**International Journal of Computing and Mathematics**
Vol. 1, Issue. 3, Sep 2024, pp. 1~7 

# Hybrid Soft Computing Techniques for Enhancement of Data Privacy on Cloud

**Idyawati Hussein[1], Zarul Fitri Zaaba[2]**
[1]School of Computing, Universiti Utara Malaysia, 06010 UUM, Sintok, Malaysia
[2]Universiti Sains Malaysia, Pulau Pinang, Malaysia

**Article Info**

***Article history:***

Received Jul 7, 2024
Revised Aug 20, 2024
Accepted Sep 3, 2024

***Keywords:***

Soft Computing
Data Privacy and Security
Cost Optimization
Cloud

**ABSTRACT**

Nowadays, cloud computing serves as an important factor in advanced software for storage and transferring large data. Cloud-based service providers provide software to their users to improve their lot, while consumers prefer to reduce their costs. The cloud is accomplished by inter-networking technology and is enduring from all the bugs that impact networking too. Data privacy and security have become a major breach in the cloud while transferring data between the client and the server. In this paper, proposed soft computing techniques to avoid the data security issues on the cloud and their cost optimization. Soft Computing is an exact term for algorithms that benefit from human ability and simulate the capabilities of individuals. Several techniques are being utilized for avoiding security issues, but any system is not nearly perfect until now. The proposed hybrid soft computing techniques help to enhance their above issues in the recent cloud computing environment.

***Corresponding Author:***

Idyawati Hussein,
School of Computing, Universiti Utara Malaysia, 06010 UUM, Sintok, Malaysia.

## 1. INTRODUCTION

Cloud computing is identified as the latest emerging technologies that in the immediate future would have a major effect on the IT sector [1]. Cloud computing is an increasingly increasing area of scientific science and business of today's period. Cloud-based computing offers "IT services over the internet" regarding the "cost-per- use" customer's request. It uses parallel computation, distributed systems, grid computing, and centralized storage to improve communication, in a virtual machine, and high - speed internet application-focused network infrastructure [2].

The information is analyzed on cloud storage and data is reached in distant regions. For these distributed cloud services, the quality and ensure the security of the encrypted information are the most crucial aspects of cloud computing since all the information to be processed is without authentication. If some of the service providers can view user data contributing to unreliable contact, security breaches are likely associated with system usage of cloud services. Researchers also incorporated the identifier in our research proposal to test the software if is safe or vulnerable. Cloud users can feel protected cloud computing from data centers by using the identifier.

If the service provider evaluates their data, because of their data protection the consumers felt uncomfortable for this. For this purpose, exposure to authentication by external parties is often unsuitable for the cloud services framework [3]. As cloud infrastructure allows individuals to develop their efficiency and development. Therefore, it organizes a lot of users to give fewer initiatives to connect network services. However, security issues or threats continue to be a major obstacle in cloud computing's growth trajectory. The reasoning is numerous. First of all, consumers and several entities keep everyone’s provided by the cloud storage, so the key objective will be that the data should be protected, and the knowledge shouldn't be destroyed and manipulated since traveling across the system on each position to the next [4]. It is therefore basic to ensure the confidentiality, availability, and integrity of the data. Third, illegal entry where the

attacker appears to be the legitimate users required. Security is a major concern, and cloud storage is no different compared to every emerging technology.

On centralized database architecture, cloud storage involves various protection threats. Data management is the key concern that arises with the existence of frameworks that keeps users from accepting private clouds. In centralized storage, using several cache methods, the data is stored away on excludes. The prior is to decrypt and archive the details on the file and the second is to store and retrieve data through cryptography. Both roles will also run up against secrecy problems.

Normally, the software isn't of the same kind and could have unique qualities. Since the customer's data is processed on distant networks and the user has no knowledge of their traditional position, the possibility of an information breach is also still present. This article reflects on the problem of security in data analytics. Wherever the knowledge is shared with the cloud service, an authentication mechanism is implemented, i.e. encryption by knowing the vulnerability standard of the data, or the data can be easily processed on the cloud storage without being protected.

