International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-10, August 2020

An Intrusion Detection System- Techniques and Algorithms of Machine and Deep Learning

Kavitha S, Uma Maheswari N, Venkatesh R

Abstract: ***Computer networks are vital component for today's development of science and technology, due to the emergence of limitless communication pattern and exponential count of network devices cyber security become crucial for this world to secure the most valuable data or information which is more vulnerable for attack by the intruders. New pattern of intrusion and attacks are created in everyday manner by potential intruders and they should be identified by efficient Intrusion Detection Systems (IDSs), also proper counter should be applied for. The paper surveys about the discussion of various machine /deep learning technology and algorithm related to Intrusion Detection System (IDSs) for the real time performance of the system. Finally the literature review investigated gives some open issues which will need to be considered for further research in the field of network security.***

Keywords: Network Security, Intrusion Detection System, Signature-Based IDS, Anomaly-Based IDS, Machine Learning, Deep Learning, Artificial Neural Network, Deep Belief Network

I. INTRODUCTION

Great numbers of data are processed by various Information and communications technology (ICT) tools are vulnerable to various internal and external attacks [1]. Many threats and security problems are faced by computer network. The risks for data are growing exponentially day by day, even though existing system has procedures and mechanism to deal with these risks, threat should be identified automatically without any delay. A better security control system should protect, identify and do control measures for attacks. Intrusion detection system (IDS), a technique detects both internal and external intrusions of the target and also find the network anomalies which indicate the potential intrusion activities. To monitor the network traffic and computer system, IDS has possible tools and mechanisms for performing analysing activities and to detect the intrusions of the targeting system [2].IDSs discover and determine the illegal system behavior such as copy, alter and destruction [3]. Security breaches can happen through Internal and External intrusions. The three types of IDS network analysis are: signature-based (misuse-based), anomaly- based, and hybrid IDS. The ML and DL methods detect and perform better for detecting intrusion in the networks of wired and wireless.

Revised Manuscript Received on August 30, 2020.
* Correspondence Author
Kavitha S, Assistant Professor, Department of Computer Science and Engineering, Velammal College of Engineering and Technology, Madurai ,Tamil Nadu, India. E-mail:kavitha3101@gmail.com
Dr. Uma Maheswari N, Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India. E-mail: numamahi@gmail.com
Dr.Venkatesh R, Professor, Department of Information Technology, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India. E-mail:rlvenkatesh@gmail.com

The IDS uses traditional machine learning (ML) algorithms like Support Vector Machines, Hidden Markov Models, Fuzzy Logic and Neural Networks [4], and the architectures are shallow in nature and not suitable for handling intrusion in the big data environment.
A common problem in large dataset is, it cannot handle the noise because of its difficulty in identifying the unknown attacks, and it's a complex task in real time environment.

Deep learning is a type of ML methods, in which numerous information-processing layers in hierarchical architectures are utilized for classifying patterns and for feature or representation learning [5]. Today, deep learning has become a very important and successful research trend in the ML community because of its great success in these fields [6]. In the survey, section II presents the network attacks and intrusion detection system, section III about machine learning and deep learning. The section IV is the literature survey of machine and deep learning approaches in intrusion detection systems and the paper concludes in section V.

II. NETWORK ATTACKS AND INTRUSION DETECTION SYSTEM

2.1 Network Attacks:

The attacks can be active or passive [7]. An active attack is the action attempting to intrude the system. During active intrusion, the intruders alter the system data and also introduce new data to the system. The active attacks types are masquerade, distributed DOS and session replay. Few examples of active attacks are Trojan, Viruses, and Worms. The passive attack learns and makes use the system information but don't affect the system resources.

The passive attacks types are Scanning, Tapping and Encryption. Insider or outsider causes intrusion in the company network. A person's computer or network exposed to insider attack (malicious attack) using authorized system access. Illegal use of system leads to outsider attack. Few types of outsider attacks are spam, spoofing and spin.

2.2 Intrusion Detection Systems:

Intrusion detection system has different criteria to classify; the architectural structure, category of system it protects and time to process the data. Two types of IDS are based on their locations: Host based IDS and Network based IDS [8]. Based on IDS techniques it is classified as Signature-Based and Anomaly-Based.

