






Research Article

Advanced cyber security using Spectral entity feature selection based on Cyber Crypto Proof Security Protocol (C2PSP)

S.Gopalakrishnan¹,, Karabi Saikia²,, Vallem Ranadheer Reddy³,

¹Department of Electronics and Communication Engineering, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai-600062,

²Department of Mathematics, Dhakuakhana College, Assam 787055. India

³Chaitanya Deemed To Be University, Kishanpura, Hanamkonda, Warangal -506001, Telangana, India,

ARTICLE INFO

Article History

Received 5 Jan 2023
Accepted 25 Feb 2023
Published 27 Feb 2023

Keywords

cyber security
data analysis
crypto security
feature selection
attack detection



ABSTRACT

The growth of the internet has become more developed in communication mediums to provide various services. Crime attackers predominantly suffer from information sharing and security because attackers carry out different models of cyber-attacks. Attackers create jamming principles, communication delays, packet dropping, and information hacking, duplicate injection to do so many activities to destroy security. Based on the communication data analysis, and features are non-identified, and challenging to find malicious activities. So the development of cyber security needs advancement to find the attackers based on communication-breaking activities. To resolve this problem, we propose a Spectral entity feature selection based Cyber Crypto Proof Security Protocol (C2PSP) to improve cyber security. The Defect Scaling Rate (DSR) estimates the communication defect rate. Marginalizing the scaling rate using the Spectral entity feature selection approach (SEFSA) is applied to select the features and trained to identify with an Artificial neural network classifier (ANN). Based on the attack principles and activities in the communication medium, the Cyber Crypto Proof Security Protocol (C2PSP) is applied to ensure the security verification and validation to process the data safer and securely. The proposed system produces high performance compared to other systems to identify malicious activities to improve security against cyber-attacks.

1. INTRODUCTION

Cybercriminals and malware builders have tailored code obfuscation techniques that undermine the effectiveness of cybersecurity mechanisms [1]. The consequently proposed a gadget that specializes in static evaluation further to an automatic behavioral evaluation in emulated surroundings that generates behavioral reviews to analyze malware. The proposed approach makes use of applications such to analyses the network histograms and decreases the explosion of features. Using the data analysis ANN model decrease misclassification and interference of features. Our gadget makes use of a hybrid approach to detect malware primarily based totally on a help vector machine classifier, in order that the functionality of the malware detection gadget may be combated with special kinds of malware at the same time as attaining excessive accuracy and low false alarms [2].

At the same time, service providers, might be in need to collect the history of the network traffic and alarm log for further analysis, or it is necessary to detect the correlation between the alarm of a distributed attack. This proposed system based on the feature selection and classification approach. These models are used to analyze the user's trust level in multi-level intrusion detection system is recommended [3]. Specific use of each user's risk level it can bring a selection of effective security strategy for the user. If the risk level feature is determined, in order to select the correct IDS to active on the user's virtual machine. The algorithm shows that is capable to propose a minimum reach false alarms that can be used in a variety of situations in a variety of ways. It means low risk of consuming an efficient computing resource for each in cloud environment it use lightweight intrusion detection system can be associated with computing resources effectively.

2. RELATED WORK

Most of the exiting survey describes cyber security threats in IoT. Multi Classifier Intrusion Detection system (MCIDS) has been proposed based on a DL algorithm for IoT threats assaults [4]. Traditional IDS structures aren't designed to paint efficiently in an IoT network as those devices have restricted sources and sparse functionality.

After analyzing the advancement of technology, the introduction and proliferation of cyber threats and attacks has grown exponentially due to the ever-present use of the Internet [5], computers, clever phones and tablets. As a result, anti-virus businesses and researchers have developed new procedures to detect and classify cyber threads [6].

Among these, system getting-to-know and large data technology are used for function extraction, detection, and clustering of cyber threats, we created and analyzed a dataset from darknet and easy documents (desirable devices) from static and dynamic features of the online architecture [6,7]. However, system logs network statistics, and file access are fake [8]. IoT security and privacy issues are major challenges, but they also help build a “trusted ecosystem” [9]. In fact, IoT device-specific vulnerabilities, limited resources, heterogeneous technologies, and the lack of well-designed IoT standards provide a good basis development of particular cyber threats [10].

