Detailed analysis of Machine Learning and Deep Learning technologies for Web Security

Chhaya Nayak
G. H. Raisoni College of Engineering and Management
Pune, Maharashtra, India.
chhaya2007@gmail.com

Dr. Ramakrishnan Raman
Professor and Director
Symbiosis Institute of Business Management
Pune & Symbiosis International (Deemed University)
Pune, Maharashtra, India
raman06@yahoo.com

Dr. P Dileep
Professor
Department of Computer Science and Engineering
Malla Reddy College of Engineering and Technology
Kompally, Hyderabad, Telangana,India
dileep.p505@gmail.com

Anita Gehlot
Uttaranchal Institute of Technology
Uttaranchal University
Dehradun, Uttarakhand, India
dranitagehlot@gmail.com

Gogula Laxmi Priyanka
Assistant Professor
Electronics and Communication Engineering
St Martin's Engineering College
Secunderabad, India.
priyagogula66@gmail.com

Dr. Dhiraj Kapila
Associate Professor
Department of Computer Science & Engineering
Lovely Professional University
Phagwara, Punjab, India
dhiraj.23509@lpu.co.in

2022 5th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-9826-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3I56241.2022.10073310

***Abstract*- As the Internet has expanded, web attacks have become more sophisticated, and web security is currently in a poor position. Websecurity technology is used to protect networks, programmes, and systems from webattacks. Webattacks are capable of getting access to delete or alter sensitive data, demand payment from users, and hinder company activities as usual. Currently, many technologies are becoming smarter than hackers and people, which make it challenging to put websecurity precautions into practise. Notwithstanding the primary writing surveys on ML and DL methods for network investigation and interruption recognition, this review report contains a concise instructional exercise portrayal of every ML/DL strategy. In light of the sequential or warm connections between's the works that addressed every strategy, they were listed, checked out, and summed up. We feature probably the most generally utilized network datasets; make sense of the troubles utilizing ML/DL for websecurity, and make ideas for future review since information are so essential to ML/DL strategies.**

Keywords: ML, DL, Web Security, intrusion detection

I. Introduction

The Web is changing the way that individual's study and work as a result of the rising joining of the Web and public activity, yet it likewise opens us to more serious security risks. It is an important issue that must be solved right away to figure out how to describe various network attacks, especially ones that have never been seen before.

Computers, networks, programmes, and data are all protected by a variety of technologies and procedures called "cybersecurity" in order to prevent assaults and unauthorized access, modification, or destruction. Computer and network security components together up a network security framework. Firewalls, antivirus projects, and intrusion detection systems are a portion of these frameworks (IDS). Unapproved framework conduct, including as use, duplicating, alteration, and erasure, can be found, verified, and detected with the aid of IDSs.

All these internal and external intrusions are termed security infractions. Hybrid, anomaly-based, and misuse-based network analysis are the three main categories for IDSs. Misuse-based detection methods look for known assaults by using their telltale signs. They don't raise many phoney alerts and are used for known attack types. However, administrators are expected to manually alter the database rules and signatures on a constant basis. Fresh (zero-day) attacks are difficult to detect with present technology.

Anomaly-based techniques can identify outliers by looking at usual network and system behaviour. They are desirable because they can detect zero-day attacks. The normal activity profiles of each system, application, or network are also distinct; it makes it even harder for attackers to determine which tasks they can perform quietly. Furthermore, it is feasible to characterize the marks for misuse locators utilizing the information that peculiarity-based approaches (new attacks) alert on. Inconsistency based procedures' greatest disadvantage is the chance for critical misleading problem rates on the grounds that already undetected framework conduct might be named as strange.

Misuse and oddity discovery are joined in hybrid detection [1]. Bringing down how much misleading up-sides for obscure attacks and increment the pace of known intrusion detection is utilized. Procedures consolidating ML and DL are normal.

The writing on ML and DL techniques for network protection applications is evaluated in this review. Every method has various purposes, and ML and DL are utilized in network intrusion detection. It underscores ML and DL innovation ML/DL draws near, and their explanations for network security. Our study focuses on articles that follow standards and use the phrases "machine learning," "deep learning," and "cyber" in Google Scholar searches. The newest hot papers are employed in particular because they outline the favoured methods.

