Computers, Materials & Continua
DOI: 10.32604/cmc.2022.027135
Article

Tech Science Press

Metaheuristics with Machine Learning Enabled Information Security on Cloud Environment

Haya Mesfer Alshahrani[1], Faisal S. Alsubaei[2], Taiseer Abdalla Elfadil Eisa[3], Mohamed K. Nour[4], Manar Ahmed Hamza[5,*], Abdelwahed Motwakel[5], Abu Sarwar Zamani[5] and Ishfaq Yaseen[5]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[2]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, 21959, Saudi Arabia
[3]Department of Information Systems-Girls Section, King Khalid University, Mahayil, 62529, Saudi Arabia
[4]Department of Computer Science, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa
Received: 11 January 2022; Accepted: 04 March 2022

Abstract: The increasing quantity of sensitive and personal data being gathered by data controllers has raised the security needs in the cloud environment. Cloud computing (CC) is used for storing as well as processing data. Therefore, security becomes important as the CC handles massive quantity of outsourced, and unprotected sensitive data for public access. This study introduces a novel chaotic chimp optimization with machine learning enabled information security (CCOML-IS) technique on cloud environment. The proposed CCOML-IS technique aims to accomplish maximum security in the CC environment by the identification of intrusions or anomalies in the network. The proposed CCOML-IS technique primarily normalizes the networking data by the use of data conversion and min-max normalization. Followed by, the CCOML-IS technique derives a feature selection technique using chaotic chimp optimization algorithm (CCOA). In addition, kernel ridge regression (KRR) classifier is used for the detection of security issues in the network. The design of CCOA technique assists in choosing optimal features and thereby boost the classification performance. A wide set of experimentations were carried out on benchmark datasets and the results are assessed under several measures. The comparison study reported the enhanced outcomes of the CCOML-IS technique over the recent approaches interms of several measures.

Keywords: Information security; cloud computing; intrusion; anomalies; data mining; feature selection; classification

1 Introduction

Cloud computing (CC) provides large number of support to the global environments in different regions such as business, education, and medical [1]. Security is the main portion of the service that is provided globally. Data security plays a significant part in a cloud network. Different kinds of security risks such as audit schedules, security application, key management and encryption, physical and user access control identity, and access management, [2] are listed in the cloud information. Recently, the encryption of information is executed by various encryption methods that have the capacity for the transformation of texts into a framework called ciphertext. This is an encrypted form of the particular input as plain text that won't be viewed by privileged users. Similarly, by utilizing a separate key, the encrypted information creates the approach for decrypting the information that is capable of offering the original text to the privileged users [3]. In cloud environment, privacy maintenance contains two factors such as data processing and data storage security. Data storage security consists of issues of potential user data confidentiality while the information is stored in the data center. Data processing security consists of the problem of how to maintain user privacy at operation time in a virtualized cloud environment. Several methods are designed for privacy preservation in the cloud. A massive number of private information are analyzed and exploited using cloud service provider (CSP) on the basis of cloud. When the CSP is taken into account as trustworthy than in the cloud, sensitive data management is easier [4]. Yet, many legal issues are remaining. But the healthcare or personal data and data subject trusted the data manager in several instances, even though they do not allow the regulator to transfer the information by the trusted member [5]. Fig. 1 illustrates security system involved in CC.

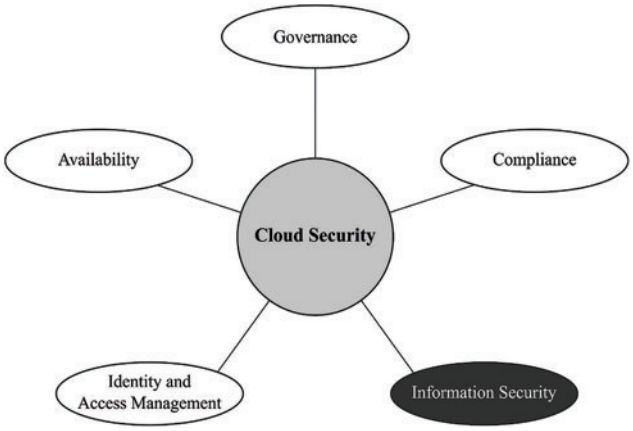

Figure 1: Cloud security

Generally, intrusion detection system (IDS) is classified on the basis of activity level as follows: Host based IDS (HIDS) and Network based IDS (NIDS) [6]. Host based IDS is developed for monitoring activity of certain host networks. Network based IDS is designed for monitoring the activity of several hosts and analyzing vehicular adhoc networks (VANET) packets taken from the system. At the same time, IDS consist of strategic detection method includes anomaly detection and signature recognition. The variance among these approaches is that anomaly detection analyses the property of common behavior whereas signature recognition recognizes intrusion based on known attack features [7]. Thus, IDS handles unbelievable amount of information that has unrelated and redundant features which presented a calculation time and extreme training [8]. Different methods for feature classification or reduction were presented for improving the efficacy of IDS in attack detection [9]. Most of them are depends on machine learning (ML) methods to improve IDS feature selection,

