A Review on Intrusion Detection System Based on Various Learning Techniques

Shiladitya Raj, Megha Jain, Megha Kamble

Abstract: ***In this world of the Internet, security plays an important role as Internet users grow rapidly. Security in the network is one of the modern periods' main issues. In the last decade, the exponential growth and massive use of the Internet have enabled system security vulnerabilities a critical aspect. Intrusion detection system to track unauthorized access as well as exceptional attacks through secured networks. Several experiments on the IDS have been carried out in recent years. And to know the current state of machine learning approaches to address the issue of intrusion detection. IDS is commonly used for the detection and recognition of cyberattacks at the network and host stage, in a timely and automatic manner. This research assesses the creation of a deep neural network (DNN), a form of deep learning model as well as ELM to detect unpredictable and unpredictable cyber-attacks.***

Keyword: Intrusion Detection System, Deep Learning, Extreme Learning, Machine, Deep Belief Network (DBN).

I. INTRODUCTION

Cyber-attacks are getting more advanced and thus creating rising risks in identifying intrusions correctly. In the absence of intrusion prevention, the credibility of security providers, such as data of availability, integrity, and confidentiality may be compromised. A critical risk to the IDS design is the evolution of malicious applications (malware). Attacks of malicious have become more complex and the main risk is to recognize unknown and malware of obfuscated, as multiple evasion methods are used by malware writers to mask details and avoid intrusion detection systems (IDS)detection [1].

An intrusion detection system detects every kind of malicious network traffic & computer usage that a conventional firewall can detect. This includes attacks on vulnerable services by the network, attacks on uses by data files, attacks on host-based services like privilege escalation, illegal logins, & sensitive data & malware. For the users, safety from external unwanted influences is necessary for their systems. One of the most common protection methods used to secure the network is the firewall technique.

Manuscript received on 27 March 2021 | Revised Manuscript received on 10 April 2021 | Manuscript Accepted on 15 April 2021 | Manuscript published on 30 April 2021.

* Correspondence Author

Shiladitya Raj, Student, Department of computer science and Engineering, Lakshmi Narain College of Technology Excellence Bhopal, India. Email: raj.shiladitya@gmail.com

Megha Jain*, Assistant professor, Department of computer science and Engineering, Lakshmi Narain College of Technology Excellence Bhopal, India. Email: meghaj@lnct.ac.in

Megha kamble, Assistant professor, Department of computer science and Engineering, Lakshmi Narain College of Technology Excellence Bhopal, India. Email: meghak@lnct.ac.in

In communication, medical applications, credit cards commit fraud, insurance agency, IDS are used [2].The artificial Intelligence branch is Machine learning (ML) that promotes the principle that devices can recognize by themselves how to solve a given problem by providing access to the correct data. ML enables robotics capable of undertaking computational functions independently that human beings have traditionally solved by using sophisticated statistical and mathematical methods. This notion of automating complex processes has produced a significant interest in the field of networking in the expectation that many operations included in the design and function of communication networks will be unloaded onto machines. In fields such as cognitive radio, traffic classification, intrusion detection, these standards have already been reached by certain implementations of ML in different networking areas. Machine learning is a technique for data algorithm training, and ultimately, DL is a kind of ML inspired in deep learning by the structure of the human brain [3]. Deep learning approaches have made an important breakthrough in various applications of useful safety tools with great performance. It is considered the best choice for discovering complex architecture by using them for backpropagation algorithms in highly dimensional files. DL is an artificial intelligence sub-set of Machine Learning. Artificial intelligence is a process that makes it easy for a machine to mimic beings. Machine learning is a technique for data algorithm training, and ultimately, Deep Learning is a kind of ML inspired in deep learning by the human brain structure. This network structure is known as an artificial neural network [4]. ELM is a method for ML (machine learning) in which hidden neurons are not in an iterative manner. Extreme Learning Machine (ELM) is more persuasive when it comes to solving challenges. Extreme Learning Machine is more persuasive when it comes to solving challenges. In NN (neural network) theory, linear system theory, control theory, and matrix theory, Extreme Learning Machine is generally considered, ELM is a system applied as a single hidden layer feed-forward NN that selects random and calculates output weights, with a single layer of inputs, an occult layer of occult nodes, &a single output layer. [5].

