Research Article

An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol

Dheresh Soni (1), Deepak Srivastava (2), Ashutosh Bhatt (3), Ambika Aggarwal (4), Sunil Kumar (4), and Mohd Asif Shah (5)

1 VIT Bhopal University, Bhopal, Madhya Pradesh, India
2 Department of Computer and Information Sciences, Himalayan School of Science & Technology, Swami Rama Himalayan University, Dehradun, India
3 Department of Computer Science and Engineering, Shivalik College of Engineering, Dehradun, India
4 School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
5 Bakhtar University, Kabul, Afghanistan

Correspondence should be addressed to Mohd Asif Shah; econbu@bakhtar.edu.af

Received 13 June 2022; Revised 14 August 2022; Accepted 24 August 2022; Published 21 September 2022

Academic Editor: Said El Kafhali

Copyright © 2022 Dheresh Soni et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cloud computing is a technology that provides resources and utility services based on user demand. Due to this demand, efficient cloud security protocols are highly required, especially at the time of data communication for user authentication and data aggregation. This article provides a practical approach to developing an efficient and empirical cloud framework in terms of cloud protocol. The framework uses fuzzy c-means (FCM) algorithm to group data, and calculation is done individually or associatively to rank the text data. Uploaded data are passed to a simple additive weighting (SAW) algorithm for ranking and making decision selection. The framework executes in three phases, namely data preprocessing, clustering, and automatic data security with an alert mechanism. The process is completely automated so there is no need of considering the individual files for the processing and the data held will be appropriately correlated with the sharing inter-cloud environment. To inspect security issues, the proposed framework is secured by three different security algorithms. The encryption process is completed by Rivest Cipher 6 (RC6); the substitution process is done by Advanced Encryption Standard (AES); and key generation is done by RC6, AES, and Rivest-Shamir-Adleman (RSA) approaches collectively. Based on the given situations, these standard approaches were automatically applied separately or collectively. Unauthorized access trapping and data deletion mechanism are also provided in the proposed framework. The experimental results with a comparative study depicted the effectiveness of the proposed work.

1. Introduction

Cloud computing is a practice where assets and other utilities will be provided to the client based on their request [1–3]. This model shows the acquiring properties with the on-request administration in the cloud environment. After the assignment of an asset to the client, it can be taken back to improve the scalability and to address the under-provisioning and over-provisioning threats in the cloud model [4–7]. To improve the overall performance of cloud computing resources, along with the other resources, cloud clients also share the memory resources [8, 9]. This advanced cloud model uses the concepts of enlisting and association of resources which give the clients adaptability, scalability, and a pay-per-use model as mentioned in [10–12]. While sharing and managing a large number of resources over the Internet, the cloud manager generally uses three cloud security models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [13–15]. These security models show flexibility, on-interest association provisioning, fundamental asset pooling, multi-inhabitancy empowering, utility...
compensation as-you-use, etc. On the other hand, these models also highlighted security as a major concern [16–18]. A portion of the well-known cloud suppliers are as follows:

1. The private cloud is used by Google, which it uses for passing on a wide scope of organizations to its customers, including maps, web examination, content translations, e-mail access, record applications, etc [19, 20].

2. Amazon Elastic Compute Cloud (EC2) is a web-based specialist organization that licenses business allies to run application programs in the Amazon.com handling ecosystem. The EC2 can fill in every way that matters, including vast game plans of virtual machines [21].

3. Microsoft has an online association known as Microsoft SharePoint, which believes substance and business data to be moved into the cloud, and Microsoft as of now makes its office applications open in a cloud [22–24].

4. Customers of Salesforce run its application in a cloud known as Force.com and Vmforce.com; this item gives engineers stages to build changed cloud organizations [25].

Data and resource sharing is the key concern in the cloud computing area. It is widely used in all areas including hospital management systems, universities, libraries, etc. It has been used with different new era technologies like big data and Internet of things. The increasing demand and the popularity of cloud computing are increasing day by day. The other side shows the high-security requirements and needs for data communication in the cloud computing environment [26, 27]. For the better use of distributed computing, there is a need for productive treatment of the assets and there ought to be components to give a type of positioning and procuring the system safely. Due to high demand, rapidly increasing user numbers, huge shared data, and possibility of backup and recovery, the need for security increases [28].

Cloud computing can be divided based on the deployment type, which can be further categorized into four parts, namely public, private, hybrid, and community cloud. The major difference between public and private cloud is the security as the public cloud can be more secure because of the security software from the cloud service provider [29, 30]. The mixing based on the requirement of public and private cloud comes in the category of the hybrid cloud. Resource sharing is possible in the community cloud. Then there is the service-based category to consider, which can be categorized into three parts, namely IaaS, PaaS, and SaaS [31–34]. IaaS is mainly for infrastructure like disk and servers (virtual), PaaS is mainly for a platform like databases and execution frameworks [35], and SaaS is mainly for the software resources like mailing services and application services.

In this article, an efficient secure cloud computing framework has been developed. This framework consists of data grouping based on FCM [36, 37]. It has been used for the individual and associative rankings of uploaded text data on the cloud. For the decision selection ranking of the data, the SAW method has been used. For data security, RC6, RSA, and AES algorithms have been used collectively and individually based on the condition [38]. The system structure is designed and developed for providing data security of the uploaded stream for communication and data processing for data sharing [39]. The major drawbacks of the existing system are that it is inefficient in cloud data security and lacks a security applicability selection procedure for the applicability of the security needs for reliable cloud communication. This situation provokes the need for data security along with the clustering approaches that will provide the grouping of data for finding the data security needed for the individual data. It may be helpful in effective data handling also.

