Original Article

Parametric Influence Of Intrusion Detection System In Healthcare Sector Using Deep Neural [LSTM] Network

Monika Khatkar[1]*, Kaushal Kumar[2], Brijesh Kumar[3], Pankaj Agarwal[1]

[1]*Member of the Centre of Excellence, School of Engineering and Technology, K R Mangalam University, Gurgaon, 122103, Haryana, India
[2]School of Engineering and Technology, K R Mangalam University, Gurgaon, 122103, Haryana, India
[3]Department of Computer Science and Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, 121010, Haryana, India

***Corresponding Author:** Monika Khatkar

*Member of the Centre of Excellence, School of Engineering and Technology, K R Mangalam University, Gurgaon, 122103, Haryana, India
DOI:10.47750/pnr.2023.14.S01.93

Abstract

With the recent advancements of computer connectivity and the number of computer-related applications, the challenge of achieving cyber security has increased. It also necessitates a strong defence system against a variety of cyber-attacks in healthcare, Manufacturing, Transportation and Government sector as well. Furthermore, the presence of trespassers with the intent to launch various attacks within the healthcare network should not be underestimated. The most focused framework intrusion detection system protects the healthcare infrastructure from potential intrusions by inspecting network traffic to ensure its confidentiality, integrity, and availability. ML techniques also offer the opportunity to detect and monitor network security issues in healthcare sectors caused by the emergence of programmable features. Recently, AI (ML) and deep learning-based interruption detection frameworks (IDS) have been used as potential solutions for proficiently recognizing network interruptions. In this research, a deep learning-based LSTM model is used on the NSL-KDD dataset. Dataset used in the study is collected from the website of New Brunswick University. Popular classification algorithms, Random Tree, Decision Tree, SVM, KNN, Decision Tree, ANN (Artificial Neural Network), and Deep Neural Network are used to detect the interferences**.** To justify the superiority of LSTM, performance metrics, precision, recall, f1-score, and accuracy are evaluated with Denial-of-Service cyber-attacks. The experimental result shows LSTM model outperforms in the case of an intrusion detection system.
This study first describes IDS and then provides a categorization based on the notable ML and DL methods used in the designing of Network-Based IDS (NIDS) systems.

Keywords: Cyber Security, Healthcare Network, Intrusion Detection System, Machine learning, Confusion Metrics, LSTM

INTRODUCTION:

With the recent awareness and progression of the internet as well as communication technologies over the last decade, network sanctuary has arisen as an important research domain. It makes use of tools such as a firewall, antivirus software, and an intrusion detection system to ensure the safety of the network and all its associated assets in cyberspace. Among these, network intrusion recognition systems are attack detection mechanisms that provide the desired security by continuously monitoring network traffic for malicious and suspicious behaviour. However, the tremendous evolution of technology over the last decade has resulted in a significant increase in network size and the number of applications handled by network nodes. Subsequently, a significant quantity of critical data is generated and dispersed across various network nodes. The safety of such networks and data nodes has become a tedious task owing to the emergence of many new attacks, either through the mutation of an old attack or through the development of a novel attack. Furthermore, the availability of trespassers with the intent to initiate various attacks within the network cannot be overlooked. Almost every node in the network is susceptible to security. Jim Anderson first proposed the concept of IDS in 1980. Many IDS products have been developed and matured since then to come across the needs of network security. Two broad terms that refer to application security practices are intrusion detection and prevention systems used to mitigate intruders and block new threats.

The Intrusion Detection System (IDS) is a private eye-like device that detects malicious activity. They operate actively gating, (in the case of NIPS) and passively monitoring network traffic and applying rules or signatures to generate alerts. As a features target, it contains several types of features as a predictor to distinguish normal attacks from abnormal ones. IDS is a machine learning classifier that is frequently used to differentiate between different types of attacks. Decision Trees, Nave Bayes, K-Nearest Neighbour, Tree C4.5, Random Forest, Support Vector Machine, and Logistic Regression are a few of the supervised classification methods that are used in IDS. To classify and anticipate possible threats, classification algorithms are evaluated using a variety of statistical metrics, especially confusion matrix results.