II. INTRUSION DETECTION SYSTEM

A kind of device is Intrusion detection is and management system of network security. A system of ID system and analyzes information in a computer or network in multiple places to locate possible safety breaches, which include intrusion or misuse (attacks from inside association). ID uses susceptibility assessment (scanning) which is a technology that has been established to measure network safety or computer system. [2]

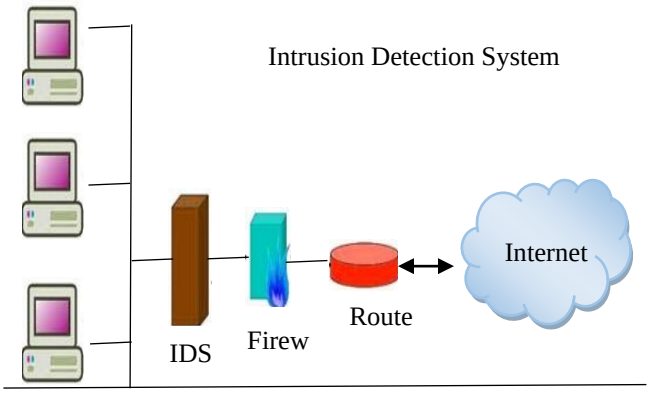

Figure 1: IDS

A. Ids Taxonomy [6]

There are two broad kinds of IDSs: host-based (HIDS) as well as network-based (NIDS)[7]. A host IDS includes the installation on specific devices of small programmed (or agents). The agents track & write data to record files & cause alarms. An interconnected IDS typically consists of a network programmed (or sensor) that operates in a promiscuous mode that manages the interface separately. In that section, the IDS is put on the network segment or boundary. Intrusion detection nowadays is focused on a combination of host and network information to build more effective hybrid networks.

1. Host-Based Intrusion Detection (HIDS)

HIDS refers to a single-host device intrusion detection. Data from a single host device are obtained. The HIDS agent tracks operations like system integrity, program behavior, file modifications, traffic on the host network/security logs. The agent provides information on the current status of the local host by using standard hacking tools, file time-stamps, system logs as well as monitors system calls as well as the local network interface. If no unwanted modification or action has been identified, the user is notified by a pop-up, the central management server is activated, it blocks or combines the above three operations. The outcome depends on the local system's policy. The passive component of these host-dependent protocols.

2. Network-Based ID (NIDS)

NIDS is utilized for network traffic monitoring & analysis to secure the network against the risks of network-related data. A NIDS helps to track suspicious actions like dos attacks, port scans including network traffic monitoring attacks. NIDS consists of a range of packet intrusion prevention sensors, One or more NIDS management feature servers, or one or more human interface management relieves. To identify patterns of interference, NIDS analyses the traffic packs of the packet in actual or near real-time. The study of intrusion detection patterns which be conducted on the sensors, on the servers, or as a result of these two devices. The active element of these networked procedures is considered.

3. Hybrid ID

The present trend is to hybrid HIDS as well as NIDS of all forms to develop hybrid systems. The versatility of the hybrid iIDS enhances the layer of safety. It integrates IDS sensor positions as well as reports for individual segments or the whole network.

B. Intrusion Detection Approaches

Several methods are presently being used to incorporate the desired elements of an ID. Intrusion detection is achieved using two common methods:

1. Anomaly Detection(AD)

The IDS anomaly efforts to reach abnormalities where the normal system has some variations. Audit data obtained throughout the regular activity is used for detecting anomalies. Detection of anomalies is essential for the detection of fraud, network interference, and other suspicious phenomena, which are important, but difficult to identify. The significance of the detection of anomalies is attributed to the assumption that anomalies in data contribute to critical operational data across a broad spectrum of applications. AD is often also called behavior-based detection since it includes consumer behavioral differences [8].

2. Misuse Detection (MD)

Misuse IDS to analyze particular traffic as well as to compare the irregular activity with rules system can notice attacks, for example matching signature pattern. MD is sometimes called signature-based detection as alerts are focused on specific signatures of attacks. These signatures involve some traffic or behavior dependent on known intrusive behaviors [9].

C. Functions Of Ids

IDS contain four important functions:

- Data collection
- Feature Selection
- Analysis
- Action [10].