Each data has different types of protection and it is unacceptable to follow instructions by knowing the standard of vulnerability and protection requirements. To enable the data protection criteria, researchers suggested a knowledge discovery framework to describe the database as per their distributed edge and then protect one other software needed to protect it via a cloud service cryptographic technique.

Machine learning is an essential field of theoretical and methodological applications in many areas, such as pattern classification and deep learning, mathematics, image processing, and healthcare. A rather sophisticated data-securing strategy will be to then separate the data into critical and non - critical information and then only protect the relevant data. This would serve to minimize the workload by accessing all information that would be incredibly expensive including both precise and quick transfers. Several encryption methods may be used to secure the data, and various learning algorithms are used in the data mining sector to identify the data. Data analysis refers to the process in data science used to determine the type of knowledge that is not marked.

Data mining utilizes special tools to identify the trends and interactions that are hidden and valid within the sample. Such methods are computational measurements, empirical models, and data analysis and assessment. Data analysis thus comprises data management, data selection, forecasting, and evaluation [22]. Deep learning algorithms are defined in two classifications: supervised and unsupervised. Classes also are described in the controlled analysis. Next, a sample dataset is specified for a supervised analysis that corresponds to different categories. Such basic skills are branded with some kind of name, efficiently. Most of the algorithms for data mining are controlled learning with a comprehensive target vector. In unsupervised classification categories, it is not defined accurately or even the data is normally arranged. The unregulated algorithm searches for correlation between two devices to figure out if they can be described as creating a group [21]. In simple terms "no target parameter is considered" in unsupervised classification. The classifier of intelligence in the sense of secrecy is the category of data depending on the degree of security that affects the entity as only approved individuals are sharing details. The selection of features allows to establish through basic protection measures are important to secure the relevant information. The information is divided into 2 learning activities, highly classified, and semi-confidential [19]. The classifier of knowledge is dependent on the benefits of sustainability.

## 2. RELATED WORKS

Cloud computing is growing significantly; it changes companies across markets and provides a framework to achieve cloud-based services with uncontrolled economic advantages and organizational development. Continuous growth and importance of cloud computing, many corporate and state service providers are shifting their tasks to ensure security. Throughout the portion, researchers also provide a few of the research relevant to our work that was done [20].

Jogdand et al. [5] introduced a classic Merkle Hash algorithm that satisfies open cloud-based inspection and guarantees data quality by the use of a different cloud DepSky method model. Tawalbeh L et al.[6] suggest a stable, data classifying dependent cloud provider. The suggested hybrid cloud helps to reduce the complexity and computing time taken to encrypt data by leveraging multiple authentication protocols of flexible encryption algorithms to include the correct amount of security available for the data.

Researchers also encrypted data on a three-stage scale, sensitive and extremely classified stage, including various cryptographic protocols to protect the data at each point. The approach proposed was checked with various data encryption and the findings of the analysis demonstrated the stability and performance of the system suggested [23].

A hybrid encryption mechanism utilizing description encoding, characteristics, and time-based techniques is introduced by Moghaddam F. et al. [7]. Categorization of analysis is required primarily on

features. The model framework has been used to create protection among the groups. Those other tightly secured rings execute the encryption algorithm to defend themselves from unauthorized access, time-based, ask from the cloud provider, and assessment risk [24]. The review of the findings reveals that the integrated framework paradigm increases the stability and performance of network security systems.

Dhamija Ankit et al. [8] suggest cloud infrastructure that guarantees safe data transfer from the client's enterprise to the cloud provider's (CP) databases. In this, the hybrid method of public-key cryptography is used as the data being exchanged on the network can have two-way protection. Initially, by utilizing the encryption method the data is transformed into structural characteristics and then this encrypted model information collected has been translated into a raw picture utilizing cryptographic primitives [23]. Encryption often covers the notification's presence, thus guaranteeing reducing agent of interfering with results.

