneath the primary generation and structure are clarified.

Key generation by ECC

Two predetermined fields clarify the operations of elliptic curve cryptography: the main field and the binary field. The right field with finitely large numbers of points is chosen for cryptographic operations. Major Field procedures pick the prime quantity and finitely great information of fundamental position are generated on the elliptic curve

$$\mathrm{pu_{ky}} = r \times P, \tag{7}$$

where r is the random values, P is the point of the curve, and $\mathrm{pu_{ky}}$ is the public key.

Here, we optimally choose the r standards established on the optimization method. Here, OLPSO algorithm is applied to choose these standards.

OLPSO-based key generation

A crucial element is an input generation wherever we include to give both community key and confidential key. As we optimally choose, the random value R is present in the input for the section.

- **Resolution initialization**

In optimization algorithm, solution initialization is a crucial procedure. The solution is to produce established on the random value R. We arbitrarily dispersed preliminary solution at first. The random value R comprises of only the prime records

$$S_i = P_i \ (i = 1, 2, \ldots t). \tag{8}$$

- **Robustness computation**

Assess the fitness function based on the equation subsequent to that chooses the finest one

$$\text{fitness} = \max \text{ key breaking time}. \tag{9}$$

- **Updation using OLPSO stage**

Based on (10) and (11), Particles update their speeds and positions. The original PSO can be updated when applying the policy as an OLPSO that associates data with and forms a better guidance vector. The inventive PSO will be modified as a CPSO using an OL method which adhere data from and to outline a raised supervision vector. The flying speed of the element is thus altered as

$$V_i^{\mathrm{d}}(t\_1) = \omega V_i^{\mathrm{d}} + cr_{\mathrm{d}}(P_{\mathrm{od}} - X_i^{\mathrm{d}}), \tag{10}$$

$$X_i^{\mathrm{d}}(t+1) = X_i^{\mathrm{d}} + V_i^{\mathrm{d}}, \tag{11}$$

where ω is the inactivity heaviness, c is the arbitrarily chosen cost which is predetermined as 1.99, r_{d} is the arbitrary charge constantly produced within intermission [0, 1], V_i^{d} is the Speed of ith element, X_i^{d} is the present place of the element i, and P_o is the supervision vector.The supervision vector P_o was used to create every particle i, likewise, beginning P_i and P_n as

$$P_o = P_i \oplus P_n, \tag{12}$$

where P_i is the Individual finest location, P_n is the Neighborhood's finest location, and $\oplus$is the stands for supportive process.

- **Preservation criterion**

The algorithm will terminate its implementation when if a greatest amount of iterations is attained and the resolution which shares the finest fitness significance is chosen and this value is attributed to the random value.

Encryption and decryption

As we have to inscribe the information for the optimal key selection process. The contribution communication is inscribed and the productivity is categorized into two cipher text as C_1 and C_2

$$C_1 = O_{\mathrm{m}} \times P, \tag{13}$$

$$C_2 = E_{\mathrm{M}} + O_{\mathrm{m}} \times P. \tag{14}$$

The O_{m} indicates the novel maximized major cost in Eq. (13). This encrypted communication C_1 and C_2 is sent to the recipient. After getting the ciphertext, the recipient encrypts the communication applying the subsequent equations

$$M = C_2 - r \times C_1. \tag{15}$$

The pseudo-code for OECC encryption algorithm is explained as follows:

pseudo code for OECC encryption

preliminary significance: The universal elliptic curve is represented as

$y^2 = x^3 + ax + b$

1. Key Generation

Input:choose the arbitrary prime records.

Output: Public key (pu_{ky}) and private key (r).

Procedure:

- Choose the arbitrarynumeral (r)

// Here the random number is optimally selected by cuckoo search

Steps for cuckoo search

Input: Arbitrary prime numbers

Output: Most favorable private key (O_m)

Begin

Generate initial population of particles (P_i where i=1, 2,…t)

Evaluate the fitness by using equation (9)

Repeat

For (i=1,2,….n)

Find out the individualfinestlocation P_i

Find the localityfinestsituationP_n

Calculate the guidance vector P_o using Eq.12

Revise the quicknessby means ofEq. 10

Revise the locationby means of Eq.11

end

- Produce the communityinput $pu_{ky} = r * P$

r- Arbitrary values

P- Point to arc

pu_{ky} - Communityinput

2. Encryption

Input: message C

Output: Ciphertext C_1 and C_2.