The rest of the article is organized as follows: Literature review is detailed in Section 2. The problem discussion and proposed work explanation are given in Section 3. Experimental results and analysis are represented in Section 4. The conclusion and future work of the proposed work are given in Section 5.

2. Related Works

Alshammari et al. [40] discussed distributed computing in terms of disseminated processing, lattice registering, and virtualization process, examined the well-being of the distributed computing climate, and analyzed and discussed about the security assaults and potential arrangements.

Salah Khaled et al. [41] proposed a classical model which can capture the behavior and analyze the network server performance in the network. They used queueing models to implement the hypo-exponential proposed model to measure the performance by incorporating features like packet loss, delay, queue size system utilization, etc.

Kandoussi et al. in [42] discussed the defense system against cyber-attack by integrating honeypot and virtual machine migration (VMM). The proposed model is effective against the attack by applying the security policies, and the model is also capable to classify potential attacks into two categories.

Koo et al. [43] examined security concerns in distributed computing. They recommended that the present security framework is not adequate for the public guard data framework. They have proposed the need for security design dependent on distributed computing for public protection in order to organize a framework.

Chalkiadakis et al. [44] proposed a system to implement a practical attestation that helps service providers to provide unified continuous service between the end cloud user and hosted application. They also tried to remove latency caused by continuously sending/receiving data from remote locations through caching system. This approach gives improved performance when compared with standard TLS handshaking.

Ghaffar et al. [45] proposed a mobile model to deal with data privacy while sharing and managing data in the cloud environment. They provide flexibility for owner data sharing.
in the cloud by introducing proxy re-encryption protocol. The proposed protocol resists security attacks and provides better performance in terms of computation, communication, and storage cost in comparison to other related protocols.

Zhou et al. [46] proposed an N-variant system for secure cloud service for cloud service provider CSP in order to save cloud applications. They discussed SecIngress, an API gateway framework, to overcome the challenge of upgrading SaaS applications. Two-stage timeout processing method has been used to lessen the service latency and analytic hierarchy process voting pre-preparing is applied depending on the weight allocated to the data. The weight relegation depends on the data elementwise mechanism with the processtimeline in the adaptability with the information. To apply and adopt a security mechanism with the process timeline in the adaptability with the framework and future protocol, the framework is divided into three parts, namely data preprocessing, clustering of data, and multiple-criteria decision-making (MCDM). The main motivation of the proposed work is to provide an efficient security protocol for user authentication and data aggregation at the time of data communication in the cloud. The communication scenario is mainly affected by the security threats in the cloud computing environment. This proposed framework provides an empirical and algorithmic study for the effective cloud protocol for crucial data security. The objectives are as follows:

1. To provide data categorization for the purpose of data separation and aggregation in a cloud computing environment for secure communication.
2. To apply the decision-making process for the security requirement to check whether it can cope with the security needs for the concurrent cryptosystem application and adaptations.
3. To apply data key hybridization for the requirement of a complex security system for the cloud data and render an alert mechanism for the protection of the data through the cloud user agreement procedure.

The proposed framework is working properly and tested under different file sets in the cloud. One such file set is attached, and to prove the working and effectiveness of the framework, a comparative analysis is done in Table1 over different parameters. Results of these parameters are also shown in (Figures 1–7) along with encryption and decryption delay. All three parts of the framework are important for the process, and the selection of parameters is also equally important. These three steps are discussed below.

3.1. Data Preprocessing. In the first stage, the information pre-preparing is applied depending on the weight allocated to the data. The weight relegation depends on the data esteemed introduced in the cloud for transferring text data. There are 10 data classifications done for the information
attribution; it is unprejudiced as it depends on the data recurrence. The total reach considered here is 1 to 10. It has been utilized for gathering dependent on the danger comparability or related loads. This stage gives the numerical capacity of the calculative loads for the further cycle and tasks. It could be useful in finding the positioning depending on the individual or acquainted loads through simple additive weight (SAW). Attribute selection is shown in Figure 8. It is the blend of the means which is utilized in all parts of boundary choice as indicated by the sink ascribes. At that point, the pre-handled worth is a contribution to the bunching stage. Figure 9 shows the data preprocessing methodology.

### 3.2. Clustering

The clustering algorithm functions in the second stage. FCM is preferred in the framework because it provides effortless and computationally deeper clustering as well as the achievement tempo, which is lofty in complex data [4, 9]. FCM has been applied to the uploaded data from cloud computing after the data preprocessing. Data grouping is done based on the weight matrix, and this matrix is in the range of 1–10. Dependent on the security closeness prerequisite or dependent on the weight accumulation, grouping of data has been performed. A completely random seed process is applied in the case of the centroid mechanism. Algorithm 1 shown below is the FCM algorithm. For data selection and ranking order, the SAW algorithm is applied.