Garg and Bawa [9] recommended the complex data multi-factor authentication framework in cloud storage to minimize the expense of processing and connectivity. This method is implemented on secure handling of the cloud and for information security and monitoring. With this method, safe communication among cloud consumers and service providers may be improved.

El-Booz et al. [10] proposed a safe cloud services framework for protected interaction in the cloud-based environment utilizing a time-based each-time authentication protocol and automated defender security procedures. In this, individuals implemented connectivity by 3rd parties that are used to encrypt the information and send it to the required users. In the complex multi-domain system methodology Al-Saffar [11] suggested honesty of domain records. This system is often used to boost healthy communication among shareholders and consumers. There, in the cloud-based setting, the user may update their details which could modify the database in the encryption modules. Authenticator must validate that data is secure; if safe, the authenticator must create the secret modules authenticated [18]. Every consumer may retrieve the cloud while using the intercepted security code. The main problem with this method is the encryption/decryption element. Today the encoded and decoded data will be used by 3rd parties. As a result, everyone could obtain files which leads to unsafe propagation.

Karthiban and Smys [12] and Sridhar and Smys [13 have suggested strategies for protecting security measures in the cloud. The service provider utilizes the honesty method in a static system, and the credibility cycle is used by the remote server in a dynamic framework. Even reliability and verification are achievable when utilizing this RIC program [14]. The cloud storage testing concerns are third party candidates who could view their data information, authorizations will interfere, cloud providers could distribute the file system, and datasets could be destroyed due to system failures. Researchers developed an innovative potential strategy to prevent these problems which are mentioned further [15].

## 3. PROPOSED METHODOLOGY

To any form of enterprise, cloud resources are freely available. The problem of secrecy and honesty emerges when various corporations and government / non- governmental organizations tend to retain some valuable information on the cloud. Information exchanged and stored in a single database allows it possible for unauthorized users to explore remove and change protected realized the importance in a challenge to privacy.

Besides that, it is necessary to know the data to analyze which information goes to be protected and so forth. To provide it, a supervised learning system was presented that defines the data as per their security level, thus encoding the only information needed to protect it via cloud context cryptographic techniques [16]. The work includes addressing different protection concerns in the cloud world in terms of secrecy, honesty, and functionality in 3 ways and evaluating its effects. The work includes investigating and evaluating the output of numerous data classifiers algorithms and techniques, such as ANN, multilayer perceptron, and logistic regression [25].

The authors propose a stable model for classifying data utilizing a conceptual framework to enhance ensemble learning. In that, the model is analyzed as per their degree of specificity [17]. Let's intercepting the data needed to be safe in the public cloud utilizing a combined security maintaining feature cryptography-dependent methodology.