To acquire useful information from network traffic, the ML-based IDS relies heavily on feature engineering means how raw data can be altered into variables for predicting modeling. While DL-based intrusion detection systems do not rely on data pre-processing and are capable of automatically learning complicated attributes from the input data due to the abundance structure. Deep learning is often used in cybersecurity, for example, to classify threats and distinguish anomalous behavior. There are also numerous open-source software libraries available for deep learning.

Here we analysed different classification or intrusion detection technique that uses machine learning and deep learning to detect attacks. We analyzed intrusion detection systems using Tensor Flow and deep learning here, we use TensorFlow, an open-source software library developed by Google, to perform deep learning and deep neural networks. Despite significant efforts by scientists, IDS continues to face challenges in improving recognition precision while reducing false alert rates and distinguishing novel interruptions. The primary goal of this research is to evaluate machine learning techniques for investigating specific aspects of DDoS attack detection to select the best one. In this paper, we extend our previous work and test various machine-learning approaches for malicious activities such as DDoS.

This research first discusses fundamental knowledge and the classification model. Next about the machine learning and deep learning models with experimental analysis of classification model in terms of metrics such as sensitivity, specificity, and accuracy.

An IDS (Intrusion Detection System) is a network security solution that was primarily designed to detect potential attacks against a specific application or computer. If properly configured, it can analyse incoming and outgoing network records and continuously monitor network patterns and notifies you immediately of any unexpected system behaviour. IDS can be categorized into two types depending upon their functioning i.e. active and passive.

1. Active IDS: Active IDS are systems that take preventative measures against an attack by blocking suspicious traffic.
2. Passive IDS: Passive IDS will simply monitor and analyse traffic, alerting the administrator about attacks in addition to vulnerabilities.

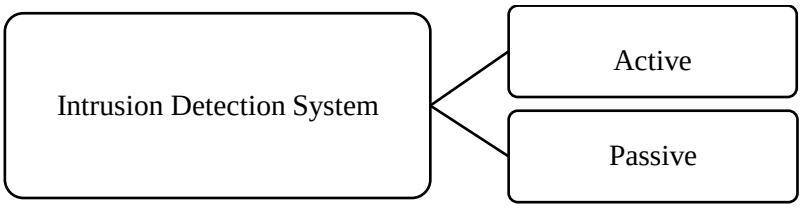

Fig 1. Categories of Intrusion Detection System based on action

There are several IDS based on their functions and how they perform, which are explained below:

1. Network intrusion detection systems (NIDS): A system that monitors and analyses incoming network traffic. Here, it can detect multiple hosts' malicious activities but if a network is busy then the packet processing rate will be smaller as compared to incoming data [4].
2. Host-based intrusion detection systems (HIDS): This system keeps track of critical operating system files and it can respond to long-term attacks [4].
3. Signature-based: A signature-based interfering detection scheme may detect an attack/intrusion if the attacker's signature is already in the internal database. SIDS (signature-based intrusion detection system) can detect well-known attacks with high accuracy, that's why they are widely used in the industry.

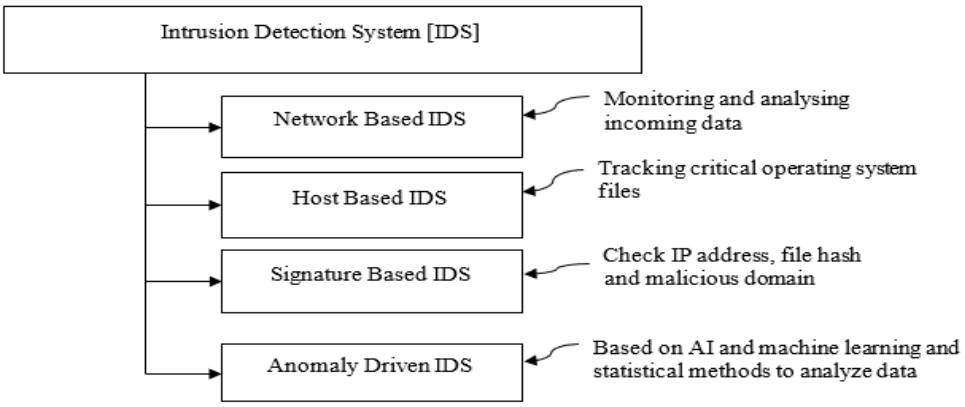

Fig 2. Categorization of IDS Systems based on their function

A signature-based system usually supervises inbound network traffic for sequences and patterns which match a specific attack signature. These can be identified in network packet headers together with data sequences matching known