#### Table 1: Comparative analysis.

| S.No. | Parameters                 | Existing method                                      | Proposed methodology                        |
|-------|----------------------------|-----------------------------------------------------|---------------------------------------------|
| 1     | Key variability            | 3 different size keys can be used for message encryption | 5 different size keys can be used for message encryption |
| 2     | Randomness                 | 4 different ways to generate keys for encryption     | 5 different ways to generate keys for encryption |
| 3     | Message encryption         | 4 different techniques to encrypt a message          | 5 different techniques to encrypt a message |
| 4     | Key size                   | Mini. 128, 192; Maxi. 256 bits                      | Mini. 128, 192, 256, 512; Maxi. 2048 bits  |
| 5     | Message encryption/decryption delay | Less time is required in comparison to the proposed system | More time is required in comparison to the existing systems |
| 6     | Unauthorized access notification | No mechanism available                              | Gives an alert on unauthorized access and destroys the shared copy |

#### Figure 1: Encryption time at the cloud server.

#### Figure 2: Decryption time at the cloud server.
3.3. Approach. Then for the conflicting criteria decision, multiple-criteria decision-making (MCDM) methods have been used. It has been useful for decision performances and provides proper separation based on the aggregated weights. The MCDM methods have been used in different scenarios for the ranking of the data based on the rule vectors or weights [50]. SAW has been used as the MCDM method for decision selection based on the performance matrix. First, the score in terms of aggregated assessment ranking has been calculated based on...
SAW. Then the decision performances have been arranged. For each data, a separate score for the decision evaluation has been calculated as per eq (1). Then it is multiplied by the multiplicative factor which is between 0 and 1, and then it has been summed based on the attributes and the data. This will arrange the data based on the performance, and ranking will be obtained. It gives the score which can be useful in the positioning criteria. The advantage of this procedure is that it compares direct score which can be useful in the positioning criteria. j+he performance, and ranking will be obtained. It gives the butes and the data. j+his will arrange the data based on the and 1, and then it has been summed based on the attri-

calculations are shown below:

\[ CS_i = \sum_{j=1}^{n} W_j r_{ij}, \]  

(1)

where \( CS_i \) is the total evaluation score of the \( i \)th data, \( W_j \) is the weight of \( j \)th attribute, and \( r_{ij} \) shows the random value for the \( i \)th data and \( j \)th attribute.

Then data sharing mechanism can be provided in our cloud platform. Now secure data transmission is possible as the security algorithms are automated on the data based on the performance ranking, weight, and aggregation. It is helpful in providing less computation security where the data are not very sensitive; otherwise, higher security is provided.

3.4. Automated Data Security. Based on the decision ranking, the observed frequency of more than 50% for the data is operated separately. RC6, RSA, and AES algorithm hybridization will be applied to the selected data. RC6 only will be applied to the rest of the data based on the security levels [51, 52]. It will be operated automatically based on the data rank, so it will be helpful in the textual data for timely delivery and operations. RC6 will be chosen for the higher key usability, RSA will be chosen for the larger key possibility, and AES will be chosen because of the single S-box capability and faster computation capability.

3.5. Security Alert. Our framework will have the capability of alerting unauthorized access from the data point. The data will be corrupted with the notification of unauthorized data handling and accessing.

Steps 1-6 in the algorithm expressed the working of the proposed model. The FCM algorithm (algorithm 1) is used for clustering and calculating the membership value, and the SAW algorithm (algorithm 2) is used for data selection, calculating ranking order and performance evaluation. RC6 (algorithm 3) is used for key generation and high key usability, RSA (algorithm 4) is used for larger key generation, and AES algorithm (algorithm 5) is used for substitution. All other algorithms (algorithms 3–5) are also used for the encryption/decryption of data.

In Figure 10, a flowchart of the framework working mechanism is represented. Initially, data are uploaded to cloud server then data preprocessing is done in the uploaded data. After preprocessing on data, attributes are selected based on 10 categories and weight is assigned. Then FCM algorithm is applied to attributes; and to remove biases, the centroid mechanism is applied, this is known as seed initialization. This step is repeated multiple times until we get the termination point. After this step, data are transferred to the SAW algorithm. Based on the SAW result, our framework will apply security to data while sharing the data in the cloud.

The overall framework structure is shown in Figure 11. The representation of steps from data uploading to weight assignment on data is the same. Based on the decision performance ranking, top higher rank whose supports or threshold value are ≥50% are adopted for further process, and the remaining data are discarded. Then FCM and SAW algorithms are applied to find the ranking of data. Based on the above result, an individual or combination of keys is applied automatically which is generated by RC6, RSA, and AES algorithms. If unauthorized access occurs, a warning is generated, and the shared copy of data in the cloud is erased.

3.6. System Requirements. This cloud computing security and auto key applicability framework has been developed, designed, and executed on Java platform version 7, NetBeans IDE 7.2 environment. Minimum suggested RAM 2GB, Intel or AMD x86 processor with 64 bit processing (suggested quad core processor), and for installation, it needs a 5GB memory for workspace and other application. There are no specific operating system requirements although a minimum of Windows 7 is required, no specific software requirements, and no specific graphics card requirements.

4. Experimental Results and Analysis

4.1. Results Based on Fuzzy C-Means (FCM). In this section, experimental results have been discussed and analyzed based on different data operations. Initially, for experimentation, 30 data points are considered. First, the data had been uploaded to the cloud computing environment. Data security was applied to the data for the shared users. First,
preprocessing was performed. Then computational weights were calculated as shown in Table 2. The weights ranged from W1 to W10. Client information was also available in the client column. When data were uploaded to the cloud, we performed data preprocessing, thereafter FCM was applied for computation as mentioned in Table 3 and Table 4. For data grouping in the range of 1 to 10, the weight matrix had been considered as shown in Table 5 and Table 6. Based on weight aggregation and similarity in security requirements, grouping had been done as shown in Figures 12 and 13.