979-8-3503-9826-7/22/$31.00 ©2022 IEEE

This paper's goal is to aid people interested in ML/DL network intrusion detection research.

A full explanation of the ML/DL methods is therefore stressed, and each ML and DL method is referenced to a seminal work. Examples of how the strategies were applied in cyber security are given.

II. Literature Review

In their investigation of technological advancements in anomaly detection, [2] analyze the annoying issues and difficulties of oddity detection systems and hybrid intrusion detection frameworks. While their study just incorporates works from 2002 to 2006, our overview likewise incorporates distributions from later years. Dissimilar to [3], this paper examines the utilization of ML/DL in an assortment of interruption location situations as opposed to zeroing in fundamentally on cloud security. The majority of the study by Revathi S et al. is devoted to machine-learning intrusion methods [4]. On the NSL-KDD interruption recognition dataset, the creators offer a wide assortment of ML procedures; by and by, their concentrate just purposes an abuse discovery setting. In contrast, both abuse detection and anomaly detection are covered in this paper.

The contributions of research that addresses a variety of facets of this topic are identified and discussed in Sahoo et al [5] detection as a machine-learning challenge (such as feature representation and algorithm design). They do not, however, go into technical specifics about the algorithm, in contrast to this paper.

The focus of [6] study is on machine learning techniques and how they are applied to intrusion detection. In-depth descriptions are provided for algorithms including Decision Trees, Fuzzy Logic, Bayesian Networks, Support Vector Machines, Genetic Algorithms, and Fuzzy Networks. Major ML/DL techniques like clustering, AI systems, and swarm intelligence are not mentioned, though. They concentrate on network intrusion detection in their article. Attackers trying to enter a wired network must get past several operating system and firewall defences or physically access the network. Wireless networks, notwithstanding, are more helpless against pernicious attacks and more challenging to shield than wired networks since they can be gone after from any hub.

Both wired and wireless networks can employ the ML and DL techniques outlined in this article for intrusion detection. For readers interested in learning more about wireless network security, studies like [7], which focus further on the intrusion detection system architectures that have been developed for MANETs, are accessible.

Artificial intelligence, deep learning, and machine learning all have complicated relationships with one another (AI). Artificial intelligence (AI), a relatively new field of technical study, investigates and develops theories, practises, approaches, and software tools that imitate, improve upon, increase human intelligence, etc. [8] A part of software engineering means to grasp the essentials of insight and make new sorts of savvy machines that look like individuals. Researchers in this field are examining natural language processing, expert systems, robotics, and computer vision. The limit of artificial intelligence to reproduce thought and mindfulness.AI is not human intelligence, despite the possibility that thinking like a human is more intelligent than human intelligence.

Machine learning and computational statistics, a subfield of artificial intelligence that likewise focuses on using computers to generate predictions, have many similarities and overlaps. The field's technique, theory, and fields of application are all closely related to mathematical optimization. Unsupervised learning, often known as data mining, is a type of machine learning that is frequently confused with machine learning (ML) [9]. After learning and creating baseline behavioural profiles for various entities, unsupervised machine learning (ML) can be utilised to find major abnormalities [10]. Arthur Samuel, the man of machine learning, claims that this field of research enables computers to learn without being explicitly taught. Classification and regression are the primary objectives of machine learning (MLmain), and they make use of previously understood, well-known properties from training data.

Machine learning's field of DL research is still quite young. It is motivated by the development of a neural network that, for analytical learning, resembles the human brain. It mirrors how the human cerebrum deciphers tactile info like pictures, sounds, and discourse [11].

[12] fostered the possibility of DL in view of the deep belief network (DBN), in which an unaided avaricious layer-by-layer preparing technique is proposed that offers expect settling the enhancement issue of profound construction. Then, a multi-layer programmed encoder's profound design is recommended. Utilizing a space relative relationship to lessen the quantity of boundaries and improve preparing execution, [13] convolution neural network is a genuine multi-layer structure preparing strategy.