D. Datasets For Ids

- **DARPA:** This dataset was developed for system security research. DARPA contains tasks including file transfer and receipt with FTP, email transmission and receipt with SMTP & POP3, web browsing, signing into remote computers using Telnet & doing work, sending and receiving IRC messages, and tracking the router with SNMP remotely.
- **KDD'99:** By processing the tcpdump part of the 1998 DARPA data set, a KDD Cup data set for 1999 was generated. Over 20 attacks like Neptune-dos, pod-dos, smurf-dos, buffer-overflow, rootkit, satan, teardrop, are used in KDD99 KDD99.
- **Kyoto:** This data set is generated using honeypots so no manual labeling and anonymization process, but it is only possible to observe attacks aimed at the honeypots. It has 10 extra functionalities, including IDS Detection, Malware Detection, as well as Ashula Detection, which are helpful in the study & analysis of NIDS.
- **Twente:** The dataset contains network packet trace files and some wireless tracks. It was created using a single TCP attack request scenario.

- **NSL-KDD**: Dataset is the intrusion detection benchmark dataset. NSL-KDD consists of 43 attributes (including the class label) and 1,47,907 examples, which are based on the DARPA data set [11,12]

III. MACHINE LEARNING APPROACH

ML is a theoretical area that focuses systematically on theory, results, & properties of education systems & algorithms. It draws on several diverse areas of ideas: optimization theory, artificial intelligence, psychology, knowledge processing, optimal controls, cognitive sciences, also other branches in research, science, and mathematics. It is a strongly interdisciplinary area. With the introduction of machine learning in a broad variety of applications, it has reached almost every research field, which has a significant influence on technology and society. A range of issues has been tackled, including advice engines, recognition mechanisms, IT and data mining, and independent testing systems. ML area is usually categorized into 3 sub-domains: supervised, unsupervised, & reinforcement learning.

1. Decision Tree (DT)

The decision tree is the function to construct a classifier to predict the value of the target class for an invisible test case. An unseen test instance is defined as a DT by several choices. As a single classifier, the Decision Tree is very common due to its simplicity or easier implementation. DT in 2 forms can be enhanced: I Description tree of a set of symbolic class labels & (ii) regression tree of a range of labels of numerical importance.

2. Naive Bayes

Based on the class label provided by NB, the attributes are linear combinations and therefore attempt to estimate the probability in support. In the classification of simplified relations, Naive Bayes also achieves positive outcomes. Naive Bayes only needs one training data scan & thus eases the classification task considerably.

3. K-nearest neighbor

In KNN numerous distance measuring methods are applied. In the training data that is nearest to the test sample, KNN can search out the k number of samples as well as give a class label to the test sample among the examined exercises. KNN is the most simple as well as a non-parametric solution to classifying samples. KNN is a case-based learner and not an inductive one.

4. Artificial Neural Network

ANN is a pattern recognition device based on human brain functionality. NN s are usually structured into levels composed of a variety of interconnected nodes that comprise an activation mechanism. The input layers provide patterns to a network that communicate with one or more hidden layers, where the actual processing is performed by a system of weighted links. hidden layers are then connected to the output layer for results.

5. Support Vector Machines

In the mid-1990s, SVM was developed. Essentially, the idea behind SVM is the use of training data mostly as a definition of a usual class of objects or recognized as a non-attack in the IDS, as well as the other data is then assumed as anomalies. The classification built by the technique of SVM discriminates against the input field in a certain region where regular interests are present.

6. Fuzzy Logic

For reasoning purposes, the true principles in dual logic may be either false (0) or true (1), but certain constraints are relaxed in Fuzzy logic. In FL, which means that the value of a statement's true degree maybe around 0 or 1 with "0" or "1." [13].

IV. DEEP LEARNING

Deep learning is often unsupervised, masterly regulated contrasting learning. It needs the development of large NNs to make it possible for the machine to learn or compute itself without direct human intervention. Learning in apps relies on arm-technical features where the researcher codes pertinent details manually about the task and then learning about it. This contrasts with the deep learning that makes the structure as viable as possible to develop its properties. Recent Google experiments on deep learning have shown that a very large, unsupervised NN can be trained to optimize the development of features for cat faces recognition. The data limitations associated with incredibly broad recommendation networks offer ample opportunities to discover new methods of transferring expertise through subsidiary sources of information. [14].

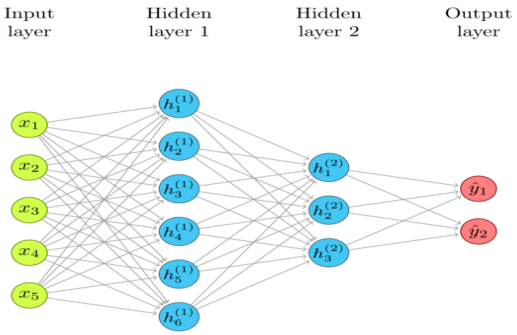

Fig. 2: Deep Learning

A. Deep Learning Techniques

1. Deep Neural Networks

DL is a perceptron, which is a single neuron in a NN, the basic building block. If a set of m inputs is finished (e.g., m words or m-pixel), each input is increased by weight (that 1 to theta m), we sum up the weighted input mix, apply distortion and finish by a non-linear function of activation.