malware or other malicious patterns. An attack signature can appear in destination or source network addresses also, along with specific data packet series. Signature-based IDS are also called misuse detection systems [4].
4. Anomaly-driven: Anomaly-based detection attempts to identify malicious behaviour. It is necessary to have previously created descriptions to define the normal behaviour of users, hosts, or networks. As a consequence during normal operation, the required data is collected and stored in a database. The above includes analysing behaviour patterns associated with all network entities. To monitor and build behaviour baselines, attributes such as source and destination IP addresses, TCP flags, source and destination ports, and bytes-in and bytes-out are used. Each entity's new activity is compared to its baseline to identify anomalous behaviour and discrepancies from the historical norm.

A behaviour or anomaly-based intrusion detection system (IDS) solution goes beyond identifying specific attack signatures to detect and analyse malicious or unusual patterns of behaviour. These systems generally uses statistical, AI, and machine learning techniques to analyse large amount of data and network traffic and identify anomalies. Afore looking for patterns connected with specific types of attacks, behaviour-based intrusion detection systems monitor behaviours which may be associated with attacks, increasing the likelihood of detecting and mitigating a malicious action before the network is compromised. Hence training is a prerequisite here. Furthermore, these systems can be split into different categories according to the techniques used, if the statistical models are used, they can be called univariate IDS, multivariate IDS, time series, or rule-based IDS whereas Finite state machines and rules, such as case-based, n-based, expert systems, and descriptor languages, are applied in knowledge-based systems. Finally, machine learning includes ANN (Artificial Neural Network), clustering, deep neural algorithms, and reinforcement learning [4].

Limitations of IDS Signature and Anomaly-based detection:

The utmost limitation of signature-based intrusion detection systems is their inability to detect unknown attacks. To avoid detection, malicious actors can simply modify their attack sequences within malware and other types of attacks. Traffic can also be encrypted to completely avoid detection by signature-based tools. Furthermore, advanced persistent threats typically involve threat actors who change their signature more than 60% of the time.

Behaviour-based IDS solutions provide the best line of defense against network breaches by intelligently analysing data using AI and machine learning. They provide comprehensive views of today's complex, sprawling networks, from the office to the data centre and cloud. It gives a high false-positive rate which is also a limitation of this kind of IDS. This implies that malicious and unusual traffic will be detected across the entire physical and virtual network attack surfaces. Host-based detection systems are poor in terms of real-time response.

The study conducted by the Ponemon Institute, sponsored by Observe IT and IBM in the past two years, the average global cost of insider threats increased by 31% to $11.45 million. Moreover, the prevalence of these incidents increased by 47 percent during the same period [7]. As a result, the choice of picking up the finest invasion recognition system for a network depends upon the priority of use cases of an organization otherwise is extremely difficult.

Machine learning and classification:

Machine learning is the field dedicated to evolving systems that can impulsively learn from data and detect hidden patterns. The main concern is that we have lots of information in our hands and all are not worthy, so it is required to mine the promising and informative data that contain sensitive information. The processing time will be prolonged if superfluous and large-size data is employed, and the desired performance will be impossible to achieve. Professionals and researchers are looking to computers to perform the analysis, and this is becoming increasingly common in a field known as data analytics. Some disciplines can be added to data analytics with predictive data. That’s why to find all these things ML models are being introduced in almost all areas**.** ML [machine learning] techniques can be classified as supervised learning, unsupervised learning, and ensemble learning. Fig no 3 gives a brief detail about the categories of machine learning techniques.