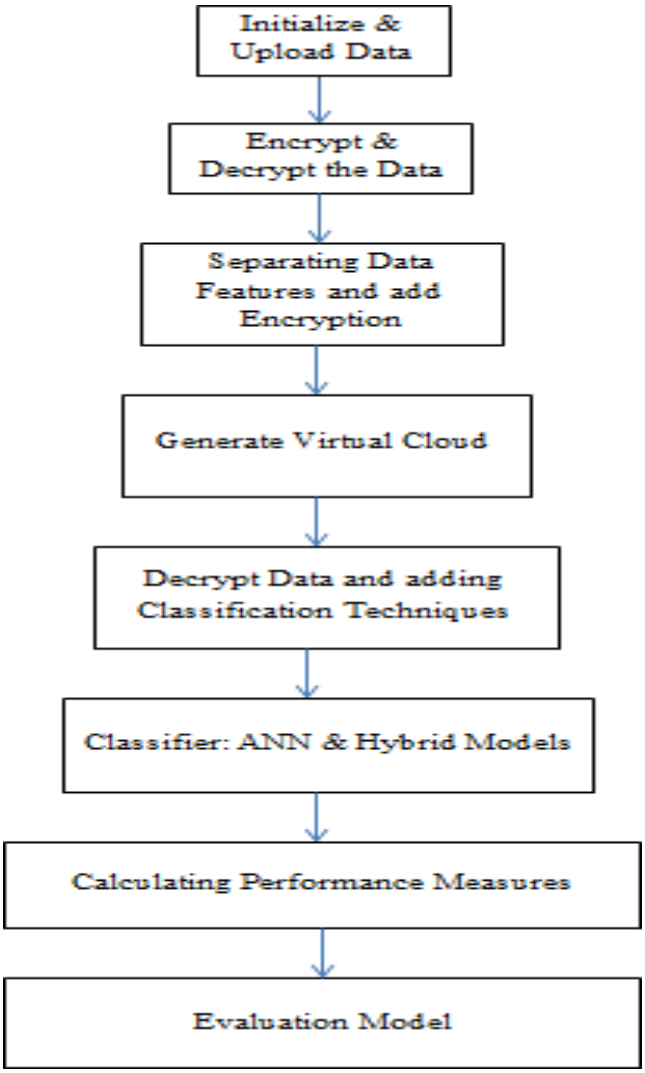


Figure 1. Proposed System

This encryption is dependent on certain visual patterns. This is quite safe every time the collection of images may shift. This encryption key for decoding frames is used for cloud security. Only valid users can enable cloud access if individuals access the appropriate learning media. After data encryption, the above software would also request the client series when accessing file transfers, this time features should be generally focused on the pattern of login credentials objects.

Use New improving Method to identify the sample. The following table displays a set of instructions for the suggested improving mobility. The accompanying framework illustrates the system architecture for the suggested improving mobility. In the illustration, Vector is the statistical model for the preparation. S is a vector that is used to iterate the sample.

This is used for the monitoring of objects. Vector is a variable included to separate data sets to identify the models. Q is the sequence of interactions that includes so many specific cases. Train the classifier model using this set of transactions Q.

Instead, determine the volume of voting by the learning algorithm and change the numbers of activities appropriately categorized and categorized. R is the program that was developed following every initialization. X is the vector for iterating the computation time for every prototype. The learning sample would be moved into the binary classification to guide it to form an opinion. Modify the distance of the true positive file or sequence and quietly standardize all transfers that perhaps the total amount of loads of the actual process remains the same.

Thus parameters P are allocated to the decision of the algorithm. Additionally, choose several data that fits their loads and low predictor variables for training. At a certain point, the proportions of classifier voting for type t are increasing.

A modern strategy has been introduced to hold confidential data safe from attacks on the network that gives confidentiality to the data of the user. By just submitting the individual information to the server in authenticated or encoded form, the relevant information is not submitted to the cloud throughout this method. In this document, encrypted data are masked and the predetermined parameters are submitted to the database in the pattern of a word document. Place both measured edge pixels from thresholding software properties in a collection with any locations i.e. an edge and panel.

For instance:Q(a, b, m)

In which Vector is the input with the edge, i= ith Panel, j = jth

Then Z = difference value on another document.

While identifying and storing the layers and statistical features of those margins in a sequence spontaneously choose the pixel length or efficiency score of that infinite number and use a feature subset predictor.

The feature is extracted in such a manner that we often save the relevant parameter estimates of that sequence in a data form and send this word document to the cloud rather than saving the feature vectors where their response component is hidden. And the list of feature vectors and their locations is processed at the local end retail outlet.

The criteria for assessing the accuracy of the developed program suggested are:

a) Amount of time needed for statistical analysis
b) The integrity of confidential data
c) Time to Encrypt

## 4. EXPERIMENTAL RESULTS

The technique suggested is applied using Cloudsim and Net beans IDE 8.0.CloudSim is the library that includes the cloud computing system model, while also main categories that define virtual computers, cloud services, clients, and frameworks. The effects of the evaluation and data hiding process are shown in Figure 2 and Figure 3, below. In these statistics, a significant difference exists among ANN with encryption and enhanced raising with hybrid Privacy preservation. The article has demonstrated the successful comparison of the technique based on the most recent process.

