*Nanotechnology Perceptions*
*ISSN 1660-6795*
*www.nano-ntp.com*

# Deep Learning to Improve Cyber Security: Swarm-Intelligent Fully Convolutional Neural Network Model for Efficient Intrusion Detection in Big Data Environment

**Iti Dayal[1], Jaskirat Singh[2], Nidhi Saraswat[3], Dr. Jaykumar Padmanabhan[4], Ashmeet Kaur[5], Dr. Priyanka Chandani[6]**

*[1]Assistant Professor, Department of Management Studies, Vivekananda Global University, Jaipur, India, Email Id- iti.dayal@vgu.ac.in*
*[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India jaskirat.singh.orp@chitkara.edu.in*
*[3]Assistant Professor, Department of Computer Science & Engineering, Sanskriti University, Mathura, Uttar Pradesh, India, Email Id- nidhi.soeit@sanskriti.edu.in*
*[4]Associate Professor, Department of Decision Science, JAIN (Deemed-to-be Univesity), Bangalore, Karnataka, India, Email Id- dr.jaykumar_padmanabhan@cms.ac.in*
*[5]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103 India, Email Id- ashmeet.kaur.orp@chitkara.edu.in*
*[6]Associate Professor and HOD, Department of CSE(Data Science), Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, Email Id- priyanka.chandani@niet.co.in*

Introduction: In the digitally interconnected world, Cyber security has become a pressing concern, necessitating the development of advanced intrusion detection systems to protect sensitive information and critical infrastructure from rising security threats in networks, the Internet, websites, and organizations, even though detecting intrusions in this vast data environment remains difficult.

Methods: Intrusion-detection systems (IDSs) have been developed using machine learning methods to detect internet attacks. However, these systems often fail to distinguish unexpected attacks or respond in real-time. This research proposed a novel Deep Learning approach called Swarm-Intelligent Fully Convolutional Neural Network (SIFCNN) for effective intrusion detection in large data environments. The technique used the NSL-KDD dataset, developed from the KDDCUP99 dataset, and employs z-score normalization and Independent Component Analysis (ICA) to extract features and improve discriminative ability. The SIFCNN model learns complex normal and harmful behavior patterns from large datasets, and uses the Lion Swarm Optimization (LSO) method to adjust hyper parameters, improving flexibility in response to changing attack patterns

and network conditions.
Result: The SIFCNN method, compared to traditional methods, demonstrated satisfactory efficiency in conditions of precision, recall, accuracy and F1 score on available dataset.
Conclusion: The adaptability to emerging threats and real-time intrusion detection makes it a promising tool for cyber defenses.

**Keywords:** Cyber Security, Big Data Environment, Intrusion Detection, Swarm-Intelligent Fully Convolutional Neural Network (SI-FCNN).

## 1. Introduction

Most sectors are moving toward artificial intelligence (AI) as the next big thing in technology. The last several years have shown that many companies are using AI to aid with various services. [(1)] The effect of these rollouts has been increased confidence in AI. As a result, the effectiveness of using AI to build a defense against cyber-attacks is established. [(2)] Exploitation of intellectual property and fraud are only two examples of digital crime. The majority of hackers did to make revenue.[(3)] It has been observed that some phishing attempts Combine Social Construction with AI techniques.[(4)] This is another proof that anti-phishing tools are practical.[(5)] The list of AI applications has been linked to expanding cyber security across several sectors. Automation's primary goals have been reduced to human involvement and boost efficiency. [(6)] Identifying unidentified dangerous code is constrained in a system based on the host. [(7)] Most of these traits are connected to society's use of artificial intelligence. [(8)] A signature might be anything from a recognized pattern or sequence utilized by malware to a byte sequence in network data.[(9)] Hacking focuses on Critical National Infrastructures (CNIs), Monitoring, and obtaining the transmission control protocol.[(10)] It originates from an antivirus program that labels the collections or patterns inside it as signatures.[(11)] Anomalies will look them by creating a model based on data profiles that anticipated behaviors.[(12)] The author [(13)] suggested that AI has become crucial to all businesses. Figure 1 shows the cyber security lifecycle. The study [(14)] provided many relevant applications with the remarkable expansion of computer networks. The paper [(15)] described safety concerns associated with the rise in internet use. AI-based techniques have been employed to construct IDS systems.