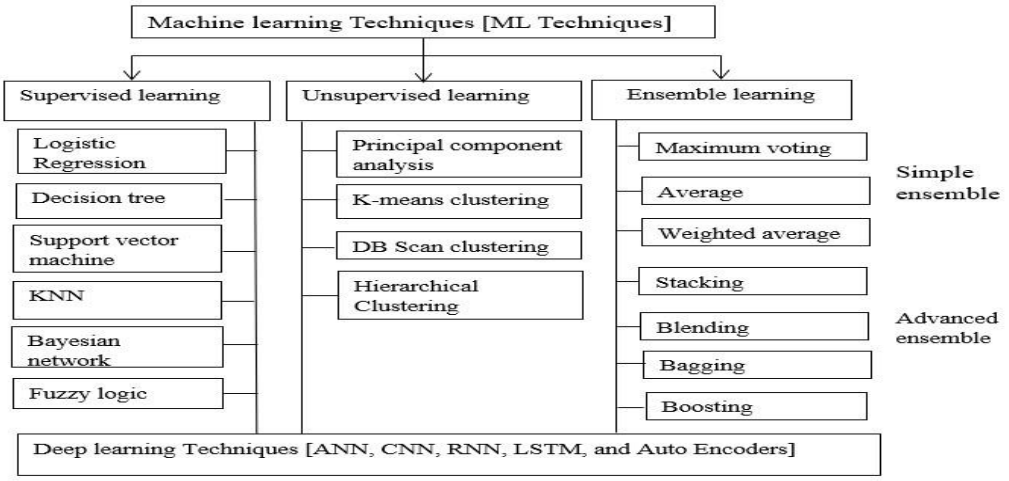

Fig. 3 Machine Learning Techniques

Several machine learning methods are being used in anomaly detection systems some are for classification problems while others are for clustering etc. Here the main of study is a classification problem and because of the nature of system traffic data, regular observations are far greater than harmful observations or malware in real-time network traffic.

The test dataset was assessed to train the machine, and many machine-learning methods were applied to anticipate attacks. Besides this, the attack was labeled by these models to discover a method for effective and efficient classification**.** The most common, efficient approaches, in this–– case, are linear anomaly detection methods or one-class anomaly detection. Moreover, Multi-class approaches, are advantageous for classifying diverse types of attacks.

Some of the main supervised learning techniques are explained here:
1.Logistic Regression: Logistic regression is a classification problem-solving technique rather than regression analysis. This supervised learning technique is more efficient and simpler for the binary outcome that is true/false, zero/one. Logistic regression [LR] is a transformation of linear regression having a sigmoid function. The logistic function is also termed as sigmoid function.
The formula for to calculate logistic regression function is

$$F(x) = \frac{1}{1+e^{-(\beta_0+\beta_1 x)}} \quad \ldots\ldots\ldots\ldots (1)$$

Here $\beta_0 + \beta_1 x$ is like the linear model $y = ax+b$.
The logistic function applies a sigmoid function to restrict the value from a large scale to within the range of 0–1 [20].

2. SVM: This classifier also comes under the supervised learning technique, which is a more geometrical method than statistical that maximizes the margins for each class. Logistic regression (LR) and SVM are similar as they both can divide the feature space using a decision boundary. It is preferred for medium and small-size datasets. Here every data item is plotted by way of a point in n-dimensional space, the number of features is n, and the significance of all features is the value of a specific coordinate. Then, classification is done by locating the hyper-plane that distinguishes between the two classes.

Hyper plane: A hyper plane is a plane that divides n-dimensional data points linearly into two components. In 2D, a hyper plane is a line; in 3D- a plane that is also known as an n-dimensional line.

3. Decision Tree (DT): It builds an architecture that predicts the output of a pattern based on various input attributes standards of the pattern. In Decision Tree the arrangement does not require any province information or parameter setting; just the given data set is learned and modeled [21, 14, and 10]. It consists of three basic elements, leaf node, edges or branch, and decision node.

4. KNN: K-Nearest Neighbour is the abbreviation for KNN. It's a machine-learning algorithm that's supervised. Both classification and regression problem statements can be solved using the approach. In this research, the author focussed only on the classification problem. Here K represents the quantity of nearby neighbours to a novel unknown variable that must be predicted or categorized. This algorithm aims to locate all of the closest neighbours around a new unknown data point to figure out what class it belongs to. This algorithm is also known as a distance-based algorithm.