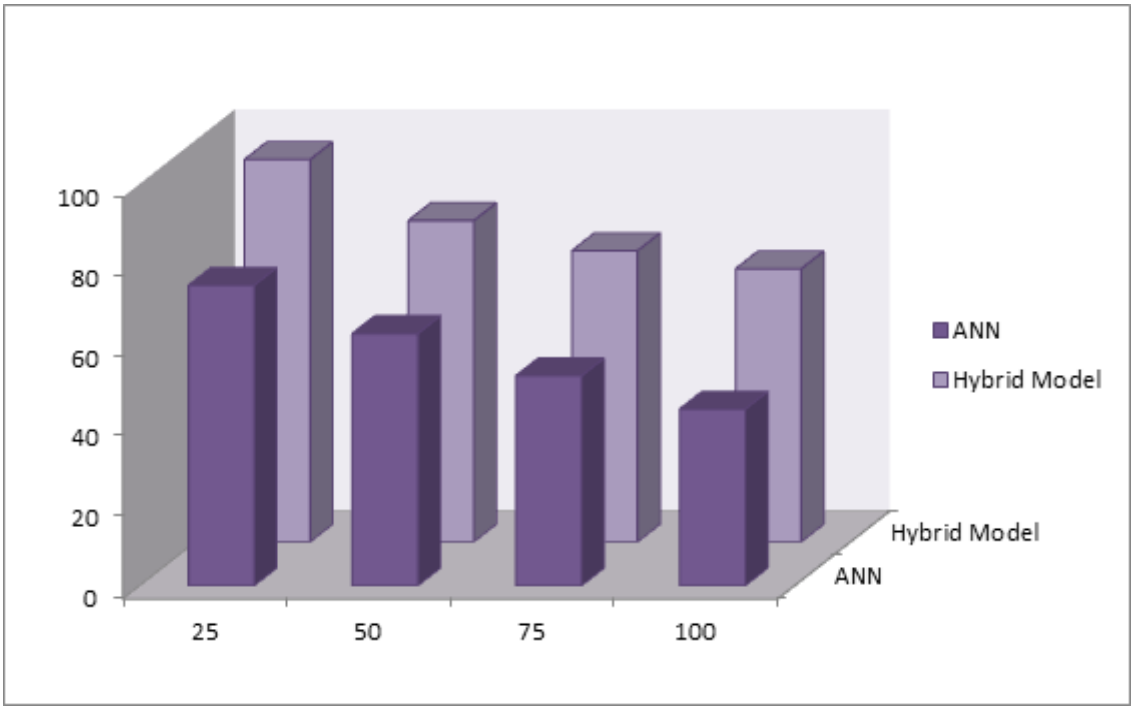


Figure 2. Performance Comparison

From the output analyses, it is explicitly evaluated that the new strategy is stronger than the prior method. Figure 2 demonstrates the performance relation of ANN and suggested adaptive method data, classification models. ANN algorithm provides performance of 74.8 percent and enhanced optimization is

95.2 percent i.e. proposed technique has categorized relevant information further reliably and results in 49.6 percent higher than the ANN algorithm.