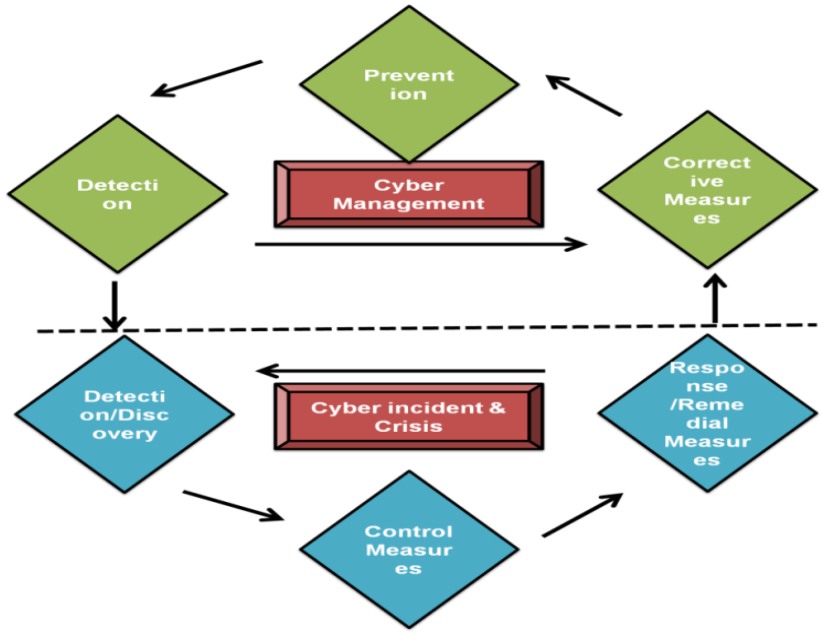



Figure 1. Cybersecurity Lifecycle (Source: https://www.researchgate.net/figure/Cyber-Security-Lifecycle_fig1_332995477)

The author [16] provided an overview of deep learning techniques, datasets, and a comparative analysis for cyber security. The author [17] provided smart services in the security field online and the Bayesian Network is one of the machine learning (ML) classification methods employed in this paper. The study [18] described that the increasing interconnection of field equipment and computer nodes has made network-based cyber-attacks seriously threatening the design of Industrial Control Systems (ICS) networks. The author [19] described ML-based systems as used as viable remedies to identify intrusions across networks effectively. The paper [20] provided that Cities are transformed by the IoT, transformational change. The study [21] described computer systems' increasing interconnectedness and interoperability. The author [22] described security as the most important factor regarding data breaches or information protection. The paper [23] determined Network managers may concentrate on developing their network security and resource-saving strategies by studying intrusion detection systems (IDS).

The objective of this study is to improve intrusion detection in large-scale information settings by putting forth a unique Deep Learning technique that can identify unexpected attacks and adjust to changing network conditions.

## 2. Methods and Materials

Review the data preprocessing technique following a description of the cyber security intrusion detection dataset. We provide the architecture and theoretical basis of the

suggested composite deep learning model. Figure 2 depicts the theoretical process model.

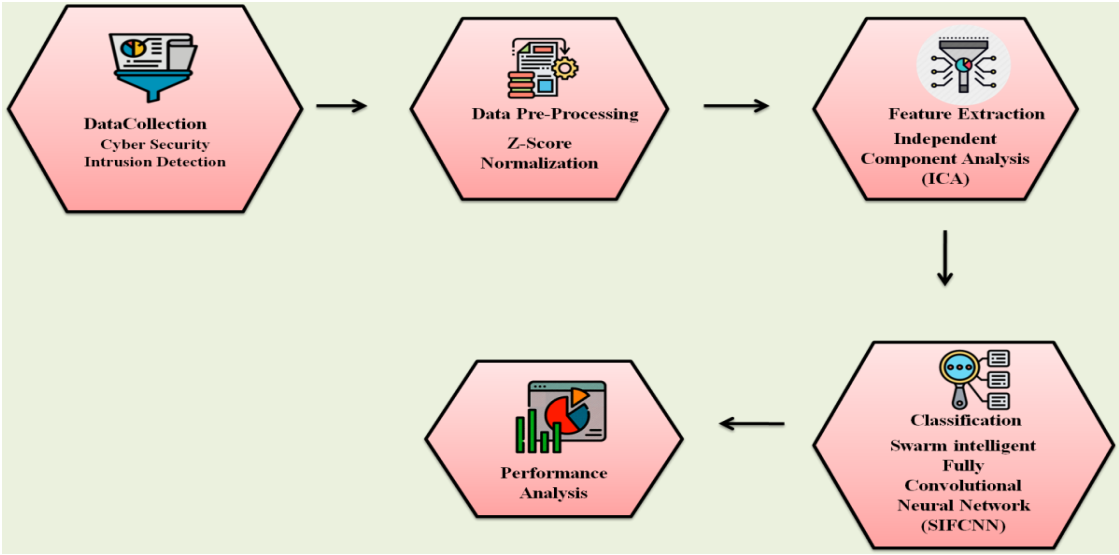



Figure 2. Suggested schematic structure [Source: Author]