The following are some of the distinctions between ML and DL:

1) *Data dependencies.* Deep learning and conventional machine learning differ mostly in how well they perform as the volume of data grows. Since deep learning calculations need a ton of information to successfully comprehend the information, they perform ineffectively when the information volumes are nearly nothing. However, the performance will be improved here if the conventional machine-learning algorithm follows the suggested recommendations [11].

2) *Hardware specifications.* There are various matrix operations needed by the DL method. The GPU is frequently effective at improving matrix operations. Therefore, for the DL to work correctly, the GPU is a requirement for hardware. DL makes greater use of GPU-powered high-performance computers than conventional machine learning methods [14].

3) *Processing of features.* The procedure of feature processing involves using domain knowledge to improve a feature extractor the data's complexity and provide patterns that help learning algorithms function more effectively. Processing features is a labor-intensive procedure that demands knowledge. Most of an application's properties in ML should be characterized by an expert prior to being encoded as an information type. Pixel values, structures, surfaces, positions, and directions are instances of highlights. The effectiveness of most ML systems depends on how accurate the retrieved attributes are. DL stands out from previous machine-learning techniques in that it tries to directly extract high-level attributes from the data [15]. As a result, developing a feature extractor for each issue using DL is quicker.

4) *Approach to problem-solving.* Traditional machine learning algorithms typically divide an issue into several smaller problems, solve the smaller problems, and then combine the results to produce the desired outcome. On the other hand, deep learning encourages direct, comprehensive problem-solving.

5) *Time for execution.* Because DL algorithms include many parameters, training them frequently takes a lengthy time; as a result, the training stage lasts longer. In contrast to ML training, which only takes a few seconds to a few hours, the fastest DL algorithm, like ResNet, requires precisely 2 weeks to compile a training session. The exam time is the exact reverse, though. Running deep learning algorithms while testing takes relatively little time. As the amount of data rises, the test duration increases in comparison to some ML algorithms. Due to the short test duration of some ML algorithms, this argument does not hold true for all of them.

6) *Interpretability.* Crucially, when contrasting ML and DL, interpretability is a crucial consideration. The performance of DL in recognizing handwritten numbers can be fairly impressive, coming close to meeting human standards. A DL algorithm won't, however, explain why it produced this outcome [11]. A deep neural network node is naturally activated mathematically speaking. But how do these layers of neurons interact with one another and how should neurons be mathematically represented? It is difficult to explain how the outcome was created as a result. The decision's explanation is clear since the machine-learning algorithm, on the other hand, explicitly states the criteria upon which it bases its conclusions.

III. Methodology

Data learning is the foundation of the machine learning technique known as DL. Similar to how an image can be defined in many different ways; a measurement can also be described more abstractly as a collection of edges, a region with a specific shape, or something else. Learning tasks from situations is made easier by the use of specialized representations. Like ML techniques, DL approaches use both supervised and unsupervised learning. Different learning frameworks have produced learning models that are very dissimilar. The advantage of DL is the effective replacement of features manually using hierarchical feature extraction and feature learning that is semi-supervised or unsupervised.

The machine learning algorithms KNN, SVM, Decision Trees, and Bayes are extensively used. DBM, CNN, and LSTM are a few examples of DL model components. There are numerous options, including ways to enhance the model and integration as well as options for selecting the number of layers and nodes. Alternative models must be assessed against a number of criteria after training is finished.

A. Support Vector Mechanism

One of the most steady and exact AI procedures is the Support Vector Machine (SVM). Support Vector Regression and SVC-Support Vector Classification make up the majority of it (SVR). The idea of decision boundaries forms the foundation of the SVC. A decision border separates two groups with distinct class values from a collection of instances. Both double and multi-class characterizations are upheld by the SVC. The ideal separation hyperplane is determined by the separation hyperplane that is closest to the support vector. The locations on the opposite side of the separation hyperplane from the feature space and the corresponding mapping input vectors fall into separate classes in the classification process. The SVM uses the appropriate kernel functions to move data points onto higher dimensional spaces where they can be separated when they cannot be separated linearly.