mostly for effective attack classification procedure. Unfortunately, none of the presented methods is effective–often there are certain drawbacks. Henceforth, let us discuss that there is a requirement for research is being undertaken to enhance the IDS efficiency [10].

In [11], a secure and efficient access control system was introduced for the CC platform for sharing knowledge and resource. In the beginning, resources or data are encrypted by the user attribute, and encrypted information is separated into the extracted and encapsulated ciphertext. Next, identity-based timed-release encryption (IDTRE) approach was utilized for encrypting the decrypted key and integrated the ciphertext of the key with the extracted ciphertext to create the ciphertext share. The researcher in [12] proposed a new method for creating innovative multi-level user authentication system with hybrid CAPTCHA codes. This code defines a novel type of cognitive CAPTCHA, where the authentication needs user special knowledge and skills, that are essential for appropriate verification. This method of verification might be focused on offering data accessing for trusted users or certain group of experts who have special perception abilities and knowledge as well as to characterize specific expert areas.

The researchers in [13] aim at cloud data delivery and storage to privileged users. Therefore, a hierarchal identity-based cryptography model is utilized for checking the data integrity and security, to guarantee that there is no modification or alteration made by a CSP or malicious attacker for their gain. In [14], the fundamental concept of the CC and its applications were examined based on the significance of privacy problems. The presented method enhances the security level in the CC via decision trees and data mining algorithms. Lower computation burden and user number independence assist in efficiently carrying out the presented method in real time. Veerabathiran et al. [15] provide a homomorphic proxy re-encryption (HPRE) which allows different cloud users that they redistributed HPRE encrypted with the PubKs using the acceptability by a close process namely INFO remotely. The examination of providing access control (AC), secrecy, and uprightness of INFO enabled cloud phases is not given for by traditional AC methods. A model was generated to fulfill the association requirements that accept complete authorization through the physical structure of the resources.

This study introduces a novel chaotic chimp optimization with machine learning enabled information security (CCOML-IS) technique on cloud environment. The proposed CCOML-IS technique primarily normalizes the networking data by the use of data conversion and min-max normalization. Followed by, the CCOML-IS technique derives a feature selection technique using chaotic chimp optimization algorithm (CCOA). In addition, kernel ridge regression (KRR) classifier is used for the detection of security issues in the network. The design of CCOA technique assists in choosing optimal features and thereby boost the classification performance. A wide set of simulations were carried out on benchmark datasets and the results are assessed under several measures.

The rest of the paper is organized as follows. Section 2 introduces the proposed model, Section 3 validates the proposed model, and Section 4 concludes the work.

2 The Proposed Information Security Technique

In this study, an effective CCOML-IS technique has been developed to accomplish maximum security in the CC environment by the identification of intrusions or anomalies in the network. The proposed CCOML-IS technique primarily normalizes the networking data by the use of data conversion and min-max normalization. Then, the CCOML-IS technique derives a feature selection technique using CCOA. Moreover, KRR classifier is used for the detection of security issues in the network. Fig. 2 illustrates the overall process of CCOML-IS technique.

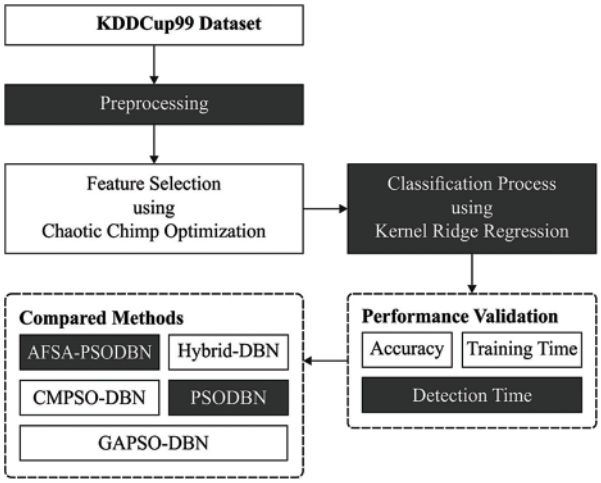

Figure 2: Overall process of CCOML-IS technique

2.1 Data Pre-Processing

For eliminating the dimension influence of all the features, the training as well as testing set are normalized. Based on the subsequent data transformation Eq. (1), all the values from the dataset achieved from the primary phase were normalized in the range zero to one.

$$Y = \frac{Y_{original} - Y_{min}}{Y_{max} - Y_{min}} \tag{1}$$

where Yoriginal implies the novel value of y feature, Ymin refers the minimal value of y feature, and Ymax stands for the maximal value of y feature.