Within the scenario of the centroid methodology, entirely random seeds are processed first, and then the SAW method is used to get data selection and ranking order as depicted in Figures 14 and 15. It clearly shows the clustering approach based on the algorithms applied. As shown in Tables 7 and 8, the data ranking and security operations were performed.

\[ A = \{a_1, a_2, a_3, ..., a_n\} \] are the data point values in the complete set and \( E = \{e_1, e_2, e_3, ..., e_n\} \) be the set of centers.

(1) Randomly choose the cluster midpoint with no biases.
(2) \( X = \sum_{i=1}^{n} X_{ij} = 1, \forall j = 1, 2, \ldots, n \) //calculate fuzzy relationship significance
(3) Based on the Euclidean approach

\[
Y(X, e_1, e_2, \ldots, e_r) = \sum_{i=1}^{r} Y_i = \sum_{i=1}^{r} \sum_{j=1}^{n} x_{ij}^m d_{ij}^2 //\text{calculate distance value}
\]

Membership value range lie [0, 1]; centroid is referred by \( e_i \) and Euclidean distance between \( i \)th centroid (\( e_i \)) & \( j \)th data point is given by \( d_{ij} \) weighting exponent is \( m \) \( \in [1, \infty) \).

\[
e_i = \left( \frac{\sum_{j=1}^{n} x_{ij}^m / \sum_{j=1}^{n} x_{ij}^m}{\sum_{j=1}^{n} x_{ij}^m / \sum_{j=1}^{n} x_{ij}^m} \right)
\]

(5) On extinction, criteria repeat Steps 2 & 3.
(6) End
a, b are randomly generated two large prime numbers and PK is the private key.

1. \( C = a \times b \)/public key
2. Private key generation:
   (a) \( \varphi(C) = (a-1) \times (b-1) \)
   (b) \( PK = (k \times \varphi(C) + 1)/e \) where \( 1 < e < \varphi(C) \)

Here \( e \) as the small exponent and \( \gcd(e, \varphi(C)) = 1 \)

3. Secret exponent calculation (d)
   \( 1 < d < \varphi(C) \) where \( ed = 1 \mod \varphi(C) \)

4. The receiver end inverts the above functionality for the complete calculation with module operation C.
   (a) Public key = \( C, e \)
   (b) Private key = \( d, a, b \) or \( C, e \)

(5) End

Algorithm 4: RSA Algorithm–Encryption/Decryption and Larger Key Generation Process

(1) Initial round is performed that contains 13 rounds.
(2) AddRoundKey round is performed. It is the XOR operation with the round key.
(3) Main round is performed. In this, the repletion is performed based on the iterations.
(4) SubBytes round is performed. In this step, bytes are split and processed through substitution Box or S-Box. The same S-Box is used for the bytes processed.
(5) ShiftRows round is performed for the shifting of the internal bits.
(6) MixColumns round is performed. It provides a diffusion approach for the input.
(7) Inverse operation is performed for the final output.
(8) End

Algorithm 5: AES 256 Algorithm–Encryption/Decryption, Substitution, and Key Generation Process

---

![Flowchart of working mechanism through FCM.](image1)

**Figure 10:** Flowchart of working mechanism through FCM.

![Overall system structure.](image2)

**Figure 11:** Overall system structure.
Table 2: Data and weights.

| Data   | W1 | W2 | W3 | W4 | W5 | W6 | W7 | W8 | W9 | W10 | Client |
|---------|----|----|----|----|----|----|----|----|----|-----|---------|
| P1.txt  | 4  | 1  | 4  | 3  | 0  | 3  | 3  | 0  | 0  | 6   | Client2 |
| S1.txt  | 0  | 1  | 7  | 1  | 0  | 0  | 0  | 10 | 4  | 7   | Client2 |
| S2.txt  | 0  | 0  | 1  | 0  | 5  | 0  | 2  | 0  | 1  | 1   | Client2 |
| S3.txt  | 5  | 2  | 10 | 5  | 10 | 6  | 10 | 2  | 8   | 10  | Client2 |
| S4.txt  | 10 | 5  | 10 | 0  | 10 | 0  | 10 | 0  | 2   | 10  | Client2 |
| S5.txt  | 10 | 3  | 10 | 10 | 10 | 10 | 10 | 10 | 10  | 10  | Client2 |
| S6.txt  | 10 | 1  | 10 | 10 | 4  | 10 | 10 | 0  | 2   | 10  | Client2 |
| S7.txt  | 0  | 0  | 1  | 1  | 0  | 0  | 10 | 0  | 10  | 0   | 10  | Client2 |
| S8.txt  | 5  | 10 | 10 | 6  | 0  | 6  | 8  | 0  | 2   | 9   | Client2 |
| S9.txt  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 0   | 0   | Client2 |
| S10.txt | 10 | 5  | 10 | 10 | 1  | 10 | 10 | 0  | 0   | 6   | Client2 |
| S11.txt | 1  | 0  | 1  | 0  | 1  | 0  | 2  | 0  | 1   | 0   | Client2 |
| S12.txt | 2  | 0  | 5  | 2  | 0  | 3  | 10 | 0  | 10  | 5   | 4   | Client2 |
| S13.txt | 10 | 1  | 10 | 10 | 10 | 10 | 10 | 10 | 5   | 10  | Client2 |
| S14.txt | 10 | 7  | 10 | 10 | 0  | 10 | 10 | 1  | 10  | 10  | Client2 |
| S15.txt | 6  | 3  | 10 | 6  | 2  | 7  | 10 | 2  | 10  | 10  | Client2 |
| S16.txt | 10 | 3  | 10 | 10 | 0  | 10 | 10 | 0  | 4   | 10  | Client2 |
| S17.txt | 2  | 0  | 5  | 2  | 2  | 2  | 10 | 1  | 10  | 3   | Client2 |
| S18.txt | 3  | 0  | 8  | 3  | 1  | 3  | 10 | 10 | 7   | 10  | Client2 |
| S19.txt | 5  | 0  | 5  | 5  | 0  | 5  | 10 | 1  | 1   | 10  | Client2 |
| J1.txt  | 10 | 1  | 10 | 10 | 10 | 10 | 10 | 10 | 2   | 10  | Client3 |
| J2.txt  | 2  | 4  | 2  | 0  | 1  | 1  | 5  | 1  | 0   | 2   | Client3 |
| J3.txt  | 2  | 0  | 2  | 2  | 0  | 2  | 3  | 0  | 0   | 4   | Client3 |
| J4.txt  | 6  | 10 | 10 | 8  | 0  | 7  | 8  | 0  | 0   | 10  | Client3 |
| J5.txt  | 5  | 6  | 10 | 6  | 0  | 6  | 10 | 0  | 0   | 10  | Client3 |
| J6.txt  | 10 | 5  | 10 | 10 | 0  | 10 | 10 | 0  | 2   | 10  | Client3 |
| S22.txt | 3  | 0  | 1  | 0  | 0  | 0  | 2  | 0  | 1   | 1   | Client3 |