2. Convolutional Neural Networks

CNN's are very much the same as common NNs, they comprise neurons with learning weights and preconditions. Every neuron obtains such inputs, generates a dot product & follows it with non-linearity optionally. A single differential score function is now represented in the entire network, from raw pixels on one end to class scores on the other. the later (completely connected) stage still has a missing purpose and we still apply all the tips and tricks we have learned to learn standard NNs.

CNN uses the fact that the feedback consists of pictures to more sensitively limit the architecture.

3. Recurrent Neural Networks

RNN is the basic algorithm for more popular and robust sequential data. Even Siri Apple uses profoundly slow RNN to process speech. RNN has a clear memory that recalls the memory input. This segment consists of the RNN principles and Process. RNN works, which are more common because of the super memory it remembers and forecasts future events. In time-series data, speech data, and other uses, RNN is commonly used.

4. An Autoencoder

A feedforward neural network is historically An autoencoder to learn a compact or distributed data set representation. A 3-layer neural network is a self-encoder, that is learned to construct its inputs with them as output. It has to learn features that capture data variation to duplicate it. If a linear activation function is only used to minimize dimensionality, it can be shown to be equal to PCA. The triggering of the secret layer is used as the trained features during training and the first layer can be disabled.

5. RBM

RBM is an undirected, visible layer and hidden layer, two-layer NN. Within-layer there are no links, but the links are concealed to clear. It is learned to optimize the expected data log opportunity. Binary vectors are the inputs since each input receives Bernoulli distributions. In the same way, as in a normal NN, the activation function is determined & the logistic function commonly used is from 0 to1. every neuron is activated if activation is higher than the random variable and is viewed as a chance. [15].

V. DEEP BELIEF NETWORK(DBN)

These days, deep architecture in ML is very common. DBNs are the deep structure used to construct an efficient generative model using training data using the stack of Restricted Boltzmann Machines (RBMs). In various applications including image processing, speech processing &, etc, DBNs have multiple capabilities such as extraction and analysis of features. Commonly, in speech recognition communities, much focus has been provided to the DBNs Even so, the required hidden layers of DBNs are usually set.

The DBN is a probabilistic, generative model collected of numerous layers of hidden units. structure of basic learning modules that form each layer can be considered. DBN consists of an RBM stacked machine that is used with greed, as seen in Fig. 3. Even so, DBN findings are very costly and time-intensive as the number of layers of DBN that have to be achieved is a lot. [16].

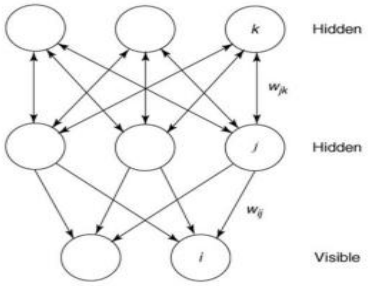

Fig. 3. A stacked RBM or known as DBN

A. Applications of DBNs

1) Image Recognition

In image recognition, DBNs can be used. The input and the output type will be an image. This methodology provides wide applications from comparatively basic tasks such as photographic organizing to vital roles such as medical diagnoses.

2) Video Recognition

Even DBNs are used in video recognition. Video recognition functions in the same manner as perception, as video data seeking meaning. It may recognize, for example, an entity or a person's gesture. It can be used in various areas, such as home automation, health care, and defense.

3) Motion-Capture Data

Motion capture data consists of monitoring entity or individual gestures, which often utilizes strong faith networks. Motion collection is tricky since, for example, a computer can lose track of a human if someone else looks like comes in or something briefly obstructs the vision [17].

VI. ELM

ELM is a modern technology that offers strong generalization efficiency at a highly rapid learning speed for classification or regression issues. Even if SVMs will generalize better, they have two disadvantages: 1) the intense and quadratic computation of their instruction about the number of training examples; 2) Produces huge network sizes for large dynamic applications [18].