5. Bayesian Network: These networks are graphical models, with indication propagation controlled by the Bayesian theorem. BNs are characteristically robust for lost pieces of evidence and are better altered to categorical data compared to distance-based classifiers [22]. The structure of Bayesian Networks and their representation is comprehensible to human operators as compared to other machine learning techniques. This structure enables the modeling of information flow over a network along with the tracing of malicious instances.

$$P(X_i - X_n) = \prod_{i=1}^{n} P(X_i \mid \text{Parents } (X_i)) \ldots\ldots\ldots\ldots (2)$$

Each variable of equation (1) should be conditionally independent of each of its non-descendants in the graph given the value of all its parents [3].

6. ANN [Artificial Neural Network]: The primary benefit of ANN processes is their acceptance of incorrect data, together with their ability to anticipate desired results without pre-defined labelling of the input data. These features make ANN a sustainable approach to intrusion detection systems. Artificial neural networks are enthused by human brains as humans want the machine to work as if it were a human, think like a human, and respond like a human, equally all these factors have created some drawbacks in neural networks, such as ANN methodologies that can sometimes fail to create satisfactory results owing to a poor erudition purpose or a lack of data. Secondly, the ANN training phase is frequently slow due to data feed intake, and during back propagation, it adjusts the weights for all neurons.

7. DL [Deep Learning]: Deep learning models learn by examples means they classify the data directly from the images, text, sound, etc. DL models use neural network architecture that's why such systems are also called deep neural networks, which may contain one to several layers. These models are trained by using a big set of labeled data. These models perform tasks that humans do naturally, and their performance sometimes exceeds expectations this is the reason that deep learning models are attaining good attention. RNN, CNN, and LSTM are examples of deep neural networks while some others are also mentioned in figure no. 3.

EXPERIMENTAL SECTION AND RESULTS

Evaluation Metrics: Key metrics for the evaluation of system performance are discussed in this section.

1. Confusion Matrix: As discussed in [22] the confusion matrix is a square pattern shown in fig. 4, in which the column signifies the actual values, and the row represents the model's predicted value, and vice versa.
The confusion matrix has four values which are:

1. True Positive [TP]: True positive is an outcome when the model predicts the results correctly.
2. False Negative [FN]: These are the values that are false/negative in fact but predicted as true/positive.
3. True Negative [TN]: These values are true/positive but predicted as false/negative.
4. False Positive [FP]: False-positive value means, the model incorrectly predicts an actual negative class as a positive class.

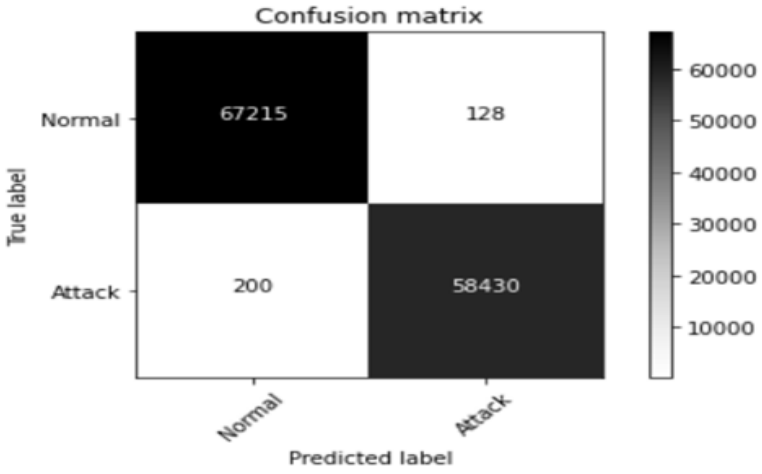

Fig. 4 Confusion Matrix

2. Precision: According to [23] precision can be calculated as

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive+False Positive}} \ldots\ldots\ldots\ldots (3)$$

$$= \text{Precision: } 0.998$$

3. Recall / Sensitivity: Recall value tells about how many of the actual positive values are to be predicted correctly out of the model. Sensitivity/Recall indicates the percentage of the positive class that was correctly classified.