Table 3: Data based on FCM for Cluster 1.

| Data   | W1 | W2 | W3 | W4 | W5 | W6 | W7 | W8 | Aggregate | Client |
|---------|----|----|----|----|----|----|----|----|-----------|---------|
| P1.txt  | 4  | 1  | 4  | 3  | 0  | 3  | 3  | 0  | 18        | Client2 |
| S1.txt  | 0  | 1  | 7  | 1  | 0  | 0  | 10 | 4  | 30        | Client2 |
| S2.txt  | 0  | 0  | 1  | 0  | 5  | 0  | 2  | 0  | 9         | Client2 |
| S7.txt  | 0  | 0  | 1  | 1  | 0  | 0  | 10 | 10 | 22        | Client2 |
| S9.txt  | 1  | 0  | 0  | 0  | 0  | 0  | 1  | 0  | 2         | Client2 |
| S11.txt | 1  | 0  | 1  | 0  | 1  | 0  | 2  | 0  | 1         | Client2 |
| S12.txt | 2  | 0  | 5  | 2  | 0  | 3  | 10 | 10 | 37        | Client2 |
| S17.txt | 2  | 0  | 5  | 2  | 2  | 2  | 10 | 1  | 34        | Client2 |
| S18.txt | 3  | 0  | 8  | 3  | 1  | 3  | 10 | 10 | 48        | Client2 |
| S19.txt | 5  | 0  | 5  | 5  | 0  | 5  | 10 | 1  | 32        | Client2 |

Table 4: Data based on FCM for Cluster 1.

| Data   | W1 | W2 | W3 | W4 | W5 | W6 | W7 | W8 | Aggregate | Client |
|---------|----|----|----|----|----|----|----|----|-----------|---------|
| S3.txt  | 5  | 2  | 10 | 5  | 10 | 6  | 10 | 2  | 8         | 58      | Client2 |
| S4.txt  | 10 | 5  | 10 | 10 | 0  | 10 | 10 | 0  | 2         | 57      | Client2 |
| S5.txt  | 10 | 3  | 10 | 10 | 10 | 10 | 10 | 10 | 83        | Client2 |
| S6.txt  | 10 | 1  | 10 | 10 | 4  | 10 | 10 | 0  | 2         | 57      | Client2 |
| S8.txt  | 5  | 10 | 10 | 6  | 0  | 6  | 8  | 0  | 2         | 47      | Client2 |
| S10.txt | 10 | 5  | 10 | 10 | 1  | 10 | 10 | 0  | 0         | 56      | Client2 |
| S13.txt | 10 | 1  | 10 | 10 | 10 | 10 | 10 | 5  | 76        | Client2 |
| S14.txt | 10 | 7  | 10 | 10 | 0  | 10 | 10 | 1  | 68        | Client2 |
| S15.txt | 6  | 3  | 10 | 6  | 2  | 7  | 10 | 2  | 56        | Client2 |
| S16.txt | 10 | 3  | 10 | 10 | 0  | 10 | 10 | 0  | 4         | 57      | Client2 |
4.2. Comparative Analysis Based on Variable Parameters in the Case of FCM. The above discussion shows that with different data set, different values of data and aggregated values were obtained. These aggregated sets will determine the security operation and the risk associated with the data uploaded to the cloud environment.

The process is completely automated, so there is no need of considering the individual files for the processing, and the data held will be appropriately correlated with the sharing inter cloud environment as shown in Figures 16–19. CW denotes the weight according to the cluster.