Therefore, function selection turned into execution with the aid of using taking the maximum crucial capabilities [11], which lets in the improvement of tracking cyber detection programs with high accuracy and low overhead. In addition, type algorithms which include Random Forest (RF), Support Vector Machine (SVM), and Neural Networks (NN) had been utilized in a progressive combination [12]

3. PROPOSED IMPLEMENTATION

Towards the development of advanced cyber security using Spectral entity feature selection based on Cyber Crypto Proof Security Protocol (C2PSP) is implemented to improve the security. Initially the preprocessing is carried to normalize the data to make noise less feature verification. After that the features log verification, the Cyber defect scaling rate (CDSR) is estimated based on Trust intensive communication rate by the actual location, transmission authenticity, packet flow and delay rate is estimated. Figure 1 describes the proposed architecture diagram SEFSA- C²PSP for implementation of proposed system.

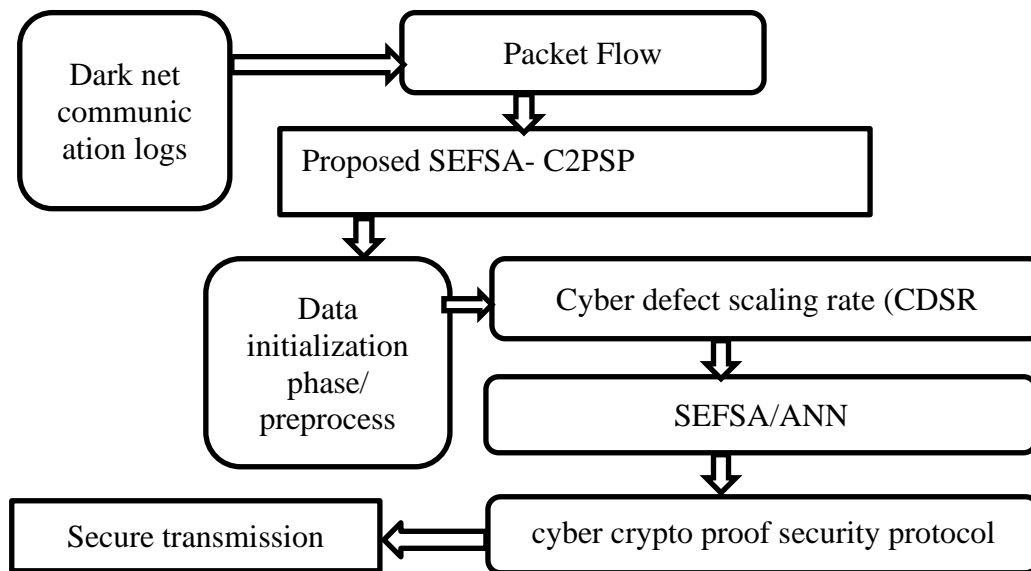


Fig. 1. Proposed architecture diagram SEFSA- C²PSP

Then Spectral entity feature selection approach (SEFSA) applied to select the features and classified with artificial neural network (ANN). Based on defect communication transmission. The cyber crypto proof security protocol (C²PSP) is applied to ensure the security verification and validation to process the data safer and securely.

3.1 Data initialization phase

In this stage communication logs are actuated by preprocessing based on Data cleaning, normalization, feature margin validation to correcting and removing incomplete data. To make marginalization to find the missing values and remove those rows. Using the pandas *dropna()* function to remove rows that contain null values in the Darknet /IoT- dataset.

dropna(nomarlization = scaling, ideal = margin ,thresh = set actual, feature = None = Remove False) .

// If the value is 1 drop column with missing values, 0 drop row with null values.

where, thresh – threshold value, subset – row and column null values, how – index values, axis–{‘0’ or index, ‘1’ or column}, in place – boolean values

After the preprocessing was done the feature selection and crypto protocol security is applied to improve the security.

3.2 Cyber defect scaling rate (CDSR)

This model creates the feature margin based on the defect rate to identify the cause of attack variation from actual metrics. Occurrence is based on failure probability, failure rate and unusable reason. To get the actual probability by comparing the ideal and actual values to get the probability of n phases is used to assess the probability ($p_{ij}(n)$) of optimistic phases.

$$p_{ij}(n) = p_{ij} \quad \text{And} \quad p_{ij}(n) = \Pr (X_{n+m} = k)|(X_n = i) \quad -$$

To calculate the changeover possibility for every progression

$$p_{ij}(n) = \Pr (X_m = k)|(X_{m-1} = i)$$

Following above equation represent a transition probability if the state $n \geq 1$, and 0 state-transition probability fault tree,

$$p_{ij}(0) = \{0, 1\}$$

Based on the probability the defects scaling features are marginalized to attain to consider the defect feature level.