Dataset for detection of intrusions in cyber security

As the source of the NSL-KDD dataset, a most frequently used data collection is KDDCUP99. Both datasets are effectively used by the proposed method. KDDCUP99 expands upon the DARPA dataset. There is a great deal of redundant information. However, the KDDCUP99 information is no longer included in the NSL KDD dataset's redundant duplicate entries. To make the dataset more difficult, new attack types are also added. The dataset is shown together with one label class in Table 1. Possess 41 traits in common, including assault and standard class categories.[24]

Table 1. Identification of Attacks in the KDD CUP Dataset[24]

| Concepts | Land | teardrop | Back | Neptune | Land |
|---|---|---|---|---|---|
| Remote to local | Load module | Perl | Buffer overflow | Rootkit | Load module |
| User to Root | Nmap | Upsweep | Satan | ports weep | Nmap |
| Probe | map | Password | Multihop | ftp write | map |

Data preprocessing using z-score normalization

Z-score normalization makes modifications based on the data's mean and standard deviation. This approach works when it is determined what the data's lowest and maximum values represent. To calculate, use this formula:

$$s_{new} = \frac{t-\mu}{\sigma} = \frac{t-Mean(t)}{stdDev(t)} \quad (1)$$

$s_{new}$=transforming the data, T= the corrected value, S= outdated value, μ =Statistics mean, σ =Standard Deviation

Feature extraction using ICA

One method to find ICA is with a fixed-point approach. Fast ICA is based on a fixed-point iteration method that determines the non-guassianity's most significant value.

Algorithm: Independent component analysis

Select m, the desired ICA constituent estimates dimension.

Filter the information to reveal Y.

Pick the appropriate blending vector. y.

They orthogonalized the matrix y.

Let $y_1 \leftarrow F\left\{x_h\left(W^S Y\right)\right\} - F\{G'(S_Y)\}y$,

Where h is defined as

$h(z) = \tanh(z)$ or

$h(z) = z^3$

Matrix with orthogonal bases X

If convergence has not occurred, repeat step 6

Go to step 6 for the subsequent ICA.

Perform for $k = 1,2,3,4 \ldots . n$

## 3. Theoretical Concepts for the Proposed Framework Using Swarm Intelligent Fully Convolutional Neural Network (Sifcnn)

It is a particular model or methodology that integrates the components discussed above, including swarm intelligence, to enhance flexibility and efficacy in intrusion detection inside large data settings. Cyber security requires processing and analyzing massive amounts of data.

Fully Convolutional Neural Network (FCNN)

In SIFCNN, pooling serves the sampling function, which substitutes the surrounding neighbor pixels with summarised features in the output at that position. The maximization procedure causes some geographic data to be lost, but skip connections allow for more significant data on the final layer, increasing the classification quality.

$$p_i(g) = \begin{cases} g(x_{ipi}(g-1) + x_i(p_i - 1(g) + e_i(h)))ikj > 1 \\ g\left(x_{ipi}((g-1)) + x_i\left(W_i + \theta(p_h)\right)\right)ikj > 1 \end{cases} \quad (2)$$

The $j^{th}$ layers of state t neurons are in constant two-way communication with the $i^{th}$ layer of stated $+ 1$.

$$I(r) = I_0 \exp(-\gamma . r_{ij}) \quad (3)$$

Lion Swarm Optimization (LSO)

Investigators created the groundbreaking swarming intelligent optimization technique. The most crucial elements in their calculations are the pups. The fundamental tenet of this strategy is that the two lionesses should cooperate to match the circumstances that provide the most significant values for the functioning goals to determine the best dominance objective.

Step 1: Initiate the current situation. The GLSO objective function l (x), location $x_i = (x_i\,1, x_i\,2, \ldots, x_i\,z)$ of the Jth one of the criteria of the structure is the number of lions in a large swarm.

Step 2: In the lion-king, we utilize formulas (4), and (5).