Table 5: Decision weight for Cluster 1.

| Data     | Decision weight | Client |
|----------|----------------|--------|
| S5.txt  | 24.8           | Client2|
| S13.txt | 22.6           | Client2|
| S14.txt | 20.67          | Client2|
| S6.txt  | 17.9           | Client2|
| S16.txt | 17.7           | Client2|
| S3.txt  | 17.19          | Client2|
| S4.txt  | 17.1           | Client2|
| S15.txt | 15.85          | Client2|
| S10.txt | 15.6           | Client2|
| S8.txt  | 11.92          | Client2|

Table 6: Decision weight for Cluster 2.

| Data     | Decision weight | Client |
|----------|----------------|--------|
| 8.txt    | 13.28          | Client2|
| S17.txt  | 10.29          | Client2|
| S12.txt  | 9.67           | Client2|
| 19.txt   | 9.57           | Client2|
| S1.txt   | 7.29           | Client2|
| P1.txt   | 5.64           | Client2|
| S7.txt   | 4.21           | Client2|
| S2.txt   | 2.54           | Client2|
| S11.txt  | 1.94           | Client2|
| S9.txt   | 0.82           | Client2|

4.3. Comparative Analysis Based on Data Security. A completely random set has been chosen to reduce the chance of biasness. The applicability of keys on sensitive data is shown by key grades [53, 54]. In methodology, mainly three keys were used, which give five different types of key distribution.
individually or in combination. Figure 20 clearly shows that keys are involuntarily applied to files; as the numbers of files increase based on sensitivity, keys are also increased to give better security and this will reduce risk.

4.4. Comparative Analysis Based on Encryption and Decryption Time. Figures 1 and 2 clearly depict the time taken in encryption and decryption. As the encryption process is completed by RC6; the substitution process is completed by AES; and the key generation process is completed by RC6, AES, and RSA algorithm collectively, the security is high and in comparison, to the aggregation, the total time taken is less. The data size in bytes shows the variability considered in the data uploading mechanism.

4.5. Comparative Analysis with Existing Methods. Comparative analysis is done based on the following parameters shown in Table 1. Figures 2–6 show the comparison based on parameters such as message, key size, delay, and randomness.

In the analysis, we compared message, key, and randomness. The message shows total generated key messages; key shows the total number of used key; and in each iteration key generation, randomization process is shown by randomness. It is clear from Figure 5 that the proposed approach shows better results when compared with
contemporary techniques. A comparison based on key size is shown in Figure 6 which clearly shows that the variability in key size (min/max) is better in our approach. Security is higher and better in our framework for higher risk due to maximum key variability and authentication. Both results show that our auto framework approaches based on FCM with three security algorithms have complex security capability.

Figure 7 depicts the discovery time (DT) of unauthorized access in the cloud environment. DT shows the time taken for the notice to the cloud user and server for the unauthorized access probability. The delay in encryption is higher in our case as shown in Figures 1 and 2 which shows the higher security complexity as compared to the previous work. The key complexity is the advantage of our approach which shows the efficiency in our approach is higher in comparison to the traditional approaches.

5. Conclusion and Future Work

In this article, a secure client framework is proposed which is efficient and secure in a cloud environment along with the security constraints. Data preprocessing and FCM and SAW algorithms are applied, and finally, decision performance ranking is calculated. The performance of clustering shown is based on the constraint used for the chosen attributes in terms of computational weights. The security constraints have been applied based on the performance matrix. The security of data while sharing in the cloud and the generation of keys for sharing data is done through the combination of three encryption standards randomly. Based on the decision performance ranking, whose supports were higher than the given threshold value, the entire three security standards have been adopted and one security standard is applied for the remaining data (random selection). The resultant process is completely automated, so there is no need of considering the individual files for the processing, and the data held will be appropriately correlated with the sharing inter-cloud environment.

Our result illustrates that based on a different number of file sets, keys spreading are automatically increased or decreased as per the sensitivity of data. The delay in encryption is higher in our case which shows the high-security complexity as compared to the previous work. The key complexity is the advantage of our approach which shows the better efficiency of our approach over the existing approaches. Key variability in the proposed approach is higher in comparison to the traditional approaches, which is also an advantage. The future suggestions are based on the proposed work and the previous analysis; work can be extended with the combination of machine learning (ML) techniques with other clustering algorithms. The parameters can be changed or extended in the future for checking the correlation variation in different ways for analyzing the system and security aspects. Computation can be enhanced with the introduction of ML, other clustering approaches, and new encryption and steganographic approaches. This proposed framework is suitable in the SaaS layer and for text data type only. The framework can be designed for other layers of cloud-like PaaS and IaaS and extended in terms of other data types like images, audio, and video.

Data Availability

The data related to experimentation and other work are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Z. Lv, L. Qiao, and I. You, “6G-enabled network in box for internet of connected vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5275–5282, 2021.
[2] B. Cao, Y. Gu, Z. Lv, S. Yang, J. Zhao, and Y. Li, “RFID reader anticollision based on distributed parallel particle swarm optimization,” IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3099–3107, 2021.
[3] W. Zheng, Y. Xun, X. Wu, Z. Deng, X. Chen, and Y. Sui, “A comparative study of class rebalancing methods for security
bug report classification,” *IEEE Transactions on Reliability*, vol. 70, no. 4, pp. 1658–1670, 2021.

[4] R. Liu, X. Wang, H. Lu et al., “SCCGAN: style and characters inpainting based on CGAN,” *Mobile Networks and Applications*, vol. 26, pp. 3–12, 2021.

[5] Z. Lv, D. Chen, H. Feng, H. Zhu, and H. Lv, “Digital twins in unmanned aerial vehicles for rapid medical resource delivery in epidemics,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2021.

[6] H. Cheng, M. Shojaifar, M. Alazab, R. Tafozolli, and Y. Liu, “PPVF: privacy-preserving protocol for vehicle feedback in cloud-assisted VANET,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, 2021.