3.3 Spectral entity feature selection approach (SEFSA) with ANN

In this stage , to generate synthetic data based on a small number of real data samples in a short training period, and use these synthetic data samples to augment the training data. From the estimated parameters, the values of the Gaussian kernel function and a linear polynomial are calculated to distinguish between legitimate nodes and malicious nodes in the network. Calculations are performed for the Eigen functions of each parameter.

Neural training is shown with the back propagation cross-entropy loss function Using the following equation. Figure 4.7 shows the GALNN- Neural training phase.

$$C(\theta) = \sum_i [y_T]_i \log(a^L(x_T)_i) + (1 - [y_T]_i) \log(1 - (a^L(x_T)_i))$$

By defining the parameters, where θ is the set of the neural network parameters, x_T is the training data vector, y_T is the label vector (Attacker/Normal), $a^L(x_T)$ is the output of the neural network at the last layer L.

To the attention of logical activation function the processing hidden layer are integration by constructing neural links based on GAN properties. In the hidden layer, sigmoid and hyperbolic tangent (Tanh) functions are discarded for implementation.

$$[\sigma(z)]_k = \frac{1}{1+e^{-zk}} , \frac{e^{zk} - e^{-zk}}{e^{zk} + e^{-zk}}$$

The z-input, k-entry count

The output layer is implemented using a smooth maximum activation problem with gradient descent given in the following equation.

$$[\sigma(z)]_k = \frac{e^z k}{\sum_j e^z j}$$

Finally the game theory model optimized with GAN to produce the predicted output for finding the jammers. Once the output value is activated, a mini-max game is initiated between the generator and the discriminator. The strategy of the game theory is explained by the equation,

$$\min_G \max_D \mathbb{E}_{x \sim p_{data}} [\log(D(x))] - \mathbb{E}_{z \sim p_{dataz}} [\log(1 - D(G(z)))]$$

Where representing the variable is defined by z- input error, p_{data} -data distribution, D-discriminator function, G-Generator function. After the mini-max game is over, the perceived output is the difference in behavior between the normal nodes and the attacking nodes. Classifies attacking hosts and excludes them from data transmission

3.4 Cyber Crypto Proof Security Protocol (C²PSP)

Finally the C²PSP security solutions that provide identity verification and data privacy fail to detect if internal nodes provide incorrect routing information or fail to cooperate with other nodes to secure resources. Detecting this type of fraud requires another layer of security measures. This layer is based on the concept of trust verification from cryptography security protocol.

Steps to Proceeds

Input: Number of node with data transmission packets.

Output: Term of request authenticity of Data packets

Step 1: Initilaze Network load balancer.

Compute the feature optimized level of detected cyber on graph level node transmission

Step 2: Node state active to valid

Transmission sink node varfied the route congestion to verify packets.

Get ack → valid

Compute crypto AES standard \$n0 set X_ 0.0 to n data

Generate key authentication validation protocol

Step 3: compute the requaet frokey of ack node

Step 4: validate node access= 1, to get packet ahndover

Estimate request consideration of key

If (Route==valid key)

Datpkt=0;I++

Step 5: verify the private key authentication access to get data

Packet::free with key match

End if

Step 6: For if Consistency buffering packet load key

Transfer data valid route ← receive packets.

Step 7: Else Key not proceed to reject route validation.

Accessing correct packet consumes resources and batch service for legitimate authorized request users. Provide continuous service, network, and adequate protection of bandwidth. . This time, the broadcasting mechanism first identifies the route list and packet request key pair you need to know the topographic information and traffic details. Use learned content, this method identifies the root list of the function the root is considered to be. For each method of identification key verified the packet flow, the system estimates the QoS support index for selection calls on routes that do not have a traffic at any time

4. RESULT AND DISCUSSION

The proposed implementation is tested on python language with an anaconda environment using publicly available cloud darknet dataset. IDS can be effectively detected by comparative parameters such as classification accuracy, sensitivity, specificity, false ratio and time complexity with the help of a confusion matrix. The comparison algorithms are Support Vector Machine (SVM), random forest classifier and ANN.