$o \leq \frac{1}{3}$ According to equation (5), the lion babies eat near their mother.

$\frac{1}{3} < o \leq \frac{2}{3}$ proves that adult females and cubs hunt together.

$$v_i^{f+1} = z^g(1 + \gamma|\left|q_i^g - z^g\right||) \quad (4)$$

$$v_i^{f+1} = \frac{q_i^f + q_t^f}{2}(1 + \propto_j \gamma) \quad (5)$$

Step 3: Calculate the objective functional score. Change the optimal settings before $p_j^k$ from each separate lion and the $s^r$ of the animal group using the updated coordinates for each lion obtained in phase 2 from the target variable. The location of the lion king is re-evaluated. If not, move to step 2.

## 4. Results

This article discusses existing methods in order to examine the suggested model; "Naive Bayes (NB) [25], Logistic Regression (LR) [25], k-Nearest Neighbors (KNN) [25], Support Vector Machine (SVM) [25], and (Intrud Tree)" [25]. The following parameters were chosen: recall, f1 score, accuracy, and precision. The proposed and existing approach results are displayed in Table 2.

Table 2. Proposed and existing approach results [Source: Author]

| Methods | Accuracy% | Recall% | F1-score% | Precision% |
|---|---|---|---|---|
| NB | 90 | 90 | 90 | 88 |
| LR | 94 | 94 | 94 | 93 |
| KNN | 94 | 94 | 94 | 94 |
| SVM | 96 | 95 | 96 | 95 |
| Intrud Tree | 96 | 98 | 98 | 98 |
| SIFCNN (proposed) | 99 | 99 | 99 | 99 |

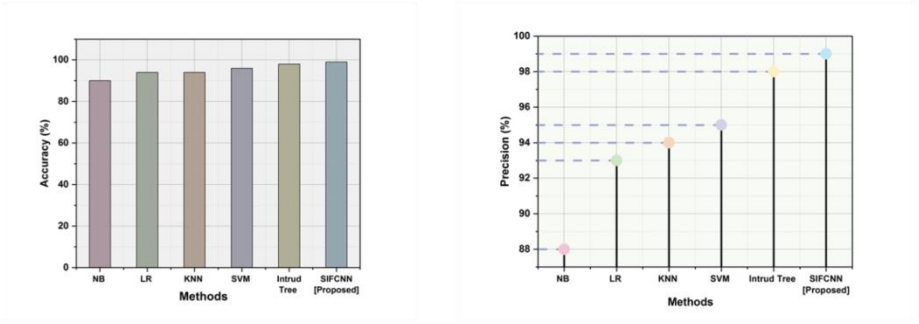
The result of insufficient accuracy is the disparity among the real number and the outcome. The proportion of actual outcomes demonstrates and evenly distributed the data are globally.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

Display the comparable values, accuracy measurements compared to the employed techniques. NB, LR, KNN, SVM, and Intrud Tree exhibit 90 %, 94 %, 96 % and 98 % of accuracy rates, respectively. With an exceptional accuracy of 99 %, the suggested method, Integrated SIFCNN, is highly effective. This method outperforms the others in terms of performance. The proportion of properly categorized incidents to the total population of cases with predicatively accurate information constitutes the definition of precision, which is an essential part of accuracy as shown in Figure 3(a).

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{6}$$

Currently, the recognizing rates of NB, LR, KNN, SVM, and Intrud Tree are 88 %, 93 %, 94 %, 95 %, and 98 %. The impressive 99 % accuracy rate of the suggested technology SIFCNN is special. This method is superior to an existing plan. The recall rate measures how a model can identify each outlier within the same data set. A quantitative definition can be found in Figure 3(b), it shows the ratio of proper diagnoses to the sum of both accurate and inaccurate conclusions.