$$\text{Recall/ Sensitivity} = \frac{True\ Positive}{True\ positive + False\ Negative}$$

$$= \frac{TP}{TP+FN} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$$= 0.997$$

4. F-1-score: The F-1score can be calculated from the harmonic mean of Precision and Recall**.**

$$\text{F-1 score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad \ldots\ldots\ldots (5)$$

$$= 0.997$$

5. Specificity: Specificity tells how many participants in the negative class were correctly classified.

$$\text{Specificity} = \frac{TN}{TN+FP} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (6)$$

6. Accuracy: It is the ratio of correctly labeled subjects to the total number of subjects.

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+FP+FN+TN)} \quad \ldots\ldots\ldots\ldots (7)$$

$$= 0.997$$

7. Validation Accuracy: Validation accuracy for this LSTM model is

$$\text{VA= Sum (TF= =TL)/ Count (TL)} \ldots\ldots (8)$$

$$\text{Val. Accuracy} = 0.997$$

VA is used for validation accuracy, TF for test features, and TL for test labels.

Validation Loss: The validation loss metric is acclimated to measure the performance of the LSTM model on a validation set.

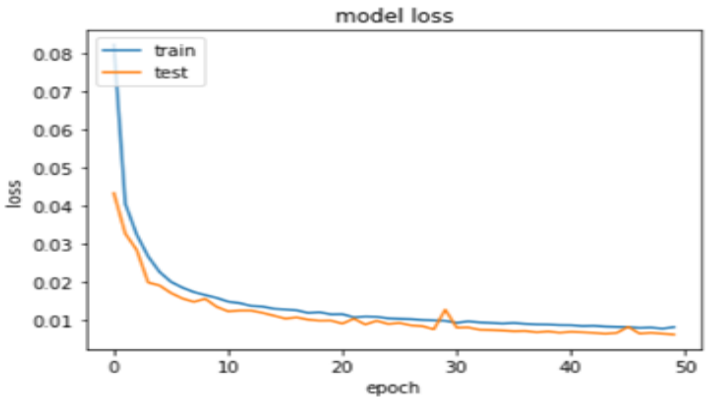

Fig. 5. Model Loss during Training and Testing

In fig 5. It is visible that the LSTM performed well on the validation set, the loss in 50 epochs is less as compared to the loss in 50 epochs on the training set. Furthermore, this architecture produced precision, F1 Score, Recall, and Validation accuracy of around 99.5% as shown in fig.6.

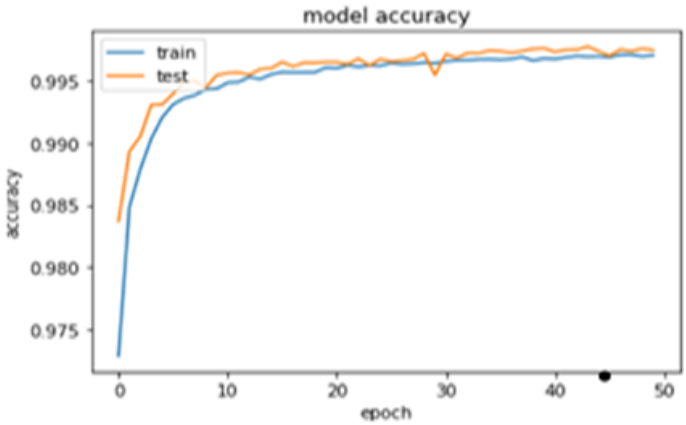

Fig. 6 Accuracy graph of the LSTM model

In order to check the accuracy of the system the difference between training data and testing data has been presented in the Fig 6. Similar type of studies has been reported by the researchers with different variables [23-30].