TABLE I: PERFORMANCE ON CYBER-ATTACK ACCURACY VS. NO OF SERVICES

Intrusion Detection Accuracy in % vs No of Services			
Comparison methods/ services	10 Services	20 Services	30 Services
SVM	70.9	73.6	78.3
RF	76.2	77.1	81.8
ANN	78.7	82.4	87.5
SEFSA- C2PSP	91.9	96.6	98.3

Table 1 describes the cyber-attack detection accuracy performance vs no of services with different techniques like SVM, and the proposed Model SEFSA- C2PSP.

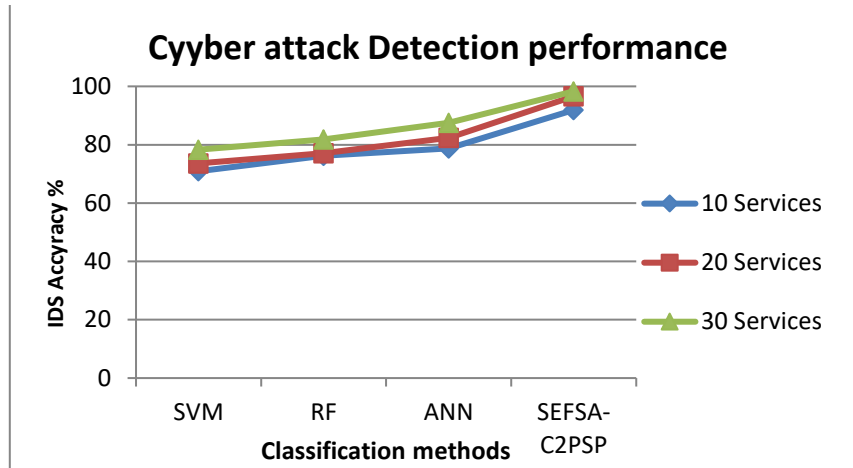


Fig. 2. Impact of cyber-attack detection accuracy performance

Figure 2 denotes impact of intrusion detection classification accuracy performance with various services like 10, 20 and 30. The proposed technique SEFSA- C2PSP method attained 98.3% produces better performance than other techniques.

TABLE II: IMPACT OF SENSITIVITY PERFORMANCE

Comparison methods/ services	10 Services	20 Services	30 Services
SVM (%)	68.6	71.8	77.1
RF (%)	73.2	75.6	80.7
ANN (%)	76.7	81.5	86.2
SEFSA- C2PSP (%)	89.3	94.5	97.1

Table 2 describes the impact of sensitivity performance the proposed compared with previous techniques.

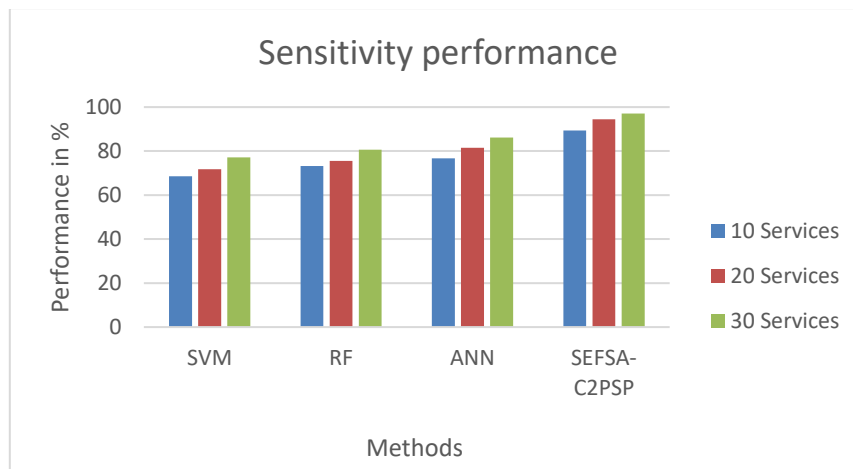


Fig. 3. Analysis of sensitivity performance

Figure 3 shows the sensitivity performance for Cyber detection using SEFSA- C2PSP algorithm. The proposed algorithm provide result is 96% of sensitivity performance for 30 services; similarly the exiting algorithm provide results are SVM is 76% attain low level rate.