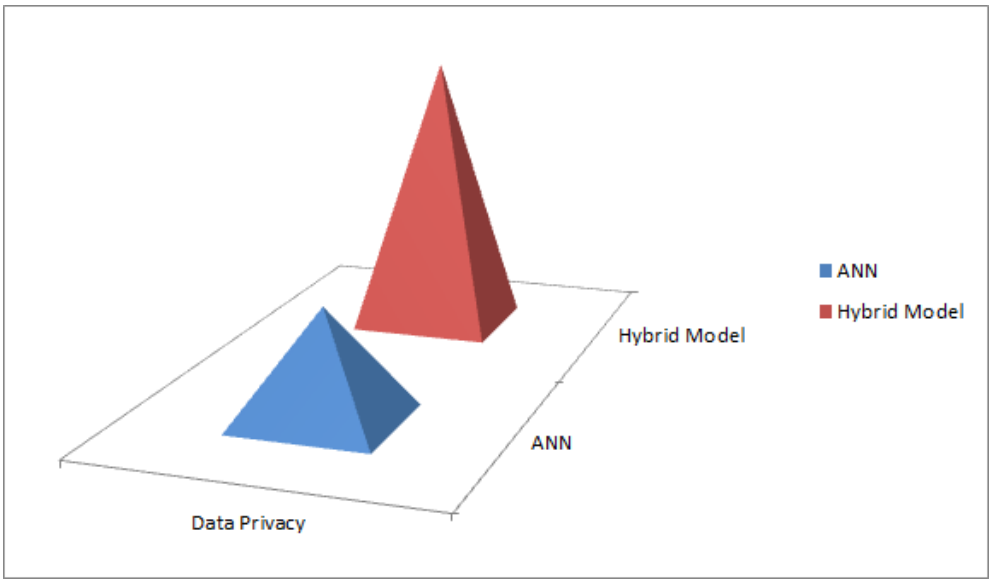


Figure 3. Performance Measures of Data Privacy on Cloud

Accordingly, Figure 3 demonstrates the contrast of the hidden period between the current solution and the existing Encryption. The suggested highly efficient feature selection plan requires the team will develop simulations to cover critical details, and the Encryption process involves cipher integers. Thus, learning techniques are used to determine the encryption period on cloud data as per the better protection. From the aforementioned study, it is seen that in terms of precision and data protecting period, the suggested approach improves the performance.

## 5. CONCLUSION AND FUTURE WORKS

A methodology for the protection of data in the cloud framework is suggested in this study. The research emphasis seems to be to classify the data including a better learning algorithm calculating the security's protection basic requirements which support a wide variety into critical and non - confidential models. The critical feature of this framework of protection is data secrecy and data processing using a classification methodology to data science. The protected sensitive data is then authenticated to use a privacy protection technique focused on advanced encryption and is retained in the cloud repository to use a cryptographic hash to preserve confidentiality integrity while the pseudo-confidential data is immediately transferred to the web world as statistical data.

Feature sequence encryption keys focused on various frameworks are often used to improve protection at the verification stage to prevent unwanted access to the data system. The proposed framework was tested using Cloud simulation tools in a built computer model system. The findings indicate that perhaps the methodology suggested is more important than preserving the data when agreeing on the data's protection needs. The findings also demonstrate that the modified enhancing method achieves better either the precision or the classification period than the ANN classification algorithm did.

In the future, to make the classification decisions to use the machine learning algorithm, much more protection criteria could be considered, as well as the enhancing technique could perhaps be improved to use neural network dependent classification methods for classifying data as per security procedures.

## REFERENCES

[1] Pitchai, R., Babu, S., Supraja, P., &Anjanayya, S. (2019). Prediction of availability and integrity of cloud data using soft computing technique. Soft Computing, 23(18), 8555-8562.

[2] Kaur, K., &Zandu, V. (2016). Secure Data Classification Model in Cloud Computing Using Machine Learning Approach. International Journal of Grid and Distributed Computing, 9(8), 13-22.

[3] Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011) “Collaboration- Based Cloud Computing Security Management Framework” IEEE conference of cloud computing, Washington (DC), pp. 364-371,2011.