Procedure:

- Obtain the text C.
- Compute ciphertext by splitting two message (C_1 and C_2),

$C_1 = O_m * P$

$C_2 = E_M + O_m * P$

O_m Represent the innovative optimized prime charge.

(E_M=C) represent the encrypted message

3. Decryption

Input: Ciphertext C_1 and C_2.

Output: Plaintext message M.

Procedure:

- Get the ciphertext C_1 and C_2.
- Estimate plaintext,

$M = C_2 - r * C_1$

Query-based retrieval module

After the storage system, we have to retrieve the query-based data. In this, data user (DU) forwards the request to the CSP. Immediately, CSP send the DU information this to owner. DO check the authentication process. If the verification is success, the Server informs the encrypted file for customer and after that customer decrypts the file by means of the private input sent by administrator. If the user id is not verified, then the request is ignored.

Results and discussion

Performance of the Projected Method is inspected in this segment. We are using JDK 1.7.0 in a windows device which consists of Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM, and the O.S is Microsoft Window 7 is implemented by suggested system using Census-Income (KDD), the suggested work is examined (Ramesh 2021) dataset which is commonly applied information set in the confidentiality investigation population.

Dataset description

In this experiment, we implemented the Census-Income (KDD) (Ramesh 2021) information set. In this data set, 299,285 reports and 40 features are included. This information set is a population survey performed by the U.S. in 1994 and 1995. This dataset was usually used to test Anonymization calculations as an accepted benchmark. The Adult Data Set subset has been widely used to test anonymization algorithms as a de facto benchmark. By deleting records containing missing values and granting enormously warped distributions, the data set is sanitized. With 153,926 documents, we found a sanitized data collection, from which information sets are sampled in the subsequent experimentation. Of the initial 40 assignments, 12 are chosen, including 10 quasi-identifier and 4 (3 arithmetical and 2 definite) responsive assignments.

Performance analysis

The fundamental scheme of our investigation is to protect the data storage and retrieval System by hybridizing the optimization of orthogonal learning particle swarm and elliptical algorithm of cryptography. The proposed scheme focuses primarily on two important contributions.

The first is secure storage of data and the second is retrieval. Here, we first break the data set into a variety of intermediate datasets for stable data storage. Then, using the oppositional cuckoo search algorithm, we choose the appropriate node from the CSP (OCS). Then, using the data gain calculation, we pick the critical data from the intermediate data. After that, we encrypt confidential data, because it is cost-effective and time consuming to encrypt all datasets. The encrypted files are saved in the CSP after that. Then, the question is sent to the CSP by the user. The data owners check the details of the user and give the user the decryption key. Finally, the CSP sends the documents associated with the query to the recipient. Here, we analyze the performance based on encryption instance, information transmit speed, information failure, and memory convention.

Table 2 Encryption time and memory convention for a variety of Entrance principles

Threshold	Encryption instance	Memory
0.3	4384	4625572
0.6	4263	4526448
0.9	3995	4431155
0.12	3917	4233545

Table 3 Encryption time and memory convention for a variety of file volumes

File volume	Encryption instance	Memory
12 kb	3045	3011125
24 kb	4263	4326448
36 kb	4692	4639281
48 kb	5015	4788245

This segment describes thoroughly the efficiency of our proposed solution. As stated by the investigation, the encryption instance increases regularly as the threshold charge decreases, as shown in Table 2, Encryption instance and memory utilize for dissimilar threshold values. When the maximum charge is 0.12, the encryption moment is low; similarly, when the threshold charge is 0.3, the encryption time is high. In addition, the identical board also displays the Remembrance use of a threshold charge that differs. It illustrates that when the maximum charge is high, the memory utilization is low; similarly, the memory usage is elevated when using small threshold charge fixing. It displays the encryption point and memory consumption for different volume of records when considering Table 3. The encryption instance increases as the size of the file continues to grow, according to the report. Similarly, as the file size continues to increase, memory consumption increases.

Comparative analysis

In this section, our projected method is compared with various optimization methods based on encryption and without optimization algorithm-based encryption. The comparative result of the privacy preservation on the intermediate dataset is shown in Tables 4, 5, 6, and 7.