(a) (b)

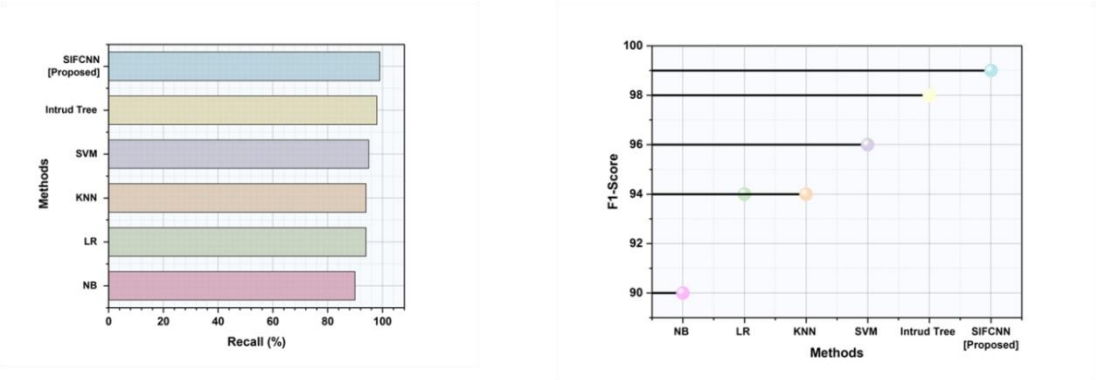
Figure 3. Outcomes of (a) Accuracy and (b) Precision [Source: Author]

An equation that provides the corresponding recall measurement comparison data can determine the recall. The NB, LR, KNN, SVM, and Intrud Tree had above-average recall rates of 90 %, 94 %, 94 %, 95 %, 98 % and 99 %. The suggested method outperformed the modern with an SIFCNN recall of 99% as shown in Figure 4(a).

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{7}$$

The accuracy and recall components of the F1 score are metrics for testing the model's accuracy and is calculated using a single number considering both measures. The proposed method merges recall and precision into a single statistic called the f1-score. Our suggested technique achieves 90 %, 94 %, 94 %, 96 %, and 98 %, while current methods like NB, LR, KNN, SVM, and Intrud Tree only manage and only manage 99 % in this comparison. It proves that our proposed method is superior to the status as shown in Figure 4(b).

$$F1-score = \frac{2\times precision\times recall}{precision+recall} \quad (8)$$




(a) (b)

Figure 4. Outcomes of (a) Recall and (b) F1 score (Source: Author)

## 5. Discussion

The efficiency of the conventional well-liked machine learning-based techniques is compared to our Intrud Tree Model for Detecting Cyber Attacks. We initially compare the machine learning-based security algorithms to industry standard methods like NB, LR, KNN, and SVM, which stand for Naive Bayes, Logistic Regression, and K-Nearest Neighbor, respectively. To show their superiority. After analyzing the cyber security data, our swarm intelligence fully convolutional neural network (SIFCNN) model performs better than the conventional deep learning classification-based techniques.

## 6. Conclusion

We suggested a deep learning SIFCNN for a vast data setting. The deep CNN uses its weight-sharing characteristic to its advantage to extract significant features from the incursion data. The extensive data research demonstrated excellent performance, with 99 % accuracy. The SIFCNN model and other deep learning techniques have many potential applications in large data settings for enhancing intrusion detection. Cyber threats will keep investigating novel approaches and strategies to improve the security of digital systems and networks.

## References

1. Yang H, Cheng L, Chuah MC. Deep-learning-based network intrusion detection for SCADA systems. 2019 IEEE Conference on Communications and Network Security (CNS) 2019 Jun 10 (pp. 1-7). IEEE. Doi: https://doi.org/10.1109/CNS.2019.8802785
2. Zeadally S, Adi E, Baig Z, Khan IA. Harnessing artificial intelligence capabilities to improve

Cybersecurity. Ieee Access. 2020 Jan 20;8:23817-37. Doi: https://doi.org/10.1109/ACCESS.2020.2968045