[7] B. Cao, S. Fan, J. Zhao et al., “Large-scale many-objective deployment optimization of edge servers,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3841–3849, 2021.

[8] Z. Lv, Y. Li, H. Feng, and H. Lv, “Deep learning for security in digital twins of cooperative intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[9] H. Chen, Y. Xiang, S. Li, Z. Song, Z. Hu, and F. Liu, “Multi-Sensor data driven with PARAFAC-IPSO-PNN for identification of mechanical nonstationary multi-fault mode,” *Machine*, vol. 10, no. 2, p. 155, 2022.

[10] B. Cao, Z. Sun, J. Zhang, and Yu Gu, “Resource allocation in 5G IoT architecture based on SDN and fog-cloud computing,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3832–3840, 2021.

[11] D. Yang, T. Zhu, S. Wang, S. Wang, and X. Zhang, “LFRSNet: a robust light field semantic segmentation network combining contextual and geometric features,” *Frontiers in Environmental Science*, p. 1443, 2022.

[12] B. Cao, J. Zhao, Z. Lv, and P. Yang, “Diversified personalized recommendation optimization based on mobile data,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2133–2139, 2021.

[13] J. Chen, Y. Liu, Y. Xiang, and K. Sood, “RPPTD: robust privacy-preserving truth discovery scheme,” *IEEE Systems Journal*, pp. 1–8, 2021.

[14] H. Chen and S. Li, “Multi-Sensor fusion by CWT-PARAFAC–IPSO-SVM for intelligent mechanical fault diagnosis,” *Sensors*, vol. 22, no. 10, p. 3647, 2022.

[15] T. Cai, D. Yu, H. Liu, and F. Gao, “Computational analysis of variational inequalities using mean extra-gradient approach,” *Mathematics*, vol. 10, p. 2318, 2021.

[16] J. Mou, P. Duan, L. Gao, X. Liu, and J. Li, “An effective hybrid collaborative algorithm for energy-efficient distributed permutation flow-shop inverse scheduling,” *Future Generation Computer Systems*, vol. 128, pp. 521–537, 2022.

[17] X. Wu, W. Zheng, X. Xia, and D. Lo, “Data quality matters: a case study on data label correctness for security bug report prediction,” *IEEE Transactions on Software Engineering*, vol. 48, no. 7, pp. 2541–2556, 2022.

[18] X. Wu, W. Zheng, X. Chen, Y. Zhao, T. Yu, and D. Mu, “Improving high-impact bug report prediction with combination of interactive machine learning and active learning,” *Information and Software Technology*, vol. 133, Article ID 106530, 2021.

[19] M. Zhang, Y. Chen, and W. Susilo, “PPO-CQ: a privacy-preserving optimization of clinical pathway query for e-healthcare systems," *IEEE Internet of Things Journal*, vol. 7, no. 10, Article ID 10660, 2020.

[20] L. Zhang, T. Gao, G. Cai, and K. L. Hai, “Research on electric vehicle charging safety warning model based on back propagation neural network optimized by improved gray wolf algorithm,” *Journal of Energy Storage*, vol. 49, Article ID 104902, 2022.

[21] H. Wang, Q. Gao, H. Li, H. Wang, L. Yan, and G. Liu, “A structural evolution-based anomaly detection method for generalized evolving social networks,” *The Computer Journal*, vol. 65, no. 5, pp. 1189–1199, 2022.

[22] G. Liu, “Data collection in mi-assisted wireless powered underground sensor networks: directions, recent advances, and challenges,” *IEEE Communications Magazine*, vol. 59, no. 4, pp. 132–138, 2021.

[23] W. Yang, X. Chen, Z. Xiong, Z. Xu, G. Liu, and X. Zhang, “A privacy-preserving aggregation scheme based on negative survey for vehicle fuel consumption data,” *Information Sciences*, vol. 570, pp. 526–544, 2021.

[24] L. Zhang, H. Zheng, G. Cai, Z. Zhang, X. Wang, and L. H. Koh, “Power-frequency Oscillation Suppression Algorithm for AC Microgrid with Multiple Virtual Synchronous Generators Based on Fuzzy Inference System,” *IET Renewable Power Generation*, vol. 16, pp. 1589–1601, 2022.

[25] F. Liu, G. Zhang, and J. Lu, “Multisource heterogeneous unsupervised domain adaptation via fuzzy relation neural networks,” *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3308–3322, 2021.

[26] G. Sun, C. Yang, J. Dong, Y. Liu, Z. Ding, and H. Yu, “What and How: Generalized Lifelong Spectral Clustering via Dual Memory,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1–10, 2021.

[27] F. Zhao, L. Song, Z. Peng et al., “Night-time light remote sensing mapping: construction and analysis of ethnic minority development index,” *Remote Sensing*, vol. 13, no. 11, p. 2129, 2021.

[28] S. El Kafhali, I. El Mir, and M. Hanini, “Security threats, defense mechanisms, challenges, and future directions in cloud computing,” *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 223–246, 2022.

[29] Yi Xie, Y. Sheng, M. Qiu, and F. Gui, “An adaptive decoding biased random key genetic algorithm for cloud workflow scheduling,” *Engineering Applications of Artificial Intelligence*, vol. 112, Article ID 104879, 2022.

[30] D. Soni and M. Kumar, “An automated cloud security framework based on PCM in user-cloud environment,” *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 3235–3240, 2019.