The concentrate by [16] joins fluffy C-implies bunching, a fake brain organization, and backing vector machine-interruption identification advances. The fluffy C-means clustering algorithm isolates the heterogeneous preparation information into homogeneous subsets, decreasing the intricacy of every subset and upgrading discovery accuracy. The last characterization is done utilizing the straight SVM classifier following introductory grouping and ANN preparing on the pertinent homogeneous subsets. The exploratory discoveries utilizing the adjusted KDD CUP 99 dataset show the adequacy of this methodology.

The KDD Cup 99 dataset was parted into 4 subgroups relying upon the different kinds of attack and prepared separately in a similar report. Assaults like DoS and Test are more successive and unmistakable from regular exercises. U2R and R2L attacks, then again, are hidden in the parcel information, making it trying to do exact assault identification. The methodology has reliably given the most noteworthy evaluations to invasions, everything being equal. DoS, Test, R2L, and U2R classes' general exactness was 99.63%, 98.65%, 98.91%, and 98.91%, separately. The trained classifier is less able to detect irregularities in the actual network, although this method's classification impact is greater than other reported intrusion detection algorithms.

B. K-Nearest Neighbour

The kNN classifier is built on the distance function, which determines how different or similar two instances are.

$$d(X,Y) = \sqrt{\sum_{k=1}^{n}(X_k - Y_k)^2} \qquad (1)$$

X_k Is the kth highlighted component of occurrence x, Y_k is the kth highlighted component of example y, and n is the absolute number of elements in the dataset. Such factors are utilized to work out the standard Euclidean distance d(x, y) between two models x and y. Expect that U is the kNN classifier's plan set. The plan set contains S tests altogether. Give C stand access for the different class assignments L that can be tracked down in S, like C1, C2, and so on. Allow x to address the information vector for which the projected class name is required. Let the kth vector in the plan set S beY_k. The kNN's calculation will likely distinguish the k vectors in plan set S that are generally like information vector x. On the off chance that by far most of the k nearest vectors have Cj as their group, then the info vector x is arranged into class Cj K.

[17] Rao et al. utilized Utilizing Listed Fractional Distance Search k-Closest Neighbor (IKPDS), a few assault techniques and k qualities are tried (i.e., 3, 5, and 10). From the NSl-KDD dataset, they arbitrarily picked 12,597 examples to dissect the arrangement results. Quicker grouping times and 99.64% exactness were found in the outcomes. IKPDS and Organization Interruption Discovery Frameworks (NIDS) give arrangement discoveries all the more rapidly, as indicated by preliminary information. Since precision and recall rate were ignored, the analysis of the experiment's test signs was faulty.

C. *Decision Tree*

Each leaf node of a decision tree addresses a classification, each inner node addresses a trial of a specific property, and each branch addresses the result of the test. An AI prescient model that shows the relationship between object values and item includes is the decision tree. Each leaf node in the tree relates to the worth of the item addressed by the way from the root node to the leaf node, while every node in the tree addresses potential trait esteem. Utilize another decision tree to deal with each result independently in the event that you really want a perplexing result. There is just a single result for the decision tree. The ID3, C4.5, and Truck decision tree models are broadly utilized.

Figure 1 shows how the decision tree categorises the samples using training conditions to improve accuracy for identified intrusion tactics; however, it is inappropriate for detecting unidentified incursion.

For the NSL-KDD dataset, Ingre and Bhupendra [18] suggest a decision tree-based IDS. 14 techniques were chosen for feature selection utilising the correlation feature selection (CFS) method. On a KDD99 dataset, the experiments were run. The method's accuracy is roughly 91.30%.