2.2 Process Involved in CCOA Based Feature Selection

A nature inspired approach called COA [16] was stimulated from the sexual motivation and individual intelligence of chimps in group hunting. It is distinct from the other social predators. In this method, four distinct stages were employed to stimulate dissimilar intelligence including barrier, attacker, driver, chaser, and so on. The arithmetical method of the presented approach was given as follows: The chasing and driving the prey or target is demonstrated below:

$$D = \left| c.a_{prey}(n) - ma_{chimp}(n) \right| \tag{2}$$

$$a_{chimp}(n+1) = a_{prey} - a.d, \tag{3}$$

In the equation, n represents the overall amount of iterations, m, and a indicates the coefficient vector. They are estimated as follows

$$a = 2.l.r_1 - l \tag{4}$$

$$c = 2.r_2 \tag{5}$$

$$m = chotic_{value}, \tag{6}$$

Here, r_1 and r_2 denotes arbitrary number within $[0, 1]$, m shows that chotic vector and l is non-linearly decreased from 2.5 to 0 by using the iteration method. In this phase, the behavior of chimps has

been mathematically implemented. Now, assume the first solution is accessible by the chaser, attacker, driver, and barrier that is better informed regarding the targeted position. Next, the other optimal solutions attained are stored, and reaming chimps are enforced to upgrade the individual position based on the optimal chimp location.

$$d_{attacker} = |c_1 a_{attacker} - m_1.x| \tag{7}$$

$$d_{barrier} = |c_2 a_{barrier} - m_2.x| \tag{8}$$

$$d_{chaser} = |c_3 a_{chaser} - m_3.x| \tag{9}$$

$$d_{driver} = |c_4 a_{driver} - m_4.x| . \tag{10}$$

Once the random vector lies within [−1, 1], then the subsequent position of chimp might be in any position among the target or prey present location:

$$x_1 = a_{attacker} - a_1.d_{attacker} \tag{11}$$

$$x_2 = a_{barrier} - a_2.d_{barrier} \tag{12}$$

$$x_3 = a_{chaser} - a_3.d_{chaser} \tag{13}$$

$$x_4 = a\ driver\ - a_4 d_{driver} \tag{14}$$

In the above equations, the location of the chimps in the searching procedure can be upgraded as follows

$$x_{n+1} = \frac{x_1 + x_2 + x_3 + x_4}{4}. \tag{15}$$

At last, in order to upgrade the position of chimps at the time of the searching procedure in the searching region was employed to the subsequent formula:

$$a_{chimp}\,(n+1) = \begin{cases} a_{prey}\,(n) - x.d, & if \phi < 0.5 \\ chaotic_{value} & if\ \phi > 0.5. \end{cases} \tag{16}$$

The optimization approach cannot demonstrate the optimal solution to complex problems. Each algorithm faces some disadvantages. Hence, because of the existing competitive situation, we need effective optimization methods, therefore it addresses complicated problems. But this technique tackles complicated functions when the exploitation and exploration process of the technique. Initialization of the searching agent in the optimization problem is randomly implemented. A random vector is set with value ranges among predetermined minimum and maximum constraints. There is no clear rule which defines the first stage for the optimization method [17]. Owing to the fact that the meta heuristic-based optimization method progresses is considerably impacted by the initialized population determination, the likelihood of attaining good results that improve when the initialized population assumption is increased. The development of the initialized population is performed by hybridization using chaotic maps. The concept of merging the chaotic map with the metaheuristic optimization method is suggested. The analysis demonstrates that the logistic chaotic map is improved when compared to each existing chaotic map. This is because of good computation efficacy and the higher likelihood for initiating arbitrary values closer to 0 and 1.