3. Toliupa S, Nakonechnyi V, Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Collection" Information Technology and Security". 2019 Jun 30;7(1):69-79. Doi: https://doi.org/10.20535/2411-1031.2019.7.1.184326
4. Tao F, Akhtar MS, Jiayuan Z. The future of artificial intelligence in Cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies. 2021 Jul 7;8(28):e3-. https://doi.org/10.4108/eai.7-7-2021.170285
5. Shneiderman B. Human-centered artificial intelligence: Reliable, safe & trustworthy. International Journal of Human–Computer Interaction. 2020 Apr 2;36(6):495-504.Doi: https://doi.org/10.1080/10447318.2020.1741118
6. Tsimenidis S, Lagkas T, Rantos K. Deep learning in IoT intrusion detection. Journal of network and systems management. 2022 Jan;30:1-40. Doi: https://doi.org/10.1016/j.jksuci.2021.12.008
7. Dash B, Ansari MF, Sharma P, Ali A. Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications (IJSEA). 2022 Sep;13(5).
8. Cyriac NT, Sadath L. Is Cybersecurity enough to study big data security Breaches in financial institutions. 2019 4th International Conference on Information Systems and Computer Networks (ISCON) 2019 Nov 21 (pp. 380-385). IEEE. Doi: https://doi.org/10.1109/ISCON47742.2019.9036294
9. Ferrag MA, Maglaras L, Moschoyiannis S, Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications. 2020 Feb 1;50:102419. Doi: https://doi.org/10.1016/j.jisa.2019.102419
10. Asif M, Abbas S, Khan MA, Fatima A, Khan MA, Lee SW. MapReduce-based intelligent model for intrusion detection using machine learning technique. Journal of King Saud University-Computer and Information Sciences. 2021 Dec 16. Doi: https://doi.org/10.1016/j.jksuci.2021.12.008
11. Fu S. Data-driven user authentication with multi-level behavior profiling (Doctoral dissertation, Iowa State University). Doi: https://doi.org/10.1016/j.ress.2023.109323
12. Maniriho P, Niyigaba E, Bizimana Z, Twiringiyimana V, Mahoro LJ, Ahmad T. Anomaly-based intrusion detection approach for IoT networks using machine learning. 2020 International Conference on Computer Engineering, network, and Intelligent Multimedia (CENIM) 2020 Nov 17 (pp. 303-308). IEEE. Doi: https://doi.org/10.1109/CENIM51130.2020.9297958
13. Sarker IH, Furhad MH, Nowrozy R. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science. 2021 May;2:1-8. Doi: https://doi.org/10.1007/s42979-021-00557-0
14. Abou El Houda Z, Brik B, Khoukhi L. "why should I trust your IDs?": An explainable deep learning framework for intrusion detection systems in Internet of Things networks. IEEE Open Journal of the Communications Society. 2022 Jul 11;3:1164-76. Doi: https://doi.org/10.1109/OJCOMS.2022.3188750
15. Jain J. Artificial intelligence in the cyber security environment. Artificial Intelligence and Data Mining Approaches in Security Frameworks. 2021 Aug 23:101-17. Doi: https://doi.org/10.1002/9781119760429.ch6
16. Mighan SN, Kahani M. A novel scalable intrusion detection system based on deep learning. International Journal of Information Security. 2021 Jun;20:387-403. Doi: https://doi.org/10.1007/s10207-020-00508-5

17. Saba T, Rehman A, Sadad T, Kolivand H, Bahaj SA. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022 Apr 1;99:107810. Doi: https://doi.org/10.1016/j.compeleceng.2022.107810
18. Kilincer IF, Ertam F, Sengur A. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks. 2021 Apr 7;188:107840. Doi: https://doi.org/10.1016/j.comnet.2021.107840
19. Bhardwaj A, Al-Turjman F, Kumar M, Stephan T, Mostarda L. Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems. IEEE Access. 2020 Jun 1;8:104956-66. Doi: https://doi.org/10.1109/ACCESS.2020.2998983
20. Peng C, Sun H, Yang M, Wang YL. A survey on security communication and control for smart grids under malicious cyber attacks. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019 Jan 1;49(8):1554-69. Doi: https://doi.org/10.1109/TSMC.2018.2884952
21. Amanoul SV, Abdulazeez AM, Zeebare DQ, Ahmed FY. Intrusion detection systems based on machine learning algorithms. In2021 IEEE International Conference on automatic control & intelligent systems (I2CACIS) 2021 Jun 26 (pp. 282-287). IEEE. Doi: https://doi.org/10.1109/I2CACIS52118.2021.9495897
22. Injadat M, Moubayed A, Nassif AB, Shami A. Multi-stage optimized machine learning framework for network intrusion detection. IEEE Transactions on Network and Service Management. 2020 Aug 7;18(2):1803-16. Doi: https://doi.org/10.1109/TNSM.2020.3014929
23. Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies. 2021 Jan;32(1):e4150. Doi: https://doi.org/10.1002/ett.4150
24. Rani D, Kaushal NC. Supervised machine learning based network intrusion detection system for Internet of Things. In2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) 2020 Jul 1 (pp. 1-7). IEEE. Doi: https://doi.org/10.1109/ICCCNT49239.2020.9225340
25. Sarker IH, Abushark YB, Alsolami F, Khan AI. Intrudtree: a machine learning based cyber security intrusion detection model. Symmetry. 2020 May 6;12(5):754. Doi: https://doi.org/10.3390/sym12050754