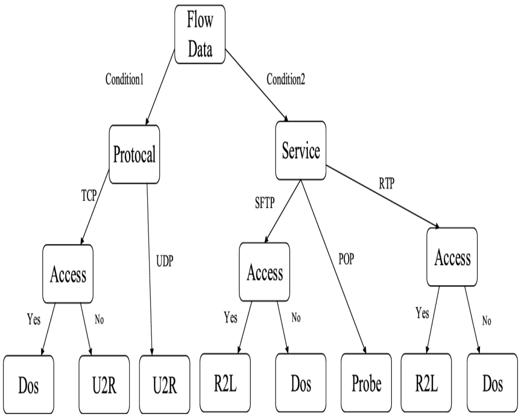

Figure 1: Decision Tree for cyber security

D. *Network for Deep Belief*

Deep Belief Network (DBN) is a probabilistic multiplicative model made out of many layers of stochastic and secret factors. Different hidden layers can efficiently train data by activating one Restricted Boltzmann Machine (RBM) for further training stages thanks to the composition and stacking of numerous RBMs. This is the connection between the DBN and the Restricted Boltzmann Machine (RBM). A specific topological structure seen in Boltzmann machines is called the RBM (BM). The BM model, in light of an energy capability, was created in factual material science to recreate high-request collaborations between factors. The symmetric coupled irregular criticism twofold unit brain organization, or BM, contains various secret layers notwithstanding a noticeable layer. The noticeable unit and secret unit of the organization hub are utilized to address an irregular organization and an irregular climate, individually. The learning model use weighting to indicate the connections between the components.

Ding and Yuxin used Deep Belief Nets (DBNs) in their study [19] to locate malware. They provide samples of PE files that can be accessed online. DBNs utilize unsupervised learning out how to uncover numerous layers of data, which are then added to and tweaked in a feed-forward brain organization to upgrade segregation. DBNs are less inclined to overfitting than feedforward brain networks with arbitrary beginning loads due to the unaided pre-preparing calculation. Also, it works with the preparation of brain networks with various secret layers. In the studies, DBNs outperformed a number of other well-known learning methods, including SVM, KNN, and decision trees, due to their capacity to learn from fresh unlabeled data. The method's accuracy is around 95.1%, but no other information is given.

E. *Recursive neural networks*

To analyse sequence data, a recursive neural network (RNN) is employed. There is no link between any of the layer's nodes in the typical neural network model's fully connected layers. Information is passed from the information layer on to the implanting layer to the result layer. This normal brain network can't tackle a ton of issues.

Multi-layer network, Figure 2 portrays the RNN timing properties as the general network design. Long Transient Memory (LSTM) and a Gated Intermittent Unit (GRU) are qualities of the upgraded RNN model. The effects of six generally utilized streamlining agents on the LSTM interruption location model are looked at in Le et al work's [20] work. The model of LSTM RNN with Nadam analyzer beats previous outcomes on the KDD Cup 99 dataset. The permitted deception rate for interruption location is 9.98%, and exactness and accuracy are 97.54% and 98.95%, separately.

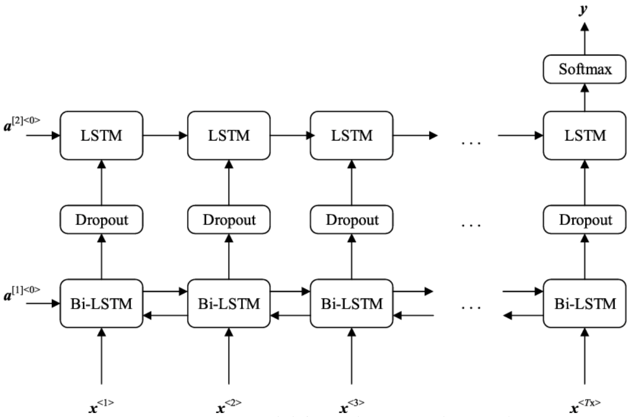

Figure 2: RNN Model for Cyber or Web Security

F. CNN Model

In the fields of discourse examination and vision acknowledgment, convolutional neural networks (CNNs) are a well-known sort of fake neural networks. Because of its weight-sharing organization structure, which all the more intently looks like a natural cerebrum organization, it is simpler to recreate and utilizes less loads. This advantage is particularly clear when a multi-layered picture is used as the organization input since the troublesome element extraction and information reproduction methodology intrinsic in the traditional acknowledgment strategy can be discarded. A complex sensor called a convolutional network was made to perceive two-layered structures that are unquestionably sturdy to interpretation, scaling, shifting, and different sorts of misshaping.

CNN, the first genuinely successful learning algorithm in this field, can be used to train the multi-layer network design shown in Fig 3.