Algorithm 1: Pseudocode of COA

Inputs: The population size Nand maximal amount of iterations t
Random population generation X_i $(i = 1, 2, \ldots, N)$
while $t <$ max.amount of iterations do
for all the chimps do
Determine the chimp's group
By utilizing is group strategy to upgrade
end for
for every search climb do
if $x < 1$ then
Upgrade the location of the existing search chimp
else if $x > 1$ then
Choose an arbitrary search chimp
end if
Upgrade the location of the existing search chimp
end for
Upgrade X Attacker, Barrier, Driver, and Chaser $t + 1$
end while

Consequently, the fast local searching is presented:

$$y_1 = rand, y_{i+1} = 4 \times y_i \times (1 - y_i), i = 1, 2, \ldots, N, \tag{17}$$

whereas rand represents an arbitrary vector within 0 and 1. The recently proposed CMOA is described by substituting the random vector named $rand_i$ estimated by the logistic chaotic mapping. Therefore, the MOA is enhanced by modifying the population initialization using the chaotic character.

The CCOA approach resolves a fitness function (FF) for determining solution under this state develop for attaining a balance amongst the 2 objectives as:

$$fitness = \alpha \Delta_R(D) + \beta \frac{|Y|}{|T|} \tag{18}$$

$\Delta_R(D)$ implies the classifier error rate. $|Y|$ signifies the size of subset which approach chooses and $|T|$ entire amount of features restricted from the current data sets. α refers the parameter $\in [0, 1]$ comparing with the weight of error rate of classifiers correspondingly also $\beta = 1 - \alpha$ stands for the significance of decrease feature.

2.3 KRR Based Classification

In typical RR, the part of the hidden state is to map the input layers to the hidden layers that are hidden layers of the RR maps information from the data space to high dimension space, whereby all the dimensions correspond to a hidden layer. Henceforth, the efficiency of RR is mainly based on the hidden layers and it is application specific. In order to prevent the abovementioned hidden layer selection problem, a KRR was utilized for classifying each microarray medical data set. In KRR, a positive regularization coefficient C is presented to make it more stable and generalized [18].

$$\beta = H^T(\frac{1}{c} + HH^T)^{-1}T \tag{19}$$

Now C indicates the regulation coefficient, T shows the output matrix and H represents the hidden neuron output matrix.

$$f(x) = h(x) H^T (\frac{1}{c} + HH^T)^{-1} T \tag{20}$$

Here, rather than knowing the hidden neuron feature mapping, $h(x)$, its respective $|\langle(u,\ v)$ is evaluated. The absence of L that is, hidden layers in *KRR* simplify KRR computational method.

$$\theta_{RR} = HH^T : \theta_{RRij} = h(x_i) \cdot h\left(x_j\right) = |\langle\left(x_i, x_j\right) \tag{21}$$

Therefore, the output of kernel ridge regression is given by

$$f(x) = h(x) H^T \left(\frac{1}{c} + HH^T\right) T, T = \begin{bmatrix} k(x, x_1) \\ \cdot \\ \cdot \\ k(x, x_N) \end{bmatrix}^{\mathrm{T}} \left(\frac{1}{c} + \theta_{RR}\right) \tag{22}$$

whereas $\theta_{RR} = HH^T$ and $k\left(x_i,\ x_j\right)$ represent the kernel function of hidden layers of single layer feed-forward networks (SLFN). Among the distinct kernel function satisfies Mercer condition accessible in radial basis function kernel (RKRR) and wavelet kernel (WKRR) are taken into consideration. RKRR is a local kernel function where λ and Y are utilized as the variables. At the same time, the complex wavelet kernel function employs vector that is $[d,\ e,\ f]$ as variable. Based on the data sets, best decision of kernel function and appropriate tuning of the variables are extremely needed to attain optimal results.

Radial basis kernel

$$\mathrm{k}(x, y) = e^{(-a\|x-y\|)} \tag{23}$$

Wavelet kernel

$$\mathrm{k}(x, y) = \cos\left(d\frac{\|x-y\|}{e}\right) e\left(-\frac{\|x-y\|^2}{f}\right) \tag{24}$$

Kernel RR is beneficial when compared to RR since there is no need to know the hidden neuron feature mapping and setting the amount of hidden layers L. It attains good generalization, is faster than SVM, and has more stability in comparison with RR.

3 Results and Discussion

The performance validation of the CCOML-IS technique is performed using the KDD dataset, which comprises of two sets namely training data and testing data. The dataset includes instances under binary class and multi-class instances. The class distribution of the samples that exist in the dataset is shown in Fig. 3. Tab. 1 and Fig. 4 relates the binary class accuracy attained by the CCOML-IS approach on the training and testing processes of KDD dataset. On KDD-training dataset, the CCOML-IS method has gained enhanced accuracy of 99.92% whereas the hybrid-deep belief network (DBN), particle swarm optimization (PSO) with DBN (PSODBN), genetic algorithm with PSO (GAPSO)-DBN, artificial fish swarm algorithm (AFSA)-PSODBN, and CMPSO-DBN techniques have obtained reduced accuracy of 99.85%, 96.83%, 97.26%, 98.27%, and 98.12% correspondingly. Besides, on the test KDD-testing dataset, the CCOML-IS system has gained higher accuracy of 87.35% whereas the hybrid-DBN, PSODBN, GAPSO-DBN, AFSA-PSODBN, and CMPSO-DBN methodologies have resulted in lesser accuracy of 83.86%, 80.58%, 81.02%, 81.98%, and 81.23% correspondingly.