[4] Song, D., E. Shi, I. Fischer, and U. Shankar,(2012) "Cloud data protection for the masses" ,
[5] IEEE Comput. Soc., 45(1): 39-45
[6] Jogdand RM, Goudar RH, Sayed GB (2015) Enabling publicverifiability and availability for secure data storage in cloudcomputing. EvolSyst 6(1):55–65
[7] Lo"aiTawalbeh, Nour S. Darwazeh, Raad S. Al- Qassas and Fahd AlDosari (2015) "A Secure Cloud Computing Model based on Data Classification", First International Workshop on Mobile Cloud Computing Systems, Management, and Security, Elsevier pp. 1153 – 1158,2015
[8] F. F. Moghaddam, M. Vala, M. Ahmadi, T. Khodadadi, and K. Madadipouya, "A reliable data protection model based on re-encryption concepts in cloud environments," 2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC), pp. 11–16, 2015.
[9] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," 2015 International Conference Green Computing and Internet of Things (ICGCIoT), pp. 346–351, 2015.
[10] Garg N, Bawa S (2016) Comparative analysis of cloud data integrity auditing protocols. J Netw Comput Appl 66:17–32
[11] El-Booz SA, Attiya G, El-Fishawy N (2016) A secure cloud storage system combining time-based one- time password and automatic blocker protocol. EURASIP J InfSecur 2016(1):1–13
[12] Al-Saffar AMH (2015) Identity-based approach for cloud data integrity in multi-cloud environment. Identity 4(8):505–509
[13] Karthiban K, Smys S (2018) Privacy preserving approaches in cloudcomputing. In: 2018 2nd international conference on inventive systems and control (ICISC).
[14] IEEE, pp 462–467
[15] Sridhar S, Smys S (2016) A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th international conference on intelligent systems and control (ISCO).IEEE, pp 1–5
[16] Cai BL, Zhang RQ, Zhou XB (2017) Experience availability: tail latency oriented availability in software- defined cloud computing.J Comput SciTechnol 32(2):250–257.
[17] P. Li,J. Li,Z. Huang,T. Li,C.-Z. Gao,S.-M.
[18] Yiu,K. Chen, Multi-key privacy-preserving deep learning in cloud computing, Future Generation. Computing Syst. 74(2017) 76–85
[19] Raja, S., Jaiganesh, M., &Ramaiah, S. (2017). An efficient fuzzy self-classifying clustering based framework for cloud security. International Journal of Computational Intelligence Systems, 10(1), 495-506.
[20] GR, V., & Reddy, A. R. M. (2012). An efficient security model in cloud computing based on soft computing techniques. International Journal of Computer Applications, 975, 8887.
[21] Ejimogu, O. H., &Başaran, S. (2017). A systematic mapping study on soft computing techniques to cloud environment. Procedia computer science, 120, 31-38.
[22] B. Li, y. Huang, z. Liu, j. Li, z. Tian, s.-m. Yiu, hybridoram: practical oblivious cloud storage with constant bandwidth, inf. Sci. (2018), doi:10.1016/j.ins.2018.02.019.
[23] M.Sumathi, U.Rahamathunnisa, A.Anitha, Druheen Das, Nallakaruppan.M.K, "Comparison of Particle Swarm Optimization and Simulated Annealing applied to Travelling Salesman Problem", International Journal of Innovative Technology and Exploring Engineering, Volume-8, Issue-6, April 2019, PP 1578- 1583. 13.
[24] M.Sumathi and S.Sangeetha, "Survey on Sensitive Data Handling- Challenges and Solutions in Cloud Storage System", Proceeding Advances in Big Data and Cloud Computing, Springer Nature Singapure, Vol.750, PP 598-609, 2018.
[25] K. Hashizume, et al., An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5) (2013).
[26] H. Liang, An Improved Intrusion Detection based on Neural Network and Fuzzy Algorithm. Journal of Networks, 9(5) (2014) pp. 1274-1280.
[27] A.S.A. Aziz, et al., Artificial Immune System Inspired Intrusion Detection System Using Genetic Algorithm. Informatica, 36, (2012) pp. 347-357.
[28] F. Zhao and H. Jin, Automated Approach to Intrusion Detection in VM-Based Dynamic Execution Environment. Computing and Informatics, 31, (2012) pp. 271-297.