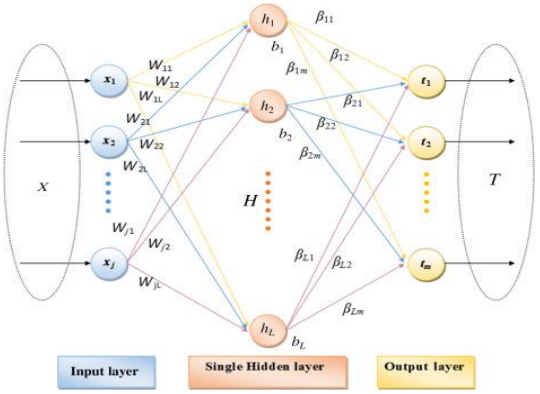

Fig .4: Extreme Learning Machine

1. Variants Of Elm

This portion introduces and describes a few common ELM variants.

Incremental ELM (I-ELM): I-ELM to create an incremental input network. In the secret layer, I-ELM inserted random nodes. This was added one at a time. This froze the performance weights of currently hidden nodes (HNs) when a new HNs was inserted. In addition to the continuous (and differentiable) enabling functions of the SLFN, I-ELM is effective for SLFNs that have partly continuous (such as threshold) activation functions. Huang et al. introduced I-ELM convex (CI-ELM) & improved I-ELM (EI-ELM) given this I-ELM sense).

Pruning ELM: If very few / many hidden nodes are deployed, the underfit-ting/overfitting of a P-ELM algo built for the design of an ELM network will lead to problems. P-ELM starts with many HNs before less relevant or irrelevant HNs are eliminated by taking into account their significance for class labels in learning.

Error-Minimized ELM: This system is capable of increasing group by group hidden nodes and of knowing the amount of HNs in generalized SLFNs automatically. During network development, performance weights are changed slowly and thus the device complexity is significantly reduced. For secret nodes of sigmoid form, the results of the simulation indicate that this technique will dramatically reduce the computation difficulty of ELM & help build an efficient application of ELM.

Online Sequential ELM: Both preparation details will be accessible for training purposes by utilizing traditional ELM. Training data can however be accessed one by one or one element per line in actual applications. Proposed an algo called the online ELM (OS-ELM) for sequential learning. This algo can be used in a unified environment with both RBF and additive nodes.

Ordinary ELM: ELM algo for common problems in regression, three ordinal algo based on ELM has been implemented and one framework based on encoding.

Fully Complex ELM: ELM algo was generalized in this application from real domain to abstract domain. Like ELM, C-ELM's secret layer preferences and input weights were randomly chosen based on the ongoing likelihood of spread. The performance weights were then measured analytically, rather than iterated. [19,20]

This paper is described in section 1st Introduction of IDS, DL, EML. In section 2nd we overview IDS and its various functions and numerous types of datasets used in IDS. Section 3rd defined the deep learning techniques also discuss different types of DL Methods like CNN, RBM, autoencoder, RNN. Then we discuss Section 5th ELM and its different types of Variants. In section 6 we provide literature reviews. And finally, we have concluded in section 7.

VII. LITERATURE REVIEW

W. Srimuang & S. Intarasothonchun (2015) developed a classification model for ID using Weighted ELM that studied with KDD'99 data set ad 4 kinds of key attack: When compared the effectiveness of the approach proposed to SVM+GA and ELM, DoS, U2R, R2L or Probing Attack concluded that a weighted method with the RBF input layer of the kernel with the value of a trade-off constant C at 25 was shown to be more efficient than other 2 methods, DoS's accuracy = 99.95%, U2R= 99.97%, R2L=93.64%, as well as Probing=96.64% have been using in the meanwhile with less time to operate. [21].

M. Z. Alom et al. (2015) This paper explores DBN's capabilities in intrusion detection through a series of tests after NSL-KDD dataset training. In addition to the identification and classification of attacks into five groups, the proposed method reliably defines and classifies network behavior based on a small, incomplete, and nonlinear source of data. For only Fifty iterations, that is state of the art associated with an existing technique for intrusion detection, the proposed system achieved detection accuracy of nearly 97.5% [22]

J. Ku et al. (2017) suggest an effective evaluation algorithm called an ELM for self-adaptive differential evolution (SADE-ELM) for intrusion classification & detection. Their approaches are compared to ELM, DE-ELM classification techniques, widely used. Simulation findings indicate that in the classification scenario, the suggested SADE-ELM solution provides better detection accuracy [23].