CONCLUSION

A new area of research in machine learning and artificial intelligence is the solicitation of various classifier methodologies in IDS Systems. For a very long time, it has been the focus of research. The critical role of the anomaly detection system is the identification and recognition of malicious activities thus in this research malicious instances are detected using deep learning techniques, in addition, to numerous assessment metrics for quantifying the performance of the intrusion detection algorithm. In future work to make the system more convenient in terms of trustworthiness some ensemble techniques and different architectures with explainable AI and high-specification systems can be applied to reduce the time complexity of the model. Secondly, there are numerous feature selection algorithms available. The classification techniques will benefit from using various feature selection algorithms, that will raise the importance of the feature selection step in intrusion detection systems as well.

REFERENCES:

1. Amouri, A., Alaparthy, V. T., & Morgera, S. D. (2020). A machine learning-based intrusion detection system for mobile internet of things. Sensors (Switzerland), 20(2). https://doi.org/10.3390/s20020461
2. Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. Communications in Computer and Information Science, 1235 CCIS, 121–131. https://doi.org/10.1007/978-981-15-6648-6_10
3. John Ugochukwu, C., & Bennett, E. O. (2018). An Intrusion Detection System Using Machine Learning Algorithm. In International Journal of Computer Science and Mathematical Theory (Vol. 4, Issue 1). www.iiardpub.org
4. Brasoveanu, A., Moodie, M., & Agrawal, R. (2020). Textual evidence for the perfunctoriness of independent medical reviews. CEUR Workshop Proceedings, 2657, 1–9. https://doi.org/10.1145/nnnnnnn.nnnnnnn
5. Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN-based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2), 493–501. https://doi.org/10.1007/s12083-017-0630-0
6. Chkirbene, Z., Erbad, A., Hamila, R., Mohamed, A., Guizani, M., & Hamdi, M. (2020). TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection. IEEE Access, 8, 95864–95877. https://doi.org/10.1109/ACCESS.2020.2994931 Cost of Insider Threats: Global Report 2020.
7. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150
8. IEEE National Aerospace and Electronics Conference 2017 Dayton, O., Institute of Electrical and Electronics Engineers, IEEE National Aerospace and Electronics Conference, & NAECON 2017.06.27-30 Dayton, O. (n.d.). Proceedings of the 2017 IEEE National Aerospace and Electronics Conference (NAECON).
9. Bhumihaar, S., Bellekens, X., Os Tacht, C., Hindy, H., Safa, N. S., Kamarudin, H., & Biswas, S. K. (2018). Intrusion Detection Using Machine Learning: A Comparison Study Related papers Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion… Azam Rashid A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Dat … A Logit Boost based Algorithm for Detect ing Known and Unknown Web At t acks Intrusion Detection Using Machine Learning: A Comparison Study. International Journal of Pure and Applied Mathematics, 118(19), 101–114.
10. Chockwanich, N., & Visoottiviseth, V. (2019). Intrusion Detection by Deep Learning with TensorFlow. International Conference on Advanced Communication Technology, ICACT, 2019-February, 654–659. https://doi.org/10.23919/ICACT.2019.8701969
11. Chiba, Z., Abghour, N., Moussaid, K., el omri, A., & Rida, M. (2019). Intelligent approach to building a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. Computers and Security, 86, 291–317. https://doi.org/ 10.1016 /j.cose.2019.06.013
12. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. In Electronics (Switzerland) (Vol. 9, Issue 9, pp. 1–29). MDPI AG. https://doi.org/10.3390/electronics9091460
13. Meryem, A. (2020). Hybrid intrusion detection system using machine learning. www.idg.com/
14. Salih, A. A., & Abdulazeez, A. M. (2021). Evaluation of Classification Algorithms for Intrusion Detection System: A Review. Journal of Soft Computing and Data Mining, 02(01). https://doi.org/10.30880/jscdm.2021.02.01.004
15. Guru, D. S., Suhil, M., Pavithra, S. K., & Priya, G. R. (2018). Ensemble of Feature Selection Methods for Text Classification: An Analytical Study. Advances in Intelligent Systems and Computing, 736, 337–349. https://doi.org/10.1007/978-3-319-76348-4_33
16. Li, X. K., Chen, W., Zhang, Q., & Wu, L. (2020). Building Auto-Encoder Intrusion Detection System based on random forest feature selection. Computers and Security, 95. https://doi.org/10.1016/j.cose.2020.101851