TABLE III: IMPACT OF SPECIFICITY PERFORMANCE

Comparison methods/ services	10 Services	20 Services	30 Services
SVM (%)	71.2	72.6	78.4
RF (%)	78.7	76.8	83.6
ANN (%)	79.4	82.8	87.4
SEFSA- C2PSP (%)	90.8	95.2	96.8

Table 3 describes the analysis of specificity performance measures in different number of services such as 10, 20, and 30 services. The proposed technique provide better result than previous approaches.

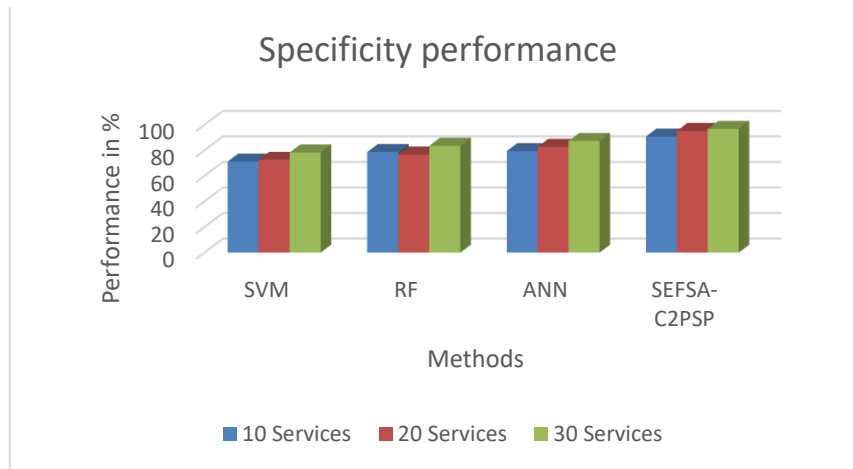


Fig. 4. Analysis of Specificity performance

Figure 4 illustrate the analysis of specificity performance the proposed and previous approaches comparison result presented. The proposed SEFSA- C2PSP algorithm has 97% of Specificity performance for 30 services; similarly the existing algorithm results are SVM is 77% of specificity performance, RF is 82% of specificity performance and ANN is 86% of specificity performance for 30 services.

TABLE IV: ANALYSIS ON FALSE CLASSIFICATION RATIO

False Classification Ratio in % vs No of Services			
Comparison methods/ services	10 Services	20 Services	30 Services
SVM	28.4	25.1	20.7
RF	23.5	21.4	16.9
ANN	20.7	16.9	12.6
SEFSA- C2PSP	6.7	2.4	1.3

Analysis of false classification ratio the proposed comparison with previous methods performance is listed in table 4.

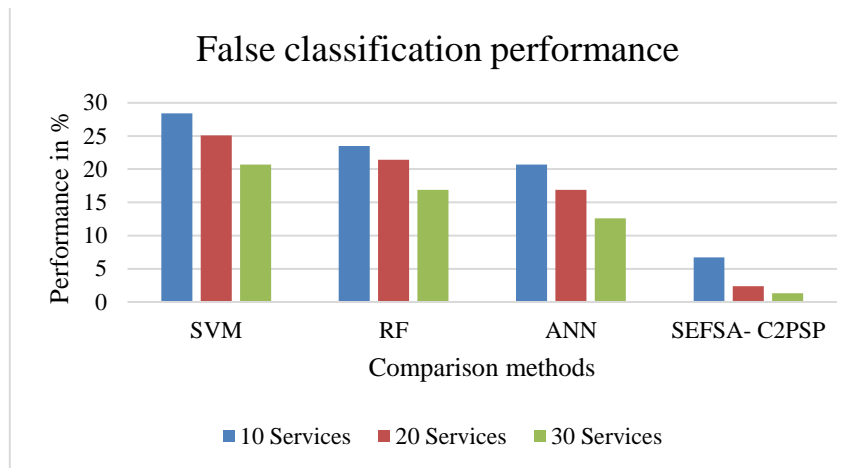


Fig. 5. Impact of false classification ratio

Figure 5 illustrates impact of false classification ratio performance for IDS with various services like 10, 20 and 30 services. In this graph, X-axis is a comparison method moreover Y-axis performance gradually decrease with each method. The proposed SEFSA- C2PSP method achieves 1.3% false classification performance compared to other system

5. CONCLUSION

The proposed cyber security system based on unusual outlier detection, using timestamp intrusion methods and delay-aware routing feature classification, gives high performance in intrusion detection. It predicts user behavior characteristics associated with malicious activity while accessing services by evaluating aggregation factors and packet loss-related characteristics. This system reduces the dimensionality of uncertain feature constraints to select and train a linear activation function. The importance of data analysis based on service access rate and throughput helps in cyber thread detection. The proposed SEFSA- C2PSP system achieves high performance as per the result proves to produce high performance.