Table 4 Proportional analysis depended on memory and encryption instance by unstable threshold

Threshold	Encryption memory				Encryption time (ms)			
	OLPSO	Elagamal	PSO	Without optimization	OLPSO	Elagamal	PSO	Without optimization
0.2	3625572	5645142	3854563	3944674	4384	5849	4562	4446
0.4	3526448	5118746	3723618	3865485	4263	5346	4436	4365
0.6	3431155	4975125	3622487	3822154	3995	5007	4264	4012
0.8	3233545	4638441	3522567	3714485	3917	4916	4153	3966

Table 5 Proportional analysis depended on memory and encryption instance by changeable file size

Record size	Encryption instance (ms)				Encryption memory			
	Without optimization	PSO	Elagamal	OLPSO	Without optimization	PSO	Elagamal	OLPSO
10 kb	4253	4386	3548	3045	4649454	4578787	3178754	3011125
20 kb	4365	4436	4763	4263	4865485	4723618	4479611	4326448
30 kb	4747	4968	5567	4692	4954875	4799935	4781246	4639281
40 kb	5159	5239	6147	5015	5066859	4850154	4854194	4788245

Table 6 Proportional analysis depended on information transmit time and information failure by changeable threshold

Threshold	Information transmit time			Information failure		
	Without optimization	CS	OCS	Without optimization	CS	OCS
0.3	4.258	3.42	3.39	0.6443	0.5489	0.4325
0.6	4.125	3.26	3.25	0.6345	0.5348	0.4217
0.9	4.025	3.15	3.15	0.6245	0.5286	0.4206
0.12	3.958	3.02	3.07	0.6008	0.5825	0.4125

Table 7 Proportional analysis depended on information transmit speed and information failure by change able records volume

File size	Information transmit speed			Information failure		
	Without optimization	CS	OCS	Without optimization	CS	OCS
12	2.936	3.86	4.53	0.5698	0.5249	0.4586
24	3.115	3.53	4.12	0.4256	0.5149	0.4568
36	2.865	3.48	4.06	0.4129	0.5264	0.4256
48	2.568	3.12	4.03	0.5268	0.4368	0.4212

The comparative results based on encryption time and memory are shown in Table 4. We used the OLPSO + ECC algorithm in this document for encryption. The main aim of the OLPSO algorithm is to decide the most excellent private key for the ECC algorithm. We should encrypt all the information accessible in the dataset for privacy preservation. The time and expense of the system proposed could be increased. To avoid this issue, we encrypt only sensitive information in this document. The minimum encryption time of 2616 ms, which is 4268 ms for the use of ECC + PSO support encryption and 3966 ms for the use of ECC supported Encryption, is achieved by our suggested solution (OLPSO + ECC) when evaluating Table 4. Similarly, the proposed encryption method's memory consumption is 3233545, which is very poor compared to other approaches. In addition, Table 5 illustrates the comparative result by varying file size depending on encryption time and memory. Our suggested strategy here achieves a smallest amount of encryption period of 3989 ms, which is 4985 ms for ECC + PSO & 51,599 ms for ECC + PSO. EEC-dependent encryption. We clearly observed the findings that our projected solution accomplishes the least amount time for encryption relative to other research work. In addition, the performance

relation depended on information transmit speed and information failure by changeable thresholds is shown in Table 6. The suggested solution attains a smallest amount transmit speed of 2.17 when evaluating Table 6, which is 2.96 for use without data transfer based on optimization and 2.48 for using data transfer based on CS. In addition, the minimum data loss of 0.3125 is achieved by our proposed solution, which is 0.4253 for use exclusive of an optimization support advance and 0.4253 for CS dependent information transport. Likewise, Table 7 demonstrates the assessment of results depended on information transport speed & failure of information by unreliable file volume. The least information transport speed of 3.15 is obtained by our proposed solution, which is an enhanced consequence compared to the remaining two methods. The implication is that our proposed plan produces a better outcome relative to other methods.