[31] Z. Niu, B. Zhang, B. Dai et al., “220 GHz multi circuit integrated front end based on solid-state circuits for high speed communication system,” *Chinese Journal of Electronics*, vol. 31, no. 3, pp. 569–580, 2022.

[32] Y. Xi, W. Jiang, K. Wei, T. Hong, T. Cheng, and S. Gong, “Wideband RCS reduction of microstrip antenna array using coding metasurface with low Q resonators and fast optimization method,” *IEEE Antennas and Wireless Propagation Letters*, vol. 21, no. 4, pp. 656–660, 2022.

[33] T. Hong, S. Guo, W. Jiang, and S. Gong, “Highly selective frequency selective surface with ultrawideband rejection,” *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 5, pp. 3459–3468, 2022.

[34] J. Yan, H. Jiao, W. Pu, C. Shi, J. Dai, and H. Liu, “Radar sensor network resource allocation for fused target tracking: a brief review,” *Information Fusion*, vol. 86-87, pp. 104–115, 2022.

[35] K. Cao, H. Ding, B. Wang et al., “Enhancing Physical Layer Security for IoT with Non-orthogonal Multiple Access}
Assisted Semi-Grant-Free Transmission,” IEEE Internet of Things Journal, 2022.

[36] D. Soni, V. Sharma, and D. Srivastava, “Optimization of security issues in adoption of cloud ecosystem,” in Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp. 1–5, Ghaziabad, India, April 2019.

[37] D. Soni, V. Tiwari, B. Kaur, and M. Kumar, “Cloud computing security analysis based on RC6, AES and RSA algorithms in user-cloud environment,” in Proceedings of the 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT), pp. 269–273, Meerut, India, December 2021.

[38] Q. Fan, Z. Zhang, and X. Huang, “Parameter conjugate gradient with secant equation based elman neural network and its convergence analysis,” Advanced Theory and Simulations, Article ID 2200047, 2022.

[39] N. Tissir, S. El Kafhali, and N. Aboutabit, “Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal,” Journal of Reliable Intelligent Environments, vol. 7, no. 2, pp. 69–84, 2021.

[40] A. Abshammari, S. Alhaidari, A. Ali, and Z. Mohamed, “Security threats and challenges in cloud computing,” in Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 46–51, IEEE, New York, NY, USA, June 2017.

[41] K. Salah and S. El Kafhali, “Performance modeling and analysis of hypoexponential network servers,” Telecommunication Systems, vol. 65, no. 4, pp. 717–728, 2017.

[42] E. M. Kandoussi, M. Hanini, I. El Mir, and A. Haqiq, “Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game,” Telecommunication Systems, vol. 73, no. 3, pp. 397–417, 2020.

[43] J. Koo, Y.-G. Kim, and S.-H. Lee, “Security requirements for cloud-based C4I security architecture,” in Proceedings of the 2019 International Conference on Platform Technology and Service (PlatCon), pp. 1–4, IEEE, Jeju, Korea, January 2019.

[44] N. Chalkiadakis, D. Deyannis, D. Karnikis, G. Vasiilias, and S. Ioannidis, “The million dollar handshake: secure and attested communications in the cloud,” in Proceedings of the 2020 IEEE 13th International Conference on Cloud Computing (CLOUD), pp. 63–70, IEEE, Beijing, China, October 2020.

[45] Z. Ghaffar, S. Ahmed, K. Mahmood, Sk H. Islam, M. M. Hassan, and G. Fortino, “An improved authentication scheme for remote data access and sharing over cloud storage in cyber-physical-social-systems,” IEEE Access, vol. 8, Article ID 47144, 2020.

[46] D. Zhou, H. Chen, G. Cheng, W. He, and L. Li, “SecIngress: an API gateway framework to secure cloud applications based on N-variant system,” China Communications, vol. 18, no. 8, pp. 17–34, 2021.

[47] B. Novković, A. Božić, M. Golub, and S. Groš, “Confidential computing as an attempt to secure service provider’s confidential client data in a multi-tenant cloud environment,” in Proceedings of the 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), pp. 1213–1218, IEEE, Opatija, Croatia, September 2021.

[48] R. ThandaiahPrabu, P. Vijayakumari, K. Chanthirasekaran, K. Jayamani, and P. Nirmala, “An efficient and secured multiple keyword cloud data searching scheme with dynamic encryption procedure,” in Proceeding of the 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), pp. 1–6, IEEE, Chennai, India, January 2022.

[49] M. Hassaoui, M. Hanini, and S. El Kafhali, “Domain generated algorithms detection applying a combination of a deep feature selection and traditional machine learning models,” Journal of Computer Security, pp. 1–21, 2022.

[50] Li Zhou, Q. Fan, X. Huang, and Y. Liu, “Weak and strong convergence analysis of Elman neural networks via weight decay regularization,” Optimization, pp. 1–23, 2022.

[51] D. Soni and M. Kumar, “Secure data communication in cloud environment: a survey,” in Proceedings of the 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), pp. 246–252, Nagpur, India, November 2017.

[52] S. Zhao, F. Li, H. Li et al., “Smart and practical privacy-preserving data aggregation for fog-based smart grids,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 521–536, 2021.

[53] T. Sui, D. Marelli, X. Sun, and M. Fu, “Multi-sensor state estimation over lossy channels using coded measurements,” Automatica, vol. 111, Article ID 108561, 2020.

[54] H. Du, Y. Deng, J. Xue, D. Meng, Q. Zhao, and Z. Xu, “Robust online CSI estimation in a complex environment,” IEEE Transactions on Wireless Communications, vol. 1, 2022.