Funding

Non.

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

Authors would like to thank the anonymous reviewers for their efforts.

REFERENCES

- [1] B. Li, P. Liu and L. Lin, "A Cluster-Based Intrusion Detection Framework for Monitoring the Traffic of Cloud Environments," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), 2016, pp. 42-45, doi: 10.1109/CSCloud.2016.43
- [2] O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha and K. Kim, "Data Randomization and Cluster-Based Partitioning for Botnet Intrusion Detection," in IEEE Transactions on Cybernetics, vol. 46, no. 8, pp. 1796-1806, Aug. 2016, doi: 10.1109/TCYB.2015.2490802
- [3] . Umbarkar and S. Shukla, "Analysis of Heuristic based Feature Reduction method in Intrusion Detection System," 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN), 2018, pp. 717-720, doi: 10.1109/SPIN.2018.8474283.
- [4] R. Vijayanand and D. Devaraj, "A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network," in IEEE Access, vol. 8, pp. 56847-56854, 2020, doi: 10.1109/ACCESS.2020.2978035.
- [5] S. Singh, S. V. Fernandes, V. Padmanabha and P. Rubini, "MCIDS-Multi Classifier Intrusion Detection system for IoT Cyber Attack using Deep Learning algorithm," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 354-360, doi: 10.1109/ICICV50876.2021.9388579.

- [6] H .Hassan, El-Desouky A. I, Ibrahim A, El-Kenawy E. M and Arnous R, "Enhanced QoS-Based Model for Trust Assessment in Cloud Computing Environment," in *IEEE Access*, vol. 8, pp. 43752-43763, 2020.
 - [7] T.H.Divyasree, "A Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach", Elsevier, *Procedia Computer Science*, vol.143, 2018.
 - [8] Z .Chkirbene, Erbad A, Hamila R, Mohamed A, Guizani M and Hamdi M, "TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection," in *IEEE Access*, vol. 8, pp. 95864-95877, 2020.
 - [9] W. Alhakami, A. ALharbi, S. Bourouis, R. Alroobaea and N. Bouguila, "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection," in *IEEE Access*, vol. 7, pp. 52181-52190, 2019, doi: 10.1109/ACCESS.2019.2912115
 - [10] L. Dali, K. Mivule and H. El-Sayed, "A heuristic attack detection approach using the "least weighted" attributes for cyber security data," 2017 *Intelligent Systems Conference (IntelliSys)*, 2017, pp. 1067-1073, doi: 10.1109/IntelliSys.2017.8324260.
 - [11] Z. Salek and F. M. Madani, "Multi-level Intrusion detection system in cloud environment based on trust level," *IEEE (ICCKE)*, 2016, pp. 94-99.
 - [12] Ali M, Malik S. U. R and Khan S. U., "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party," in *IEEE Transactions on Cloud Computing*, vol. 5, no. 4, pp. 642-655, 1 Oct-Dec. 2017.
 - [13] J. Liu and S. S. Chung, "Automatic Feature Extraction and Selection For Machine Learning Based Intrusion Detection," 2019 *IEEE SCALCOM/UIC/ATC/CBDCom/IOP/SCI*, 2019, pp. 1400-1405, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00254
 - [14] X. Xu et al., "PDM: Privacy-Aware Deployment of Machine-Learning Applications for Industrial Cyber-Physical Cloud Systems," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5819-5828, Aug. 2021, doi: 10.1109/TII.2020.3031440.
- W. A. H. M. Ghanem et al., "Cyber Intrusion Detection System Based on a Multiobjective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks," in *IEEE Access*, vol. 10, pp. 76318-76339, 2022, doi: 10.1109/ACCESS.2022.3192472