Conclusion

In this work, we have projected an efficient method that distinguish which element of transitional information deposit wants to be encrypted while the remaining may not, to accumulate confidentiality and preserve costs and instance. The intended technique is implemented in the cloud sim with the support of the JAVA platform. Due to vulnerable, optimal encryption method, the confidentiality of projected technique is derived directly. The advantage of projected approach is that the further exterior aggressor is unable to produce valid signatures or authenticate the valid messages. The cloud server does not know the corresponding owner's hidden info. Based on encryption, memory use, encryption, data loss, and data transfer rate, the efficiency of the proposed method is assessed. In the cloud system, our proposed safe data retrieval, OLPSO + ECC encryption algorithm provides a successful result compared to other algorithms. These protection mechanisms can be improved in the future to provide high-level security in data storage and data sharing.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

Adams I, Long DDE, Miller EL, Pasupathy S, Storer MW (2009) Maximizing efficiency by trading storage for computation. In: Proc. of workshop on hot topics in cloud computing, pp 1–5

Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M (2010) A view of cloud computing. Commun ACM 53(4):50–58

Bellare M, Boldyreva A (2000) Public-key encryption in a multi-user setting: security proofs and improvements. Springer, Berlin

Cloud Security Alliance (2017) Security guidance for critical areas of focusin cloud computing. http://www.cloudsecurityalliance.org. http://archive.opengroup.org/public/member/proceedings/q309/q309a/Pre

Haghighat M, Zonouz S, Abdel-Mottaleb M (2015) cloudID: trustworthy cloud-based and cross-enterprise biometric identification. Expert Syst Appl 42(21):7905–7916

Hassan and Qusay (2011) Demystifying cloud computing. J Defense Softw Eng CrossTalk 16–21

Hussein NH, Khalid A, Khanfar K (2016) A survey of cryptography cloud storage techniques. Int J Comput Sci Mob Comput 5(2):186–191

Keerthiga S, Savitha Karpagam S, Sathish Kumar TM (2015) Searching on encrypted cloud documents using keywords. Int J Innov Res Comput Commun Eng 3(5):4379–4384

Mather T, Kumaraswamy S, Latif S (2009) Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media Inc, Newton

Mell P, Grance T (2011) The NIST definition of cloud computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce

Parameswari DVL, Rao CM, Kalyani D et al (2021) Mining images of high spatial resolution in agricultural environments. Appl Nanosci. https://doi.org/10.1007/s13204-021-01969-3

Ramachandran S, Chithan S, Ravindran S (2014) A cost-effective approach towards storage and privacy preserving for intermediate sets in cloud environment. In: International conference on, 2014

Ramesh G (2020) A survey on NLP based text summarization for summarizing product reviews. In: 2020 second international conference on inventive research in computing applications (ICIRCA), Coimbatore, India, 2020, pp 352–356. https://doi.org/10.1109/ICIRCA48905.2020.9183355

Ramesh G (2020c) Detection of plant diseases by analyzing the texture of leaf using ANN classifier. Int J Adv Sci Technol 29(8s):1656–1664

Ramesh G (2020d) Data Storage in Cloud Using Key-Policy Attribute-Based Temporary Keyword Search Scheme (KP-ABTKS). Lect Notes Netw Syst 98:630–636

Ramesh G (2021) A machine learning-based IoT for providing an intrusion detection system for security. Microprocess Microsyst 82:103741

Ramesh G (2020) A survey on hybrid machine translation. In: 2nd International conference on design and manufacturing aspects for sustainable energy (ICMED 2020), vol 184

Ren SQ, Tan BH, Sundaram S, Wang T, Ng Y, Chang V, Aung KM (2016) Secure searching on cloud storage enhanced by homomorphic indexing. J Future Gener Comput Syst 65:102–110

Saikeerthana R, Umamakeswari A (2015) Secure data storage and data retrieval in cloud storage using cipher policy attribute based encryption. Indian J Sci Technol 8:318–325

Tari Z, Yi X, Premarathne US (2015) Security and privacy in cloud computing: vision, trends, and challenges. J IEEE Cloud Comput 2(2):30–38

Wu C, Yao J, Songjie (2011) Cloud computing and its key techniques. Electron Mech Eng Inf Technol 1:320–324

Xia Z, Wang X, Sun X, Wang Q (2015) A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parallel Distrib Syst 27(2):340–352

Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 28(1):75–86

Zhang X, Liu C, Chen J (2011) An upper-bound control approach for cost-effective privacy protection of intermediate dataset storage in cloud. IEEE