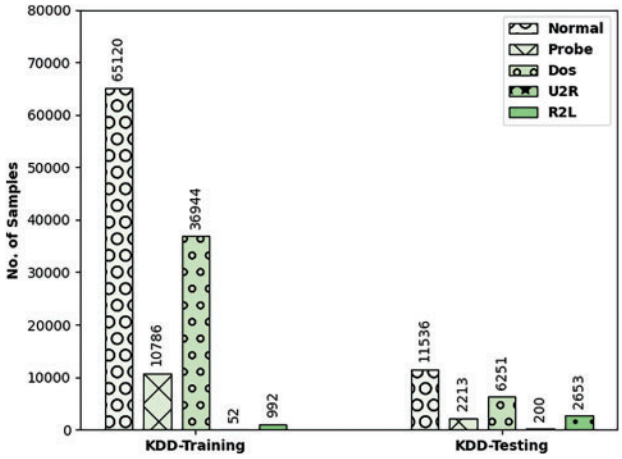

Figure 3: Sample classes

Table 1: Binary class accuracy analysis of CCOML-IS technique under training and testing of KDD dataset

Binary class-accuracy (%)		
Methods	KDD-training	KDD-testing
Hybrid-DBN	99.85	83.86
PSODBN	96.83	80.58
GAPSO-DBN	97.26	81.02
AFSA-PSO-DBN	98.27	81.98
CMPSO-DBN	98.12	81.23
CCOML-IS	99.92	87.35

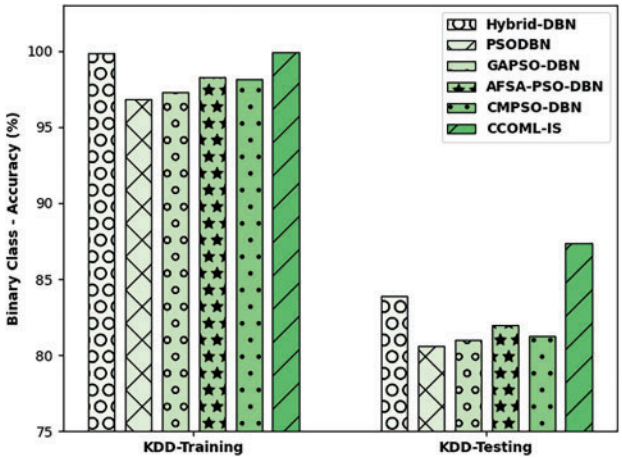

Figure 4: Accuracy analysis of CCOML-IS technique under binary class

The accuracy outcome analysis of the CCOML-IS technique under binary class is portrayed in Fig. 5. The results demonstrated that the CCOML-IS technique has accomplished improved validation accuracy compared to training accuracy. It is also observable that the accuracy values get saturated with the epoch count of 1000.

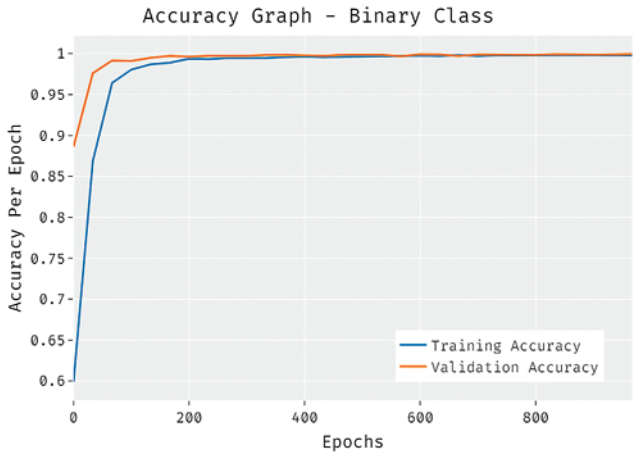

Figure 5: Accuracy graph analysis of CCOML-IS technique under binary class

The loss outcome analysis of the CCOML-IS technique under binary class is depicted in Fig. 6. The figure revealed that the CCOML-IS technique has denoted the reduced validation loss over the training loss. It is additionally noticed that the loss values get saturated with the epoch count of 1000.