M. H. Ali et al. (2018) This study proposes that ELM is the most common ML algorithm that is easy to use with superior efficiency. After all, the internal power (weight as well as basis) parameters of ELM are arbitrarily initialized, creating an unpredictable algorithm. PSO is a popular metaheuristic that is used to maximize ELM in this study. Their model has been validated by NSL-KDD focused on intrusion detection. Their model was compared to a fundamental ELM. The test accuracy of PSO-ELM has been superior to a simple one [24].

D. Liang and P. Pan (2019) The improved model uses DBN to train as well as classify the NSL-KDD datasets. At any middle level of DBN-ELM, a classifier is associated. The actual output is determined by integration by majority votes for output of classifier & ELM. Analyses showed that an improved model improves the confidence or accuracy of classification. the algorithm was benchmarked with the NSL-KDD dataset & model accuracy increased to 97.82% whereas the false alarm rate decreased to 1.81%. In comparison with DBN, ELM, DBN-ELM, the proposed enhanced approach outperforms competitive accuracy. [25].

K. Singh and K. J. Mathai (2019) proposed an ML classifier state Preserving ELM (SPELM) algorithm comparing its output and DBN with the KDD NSL data set. Contrasted with the DBN algorithm. NSL- KDD dataset has 4 lakhs of data information, of which 40% have been utilized for testing & 60% applied to assess the performance of 2 algorithms. outcomes showed improved efficiency of SPELM: compared with 53.8% of the DBN algorithm 93.20%, SPELM precision 69.492 DBN 66.836 and Computational time 90.8 seconds, SPELM 102 seconds, and DBN algorithm 90.8 seconds.[26].

P. Wei et al. (2019) This paper proposes to boost the network configuration of the DBN a new collaborative optimization algorithm. algorithm for optimization is utilized as intrusion classification model Network Configuration. tentative findings indicate that associated with other DBN-IDS optimization algorithms, with an improvement in average training time by at least 6.9 percent, their algorithm shores average detection time by a minimum of 24.69 percent; their DBN IDS enhances average classification precision by at least 1.3 percent & by up to 14.80 percent in t as compared with the classification algorithms tested [27] .

E. D. Alalade et al. (2020) This paper introduces early IDS detection by ELM & Artificial Immune System, anomalies in smart home networks. To refine input parameters, AIS uses the clonal algorithm, and ELM analyzes input to maximize convergence in the identification of anomalous.

The key area of this paper is to use this method in the home automation network gateway & to combine it thru a push notification system, enabling owners in the intelligent home routers to identify any abnormalities [28].

N. A. H. Qaiwmchi (2020) suggests a novel method for result optimal weights of an input-hidden layer. paper provides a method for OSELM integration & backpropagation (OSELM-BP). Following integration, BP variations iteratively random weights & usages a repeated error analysis to correct feedback on weights. The method is estimated dependent on different OSELM scenarios and the number of iterations for BP instead. A comprehensive examination of the method and correlations to the original OSELM show that an optimal accuracy is achieved with a small no. of iterations of OSELM-BP [29].

VIII. CONCLUSION

An IDS plays a key role in cybersecurity to deter attacks on the networks. Its reliability depends specifically on the decision method utilized. This paper presents an overview of various versions of ID & DL algorithms in a brief survey of deep learning-based IDS. Deep learning is the best approach to learning, supervised, time-consuming, and cost-effective. Deep learning is often unsupervised, masterly regulated contrasting learning. Because of its appropriate structural efficiency, ELM attracted increasing attention from the ML community at a much faster speed.