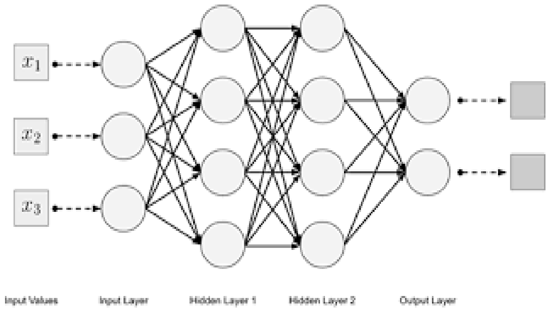

Figure 3: CNN model for Cyber or Web Security

One-layered convolutional neural network starts to finish scrambled traffic order is presented by[21]. A public datasets, ISCX VPN and nonVPN traffic dataset is utilized for the technique's confirmation.

IV. Results and Discussion

As seen in Table 1, deep learning and machine learning have been used extensively in academic research on intrusion detection. These studies attract attention to certain inequities and a few issues in this field of study, particularly in the following areas: I Despite the fact that the same dataset is used, the benchmark datasets are unusual, and each institute uses a different sample extraction method. (ii) The outcome is biassed, the evaluation measures are inconsistent, and many studies just analyse test accuracy. However, multi-criteria evaluation studies usually employ unique metric combinations, making it impossible to compare the results of several studies. (iii) Despite the algorithm's temporal complexity and the effectiveness of its detection in actual networks, with deployment effectiveness receiving less attention and the majority of research is carried out in lab settings.

In addition to the problem, Table 1 also displays trends in intrusion detection. (i) Hybrid model research has grown in popularity recently and by carefully combining different methods, better data metrics can be obtained. (ii) The progression in deep learning has made start to finish picking up, including the mechanized treatment of tremendous volumes of information, possible. Although there is little room for interpretation, fine-tuning demands a lot of trial and error and experience. (iii) More research is starting to recognise the importance of algorithms and models in practical applications, as seen by the rise in studies comparing the performance of various algorithms over time. (iv) The organization is responsible for various new datasets that will propel the flow research on Web security-related subjects.

TABLE I: Methods for ML and DL and data utilization

Methods	Data Used	Accuracy	Precision	FAR	F1 Score
C-SVM	10% KDD Cup 99	98.91%	99.52%	-	0.99
IPDS-KNN	Part of NSL-KDD	99.64%	-	-	-
CFS-DT	NSL-KDD	91.30%	-	9.72%	-
DBN	Net flow	95.10%	-	-	-
LSTM	KDD Cup 99	97.54%	97.95%	9.98%	-
1D-CNN	ISCX dataset	-	98.30%	-	0.97

A future for intrusion detection research is also provided by the issues and trends mentioned above:

A. Data sets

There are problems with redundant data, and in data, and an imbalanced number of categories in existing databases. After processing, the data can be improved, but there is a volume issue. Building network intrusion detection datasets with strong information, wide sort inclusion, and adjusted example quantities of assault classifications consequently happens to most extreme significance in the interruption recognition area.

B. Hybrid Method

Despite the paucity of research on intrusion detection that blends deep learning and machine learning methodologies, hybrid detection systems commonly include machine learning techniques. This is an important avenue of study, and AlphaGo has shown that it is viable.

C. Detected speed

The approach can be employed for shorter periods of time given the intricacy of MI and DL algorithms by reducing the duration of detection and speeding up detection from algorithm and hardware aspects. For parallel computing, hardware can make use of many computers. The idea of combining the two strategies is very intriguing.

D. Electronic Learning

Network intrusion strategies are continuously evolving. One more fascinating area of exploration is the manner by which to grow the prepared model's ability to fit the approaching information. The model may currently be improved for all intents and purposes with move learning with less marked information ought to upgrade network discovery execution.

V. Conclusion

In this article, we assess the advancement on machine learning (ML) and deep learning (DL) strategies for security of network. The paper presents the latest ML and DL applications in the interruption identification field, with an emphasis on the past three years. Unfortunately, the ideal technique for recognizing interruptions has not yet been found. The correlations of the elective thoughts uncover that each way to deal with fostering an interruption location framework has advantages and disadvantages of its own. Choosing an implementation approach for an intrusion detection system might be challenging.