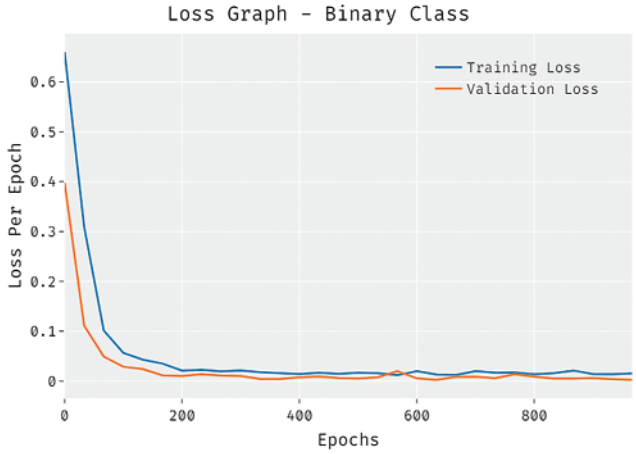

Figure 6: Loss graph analysis of CCOML-IS technique under binary class

Tab. 2 and Fig. 7 compare the multi-class accuracy obtained by the CCOML-IS technique on the training and testing processes of KDD dataset. On KDD-training dataset, the CCOML-IS technique has gained improved accuracy of 99.08% whereas the hybrid-DBN, PSODBN, GAPSO-DBN, AFSA-PSODBN, and CMPSO-DBN techniques have obtained reduced accuracy of 98.55%, 95.72%, 96.35%, 97.26%, and 97.12% respectively. Similarly, on the test KDD-testing dataset, the CCOML-IS technique has attained enhanced accuracy of 88.75% whereas the hybrid-DBN, PSODBN,

GAPSO-DBN, AFSA-PSODBN, and CMPSO-DBN techniques have resulted to lower accuracy of 82.36%, 79.22%, 80.42%, 80.68%, and 80.13% respectively.

Table 2: Multiclass accuracy analysis of CCOML-IS technique under training and testing of KDD dataset

Multiclass-accuracy (%)		
Methods	KDD-training	KDD-testing
Hybrid-DBN	98.55	82.36
PSODBN	95.72	79.22
GAPSO-DBN	96.35	80.42
AFSA-PSO-DBN	97.26	80.68
CMPSO-DBN	97.11	80.13
CCOML-IS	99.08	88.75

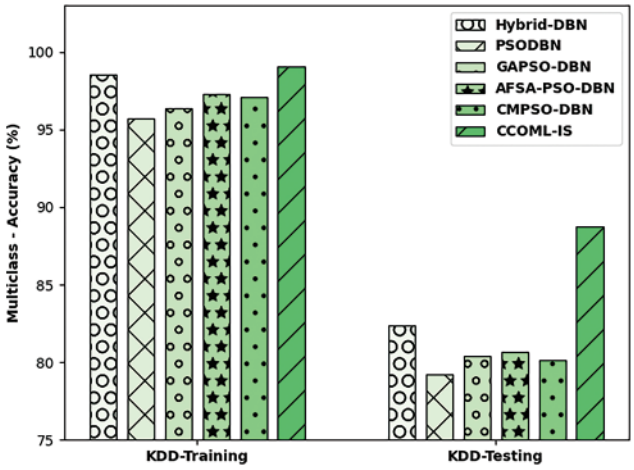

Figure 7: Accuracy analysis of CCOML-IS technique under multiclass

The accuracy outcome analysis of the CCOML-IS approach under multiclass is demonstrated d in Fig. 8. The outcomes depicted that the CCOML-IS method has accomplished higher validation accuracy compared to training accuracy. It can be also observable that the accuracy values get saturated with the epoch count of 1000.

The loss outcome analysis of the CCOML-IS technique under multiclass is depicted in Fig. 9. The figure stated that the CCOML-IS system has represented the lower validation loss over the training loss. It can be additionally noticed that the loss values get saturated with the epoch count of 1000.