REFERENCES

1. A.Dretheyk-Ossowicka, “A survey of neural networks used for intrusion detection systems,” J. Ambient Intell. Humaniz. Comput., 2020 [CrossRef]
2. AKhraisat, “Survey of intrusion detection systems: techniques, datasets, and challenges,” 2019[CrossRef]
3. Musumeci et al., “An Overview on Application of Machine Learning Techniques in Optical Networks Francesco Musumeci,” IEEE Commun. Surv. vol. 21, no. 2, pp. 1383–1408, 2019, DOI: 10.1109/COMST.2018.2880039. [CrossRef]
4. S.Pouyanfar et al., “A Survey on Deep Learning,” ACM Comput. Surv., vol. 51, no. 5, pp. 1–36, 2019, DOI: 10.1145/3234150. [CrossRef]
5. Gupta and N. S. Gill, “Machine Learning Techniques and Extreme Learning Machine for Early Breast Cancer Prediction,” Int. J. Innov. Technol. Explore. Eng., vol. 9, no. 4, pp. 163–167, 2020, DOI: 10.35940/ijitee.d1411.029420. [CrossRef]
6. V. Jaiganesh,” Intrusion Detection Systems: A Survey and Analysis of Classification Techniques”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013
7. Glenn M. Fung and O. L. Mangasarian, “Multicategory Proximal Support Vector Machine Classifiers”, Springer Science and Business Media, Machine Learning, 59, 77–97, 2005[CrossRef]
8. Guang-Bin Huang, Dian Hui Wang and Yuan Lan, “Extreme learning machines: a survey”, Published: 25 May 2011_ Springer-Verlag, 2011
9. Hyeran Byun and Seong-Whan Lee, “Applications of Support Vector Machines for Pattern Recognition: A Survey”, Springer-Verlag Berlin Heidelberg, 2002
10. Manasa, P. R. M. V, and S. B. Patil, “A SURVEY on ‘ INTRUSION DETECTION SYSTEM,’” vol. 1, no. 4, pp. 928–932, 2012.
11. N. Sameera and M. Shashi, “Intrusion Detection Analytics: A Comprehensive Survey,” Int. J. Adv. Sci. Res. Manag., vol. 4, no. 6, 2019, DOI: 10.36282/ijasrm/4.6.2019.1279. [CrossRef]
12. S. Vijayarani and R. Kalaivani, “Intrusion Detection System – A Survey,” Int. J. Bus. Intelligence, vol. 004, no. 002, pp. 57–61, 2015, DOI: 10.20894/ijbi.105.004.002.001. [CrossRef]
13. Nutan Farah Haq, Application of Machine Learning Approaches in Intrusion Detection System: A Survey”, (IJARAI) International Journal of Advanced Research in Artificial Intelligence, Vol. 4, No.3, 2015 [CrossRef]
14. V. Pream Sudha,” A SURVEY ON DEEP LEARNING TECHNIQUES, APPLICATIONS AND CHALLENGES”, International Journal of Advance Research In Science And Engineering, ISSN-2319-8354, IJARSE, Vol. No.4, Issue 03, March 2015
15. J.Pamina, J.Beschi Raja,” Survey On Deep Learning Algorithms”, International Journal of Emerging Technology and Innovative Engineering Volume 5, Issue 1, January 2019 (ISSN: 2394 – 6598)
16. A‟inur A‟fifah Amri, Amelia Ritahani Ismail,* Abdullah Ahmad Zarir,”Comparative Performance of Deep Learning and Machine Learning Algorithms on Imbalanced Handwritten Data”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 2, 2018 [CrossRef]
17. M. A. Keyvanrad and M. M. Homayounpour, “A brief survey on deep belief networks and introducing a new object-oriented toolbox (DeeBNet),” pp. 1–27, 2014, [Online]. Available: http://arxiv.org/abs/1408.3264.
18. S. Mangayarkarasi,” Intrusion Detection Systems: A Survey and Analysis of Classification Techniques”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013
19. B. Deng, X. Zhang, W. Gong, and D. Shang, “An Overview of Extreme Learning Machine,” in 2019 4th International Conference on Control, Robotics and Cybernetics (CRC), 2019, pp. 189–195, DOI: 10.1109/CRC.2019.00046. [CrossRef]
20. M. Uzair and A. Mian, “Extreme Learning Machine Features,” Ieee Trans. Cybern., vol. 47, no. 3, pp. 651–660, 2017. [CrossRef]
21. W. Srimuang and S. Intarasothonchun, "Classification model of network intrusion using Weighted Extreme Learning Machine," 2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE), Songkhla, Thailand, 2015, pp. 190-194, doi: 10.1109/JCSSE.2015.7219794. [CrossRef]
22. M. Z. Alom, V. Bontupalli, and T. M. Taha, “Intrusion detection using deep belief networks,” 2016, doi: 10.1109/NAECON.2015.7443094. [CrossRef]
23. J. Ku, B. Zheng and D. Yun, "Intrusion Detection Based on Self-Adaptive Differential Evolutionary Extreme Learning Machine," 2017 International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 2017, pp. 94-100, doi: 10.1109/ICCNEA.2017.57. [CrossRef]
24. M. H. Ali, M. Fadlizolkipi, A. Firdaus and N. Z. Khidzir, "A hybrid Particle swarm optimization -Extreme Learning Machine approach for Intrusion Detection System," 2018 IEEE Student Conference on Research and Development (SCOReD), Selangor, Malaysia, 2018, pp. 1-4, doi: 10.1109/SCORED.2018.8711287. [CrossRef]
25. Liang and P. Pan, "Research on Intrusion Detection Based on Improved DBN-ELM," 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, 2019, pp. 495-499, doi: 10.1109/CISCE.2019.00115. [CrossRef]
26. K. Singh and K. J. Mathai, “Performance Comparison of Intrusion Detection System Between Deep Belief Network (DBN)Algorithm and State Preserving Extreme Learning Machine (SPELM) Algorithm,” 2019, doi: 10.1109/ICECCT.2019.8869492. [CrossRef]
27. P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, and D. Liu, “An optimization method for intrusion detection classification model based on deep belief network,” IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2925828. [CrossRef]
28. D. Alalade, "Intrusion Detection System in Smart Home Network Using Artificial Immune System and Extreme Learning Machine Hybrid Approach," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2, doi: 10.1109/WF-IoT48130.2020.9221151. [CrossRef]
29. N. A. H. Qaiwmchi, H. Amintoosi, and A. Mohajerzadeh, “Intrusion Detection System based on Gradient Corrected Online Sequential Extreme Learning Machine,” IEEE Access, p. 1, 2020, doi: 10.1109/ACCESS.2020.3047933. [CrossRef]