For framework testing and preparing, network interruption identification datasets are vital. Without delegate information, the ML and DL calculations can't be utilized; yet, creating such a dataset is testing and tedious. The ongoing public dataset, be that as it may, has various issues, including conflicting information, obsolete data, and so forth. The development of this course's review has been seriously compelled by these issues.

Quick organization data changes make it hard to prepare and utilize DL and ML models. Models should be rapidly and broadly retrained thus. Consequently, the future examination in this space will focus on gradual learning and long lasting learning.

References

[1] E. Viegas, A. O. Santin, A. França, R. Jasinski, V. A. Pedroni, and L. S. Oliveira, "Towards an Energy-Efficient Anomaly-Based Intrusion Detection Engine for Embedded Systems," IEEE Trans. Comput., vol. 66, no. 1, pp. 163–177, 2017.

[2] A. Patcha and J. M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput. Netw., vol. 51, no. 12, pp. 3448–3470, 2007.

[3] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "Review: A survey of intrusion detection techniques in Cloud," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, 2013.

[4] S. Revathi and A. Malathi, "A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection," in International Journal of Engineering Research and Technology, 2013.

[5] D. Sahoo, C. Liu, and S. C. H. Hoi, "Malicious URL Detection using Machine Learning: A Survey," arXiv:1701.07179, 2017.

[6] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Commun. Surv. Tutor., vol. 18, no. 2, pp. 1153–1176, 2016.

[7] M. Soni, M. Ahirwa, and S. Agrawal, "A Survey on Intrusion Detection Techniques in MANET," in International Conference on Computational Intelligence and Communication Networks, 2016, pp. 1027–1032.

[8] V. Panwar, D.K. Sharma, K.V.P.Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings, https://Doi.Org/10.1016/J.Matpr.2021.03.642

[9] A. Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191. https://doi.org/10.1016/j.matpr.2019.06.292

[10] A. Jain, A.K.Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684. https://doi.org/10.1016/j.matpr.2019.12.010

[11] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261. https://doi.org/10.1016/j.matpr.2017.07.054

[12] G. E. Hinton, "Deep belief networks," Scholarpedia, vol. 4, no. 6, p. 5947, 2009. doi:10.4249/scholarpedia.5947

[13] Y. Lécun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," Proc. IEEE, vol. 86, no. 11, pp. 2278–2324, 2001. 10.1109/5.726791

[14] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Fiber Matrix Composite through Electric Discharge Machining: A short review" Material Today Proceeding. https://doi.org/10.1016/j.matpr.2021.07.288

[15] A. M. Chandrasekhar and K. Raghuveer, "Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset," in International Conference on Communications and Signal Processing, 2014, pp. 672–676. 10.1109/ICCSP.2014.6949927

[16] B. B. Rao and K. Swathi, "Fast kNN Classifiers for Network Intrusion Detection System," Indian J. Sci. Technol., vol. 10, no. 14, pp. 1–10, 2017. 10.17485/ijst/2017/v10i14/93690

[17] B. Ingre, A. Yadav, and A. K. Soni, "Decision Tree Based Intrusion Detection System for NSL-KDD Dataset," in International Conference on Information and Communication Technology for Intelligent Systems., 2017, pp. 207–218. 10.1007/978-3-319-63645-0_23

[18] Y. Ding, S. Chen, and J. Xu, "Application of Deep Belief Networks for opcode based malware detection," in International Joint Conference on Neural Networks, 2016, pp. 3901–3908. 10.1109/IJCNN.2016.7727705

[19] G. Kim, H. Yi, J. Lee, Y. Paek, and S. Yoon, "LSTM-Based System-Call Language Modeling and Robust Ensemble Method for Designing Host- Based Intrusion Detection Systems," arXiv:1611.01726, 2016.https://doi.org/10.48550/arXiv.1611.01726

[20] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 43–48. 10.1109/ISI.2017.8004872.