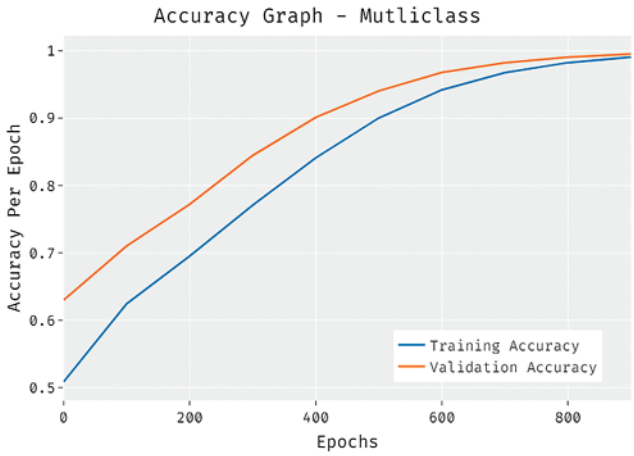

Figure 8: Accuracy graph analysis of CCOML-IS technique under multiclass

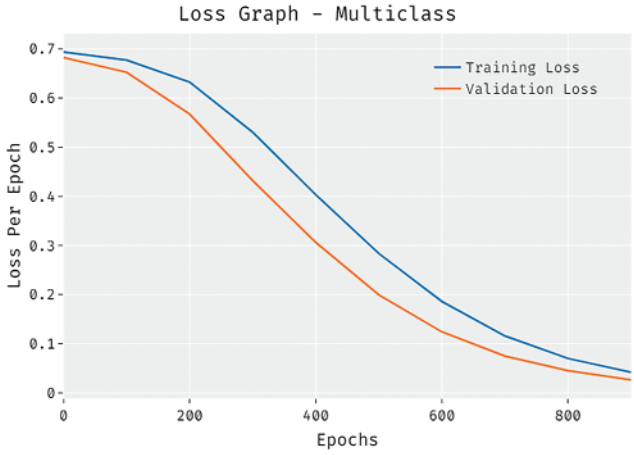

Figure 9: Loss graph analysis of CCOML-IS technique under multiclass

Finally, a detailed computation time (CT) analysis of the CCOML-IS technique is provided [19]. A brief training time (TT) analysis of the CCOML-IS technique is compared with recent methods in Fig. 10. The results show that the Hybrid-DBN, GAPSO-DBN, and AFSA-PSODBN techniques have obtained least outcome with the extreme TT of 222.64, 205.59, and 255.36 min respectively. In line with, the PSODBN and CMPSO-DBN techniques have obtained slightly reduced TT of 188.76 and 172.55 min respectively. However, the CCOML-IS technique has resulted in enhanced outcomes with the minimal TT of 142.38 min.

A detailed detection time (DT) analysis of the CCOML-IS approach was related to recent techniques in Fig. 11. The outcomes demonstrated that the Hybrid-DBN, GAPSO-DBN, and AFSA-PSODBN methods have obtained worse outcomes with the extreme DT of 136.69, 129.83, and 142.92 min correspondingly. Also, the PSODBN and CMPSO-DBN systems have reached slightly minimal DT of 123.81 and 125.47 min correspondingly. At last, the CCOML-IS technique has resulted in improved outcomes with the reduced DT of 101.26 min. The above mentioned results and discussion ensured the enhanced outcomes of the CCOML-IS technique over the other techniques.

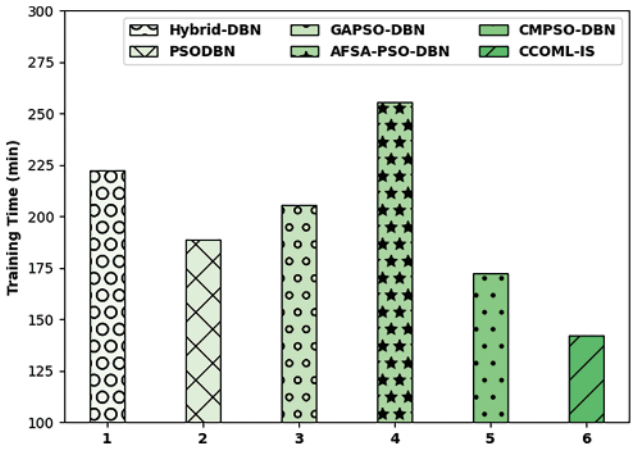

Figure 10: Training time analysis of CCOML-IS technique with existing approaches

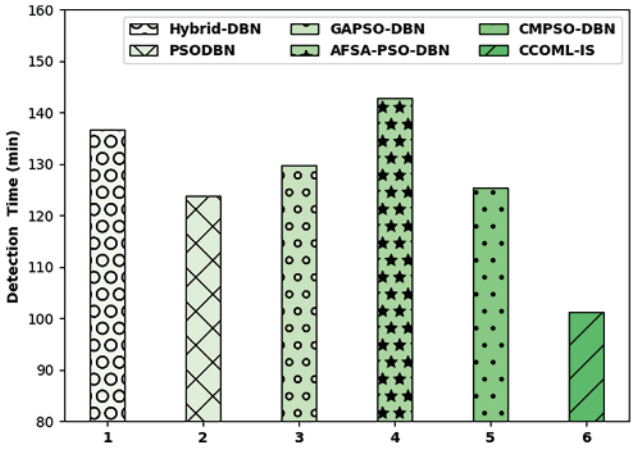

Figure 11: Detection time analysis of CCOML-IS technique with existing approaches