AUTHOR PROFILE

Shiladitya Raj, was born in India on January 8, 1988. He received the Engineering degree of B.E. in Electronics and communication from Swami Vivekananda College of Engineering & Technology Indore in 2009 and Post Graduate degree M.Tech in Computer Science from LNCT Bhopal in 2021.

He is Currently running a successful IT Development and Training Company in Bhopal, named with Saksham Digital Technology from 2018. He had a 11years of experience in IT Industry, in this duration he worked with reputed IT companies and got many Certifications as well. Being a android Developer, he developed many Mobile Applications like Cracko, Mobile Tracker, BusRoute, ETC.

Now a days he is working on some projects based on Artificial Intelligence and Machine Learning. Also providing training to corporate professionals on Android and IOS Mobile Application Development using trending languages like Flutter, Kotlin, Java, etc. Recently he developed on application where user can prepare for online exams, watch video, read notes and give Test online, with lot of other features. He has a collaboration with **Pearson VUE**, Pearson VUE is the leader in global computer-based testing solutions for academic, government, and professional testing programs, such as skills tests, IT certifications, and real estate licenses.

Megha Jain, was born in India on October 5, 1988. She received the Engineering degree, B.E. in Computer Science and engineering from TRUBA group of Institute Bhopal in 2010 and post graduate degree MTech. in Computer Science and Engineering From SATI Vidisha Bhopal, Madhya Pradesh, India, in 2012 and pursuing P.HD from VIT Bhopal. She is currently a Assistant Professor in the Department of Computer Science and Engineering, at Lakshmi Narain College of Technology, Excellence, Madhya Pradesh, India, She possesses 8 years of teaching experience. She has published more than 10 scientific papers in International and National reputed Journals and conference proceedings in the field of image processing, machine learning. She had been student project mentors under Smart India Hackathon.

Megha Kamble, was born in India on April 6, 1976. She received the Engineering degree, B.E. in Computer Science and engineering from Govt. engineering college, Aurangabad (Maharashtra) in 1996 and post graduate degree M.Tech. in Computer Science and Engineering and the Ph.D. degree in Information Technology from the Rajiv Gandhi State Technical University, Bhopal, Madhya Pradesh, India, in 2007 and 2017, respectively.

She is currently a Professor in the Department of Computer Science and Engineering, at Lakshmi Narain College of Technology, Madhya Pradesh, India, and has been the Head of Department and R&D cell convener from 2008 to 2015 in reputed institution in M.P. India. She possesses 21 years of experience including teaching, industrial and research work She was annual member of CSI from 2011 to 2014 and member of IAENG, life member of SSIRT.

She has published more than 30 scientific papers in International and National reputed Journals and conference proceedings in the field of mobile computing, soft computing, image processing, and wireless networks. Her current research interests include aging Multi gent System, Deep learning, Machine Learning, Soft Computing, Cellular Network, Channel Allocation, Software Engineering, Computer Graphics, Data analytics, IoT, NLP. She had been student project mentors under IEDC, and Smart India Hackathon, Govt of India initiative. She has been invited for expert talks for DST, Govt of India funded FDPs on Big data and AI in Bhopal, India. She has completed TEQIP funded CRS project on Solar Irradiance prediction using applied machine learning.