17. Belouch, M., el Hadaj, S., & Idlianmiad, M. (2018). Performance evaluation of intrusion detection based on machine learning using apache spark. Procedia Computer Science, 127, 1–6. https://doi.org/10.1016/j.procs.2018.01.091
18. Hosseini, S., & Seilani, H. (2021). Anomaly process detection using negative selection algorithm and classification techniques. Evolving Systems, 12(3), 769–778. https://doi.org/10.1007/s12530-019-09317-1
19. Sinnott, R. O., Duan, H., & Sun, Y. (2016). A Case Study in Big Data Analytics: Exploring Twitter Sentiment Analysis and the Weather. In Big Data: Principles and Paradigms (pp. 357–388). Elsevier Inc. https://doi.org/10.1016/B978-0-12-805394-2.00015-5
20. Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Ahmadi, S. B. B., & Ayobi, S. (2021). A review on machine learning approaches for network malicious behavior detection in emerging technologies. In Entropy (Vol. 23, Issue 5). MDPI AG. https://doi.org/10.3390/e23050529
21. Aljanabi, M., Qutqut, M. H., Hijjawi, M., & Al-Janabi, M. I. (2018). Data Offloading Framework Using Mobile Small Cells and Urban WiFi View project Studying and evaluating several aspects of the Internet of Things (IoT) platforms and implementations View project Machine Learning Classification Techniques for Heart Disease Prediction: A Review. Review Article in International Journal of Engineering and Technology, 7(4), 5373–5379. https://doi.org/10.14419/ijet.v7i4.28646
22. Farhan, R. I., Maolood, A. T., & Hassan, N. F. (2020). Performance analysis of flow-based attacks detection on CSE-CIC-IDS2018 dataset using deep learning. Indonesian Journal of Electrical Engineering and Computer Science, 20(3), 1413–1418. https://doi.org/10.11591/ijeecs .v20.i3.pp 1413-1418.
23. Gupta S., Singh J. and Kumar K. Analyzing and modeling of activity patterns of stn-gp network in parkinson's state vs normal state, PalArch's Journal of Archaeology of Egypt/Egyptology. 9(17) (2020), 9653-9663.
24. Gupta S., Singh J., Kumar K.: Study of Discharge Outlines of Subthalamic Nucleus-Globus Pallidus External and the Favorable Impact of Deep Brain Stimulation in the Parkinson State, Journal of Pharmaceutical Research International, 2022, DOI: 10.9734/jpri/2022/v34i12B35563.
25. Gupta S., Singh J., Kumar K.: Ionic concentration and action potential differences between a healthy and alzheimer's disease person", a book series of springer publication "communications in computer and information science". Data Science and Analytics a book chapter in book series Communications in Computer and Information Science (CCIS) 2019: 1229 pp 266-277 : ISBN 978-981-15-5826-9.
26. Gupta S., Kumar K., Singh J.: A Comprehensive Study of Deep Brain Stimulation during Last Decade. Journal of Pharmaceutical Negative Results, (2022). 3866–3869. https://doi.org/10.47750/pnr.2022.13.S08.483.
27. Gupta, S., Kumar, K., Singh J.: Role of deep brain stimulation in globus Pallidus Neuron. Neuroquantology, 2022; 20(14): 159-162.
28. Khatkar, Monika & Kumar, Kaushal & Kumar, Brijesh. (2020). An overview of distributed denial of service and internet of things in healthcare devices. 44-48. 10.1109/INBUSH46973.2020.9392171.
29. Monika Khatkar, Kaushal Kumar, Brijesh Kumar: Unfolding the network dataset to understand the contribution of features for detecting malicious activities using AI/ML Materials Today: Proceedings, Volume 59, Part 3,2022,1824-1830, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2022.04.391.
30. Khatkar, Monika & Phogat, Nisha & Kumar, Brijesh. (2014). Reliable data transmission in Anonymous Location Aided Routing in MANET by preventing replay attack. 1-6. 10.1109/ICRITO.2014.7014731.