4 Conclusion

In this study, an effective CCOML-IS technique has been developed to accomplish maximum security in the CC environment by the identification of intrusions or anomalies in the network. The proposed CCOML-IS technique primarily normalizes the networking data by the use of data conversion and min-max normalization. Then, the CCOML-IS technique derives a feature selection technique using CCOA. Moreover, KRR classifier is used for the detection of security issues in the network. The design of CCOA technique assists in choosing optimal features and thereby boost the classification performance. A wide set of experimentations were carried out on benchmark datasets and the results are assessed under several measures. The comparison study reported the enhanced outcomes of the CCOML-IS technique over the recent approaches interms of several measures. In future, outlier removal approaches can be included to further improvise the security.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4310373DSR01).

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 2/49/42). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R237), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Shabbir, A. Shabbir, C. Iwendi, A. R. Javed, M. Rizwan *et al.,* "Enhancing security of health information using modular encryption standard in mobile cloud computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021.

[2] S. Namasudra, R. Chakraborty, S. Kadry, G. Manogaran and B. S. Rawal, "FAST: Fast accessing scheme for data transmission in cloud computing," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2430–2442, 2021.

[3] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami *et al.,* "A systematic literature review on cloud computing security: Threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021.

[4] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 9–15, 2020.

[5] M. Joshi, S. Budhani, N. Tewari and S. Prakash, "Analytical review of data security in cloud computing," in *2021 2nd Int. Conf. on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, pp. 362–366, 2021.

[6] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami *et al.,* "IoT and cloud computing issues, challenges and opportunities: A review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, 2021.

[7] B. Mondol and M. A. Mahmood, "An efficient approach for multiple user data security in cloud computing," in *2021 Int. Conf. on Artificial Intelligence and Smart Systems (ICAIS)*, Coimbatore, India, pp. 1130–1135, 2021.

[8] A. H. Shaikh and B. B. Meshram, "Security issues in cloud computing," *Intelligent Computing and Networking*, pp. 63–77, 2021. https://doi.org/10.1007/978-981-15-7421-4_6.

[9] P. Chinnasamy, S. Padmavathi, R. Swathy and S. Rakesh, "Efficient data security using hybrid cryptography on cloud computing," *Inventive Communication and Computational Technologies*, pp. 537–547, 2021. https://doi.org/10.1007/978-981-15-7345-3_46.

[10] H. Abroshan, "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, pp. 31–37, 2021.

[11] S. Namasudra, "An improved attribute-based encryption technique towards the data security in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 3, pp. e4364, 2019.

[12] U. Ogiela, "Cognitive cryptography for data security in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 18, pp. 1–4, 2020.

[13] S. Kaushik and C. Gandhi, "Ensure hierarchal identity based data security in cloud environment," *International Journal of Cloud Applications and Computing*, vol. 9, no. 4, pp. 21–36, 2019.

[14] Q. He and H. He, "A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining," *Sustainability*, vol. 13, no. 1, pp. 101, 2020.

[15] V. K. Veerabathiran, D. Mani, S. Kuppusamy, B. Subramaniam, P. Velayutham *et al.,* "Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption," *Soft Computing*, vol. 24, no. 24, pp. 18893–18908, 2020.

[16] M. Kaur, R. Kaur, N. Singh and G. Dhiman, "SChoA: A newly fusion of sine and cosine with chimp optimization algorithm for HLS of datapaths in digital filters and engineering applications," *Engineering with Computers*, 2021. https://doi.org/10.1007/s00366-020-01233-2.

[17] M. A. M. Shaheen, H. M. Hasanien, M. S. E. Moursi and A. A. E. Fergany, "Precise modeling of PEM fuel cell using improved chaotic MayFly optimization algorithm," *International Journal of Energy Research*, vol. 45, no. 13, pp. 18754–18769, 2021.

[18] P. Mohapatra, S. Chakravarty and P. K. Dash, "Microarray medical data classification using kernel ridge regression and modified cat swarm optimization based gene selection system," *Swarm and Evolutionary Computation*, vol. 28, pp. 144–160, 2016.

[19] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li *et al.,* "An optimization method for intrusion detection classification model based on deep belief network," *IEEE Access*, vol. 7, pp. 87593–87605, 2019.