- Host-Based IDS: server attack can be detected by registration files, listening to the traffic, and transactions.
- Network-Based IDS: can be detected by recording the content of each packet passing through the network, by listening the network traffic and cutoff the attacks when needed and report creation.

• Signature-Based IDS: Known attack types are detected.
• Anomaly-Based IDS: Unseen attacks are detected.

2.3 Intrusion Detection Approaches:

The Intrusion Detection System developed various techniques for data modeling and table creation using classified modeled data [9]. The techniques are: Statistical: The statistical measurements are the systems first instances. The statistical models are created using the first instances by examining the behaviour of system or user. The newly created statistical model can determine new type of intrusions. Chi-square distributions, Principal Component Analysis, Gaussian Mixture Distribution are some statistical methods

• Artificial Neural Networks: The given data are modeled using artificial neuron graphs in ANN. In this model, the algorithms associate their vectors to create new data. This approach can be used to learn and examine the system data behavior [10].

• Support Vector Machines: The feature vector selection for IDS can be done using this method. The method distinguishes two classes of data in appropriate way using feature vector. Sound analysis, face recognition systems are some classification problems use this support vector machines.

• Data Mining: It uses information reaching in data of large scale environment. Data mining uses rule extraction to find relation between user and data.

• Rule-Based Systems: The system traffic are examined, rules are formed and detects attacks. This is done by the specialized person in this area.

• Fuzzy Logic: It's a human like thinking and aims to process by converting to mathematical functions.

III. MACHINE LEARNING AND DEEP LEARNING

The relation among Machine learning, Deep learning and artificial intelligence are some great riddles. Artificial Intelligence is a technical study that models the procedures and methods of human intelligence [11]. AI understands the human intelligence and a new intelligent machine type is produced to respond like human. AI is a human like thinking and not a human intelligent but thinking may exceed human intelligence. Machine Learning is related to computational statistics focuses on making computer prediction. It has mathematical function that connects methods, procedures and application domain of the field. Sometimes Machine learning combined with data mining and its subfield focus on exploratory data to analyze it and known as unsupervised learning [12].The unsupervised learning establish and learn the behavioral pattern of different entities and find meaningful anomalies[13]. Ml is the field that allow computers to learn without explicit programming, is the concept by Arthur Samuel (pioneer of ML). Classification and regression focused in ML that learns known features from the previously trained data. Deep learning is the representation of data learning. For example, an image can be represented in different ways like vector value of pixel intensity, or as a value of edges, particular region shape. Supervised Learning and unsupervised learning are two approaches of deep learning like machine learning. Different learning frameworks are used to build different learning models. The benefit of deep learning is the feature extraction methods like unsupervised or semi-supervised feature learning and hierarchical feature are used for manual feature replacement [14].

3.1 ML and DL differences include the following

• Data dependencies: Performance is the great difference between machine learning and deep learning, as there is an increase in data. Machine learning performs well even in small volume of data, as it follows algorithm as the established rules for handling it. Deep learning performs well only in large quantity of data, as it needs to perfectly understand the data [15].

• Hardware dependencies: GPU is the hardware requirement of Deep learning, as it requires matrix operations to be performed efficiently. The high performance of Deep learning algorithm relies on machine with GPUs than to do with machine learning algorithm [16].

• Feature processing: It is done to extract feature using domain knowledge to reduce data complexity and make algorithm to work better based on pattern generated. Feature processing consumes more time and requires knowledge specialization. The machine learning uses expert to determine the application characterization and encode the type of data. The features are pixel value, locations, shape, orientations and textures. Machine learning algorithm performance is determined by the extraction of feature accurately. The great difference between deep learning and machine learning algorithm is the high level of feature extraction from data. The effort taken to design the problem feature extraction is reduced in deep learning [14].

• Problem-solving method: Traditional Machine learning algorithm solve problem by breaking problem into sub problems and the sub problems are solved , to get final result where as deep learning involves end to end problem solving.

•Execution time: To train a deep learning algorithm, it takes long time due to the number of parameters. ResNet is the deep learning algorithm takes 2 weeks to complete the training, whereas the training by machine learning takes maximum hours. When consider test time, deep learning is better than machine learning, as the time increases as the amount of increased data in machine learning and this is not the case in all machine learning, some machine learning may have shortest test time.

•Interpretability: To compare machine learning with deep learning, interpretability is considered to be one of the important factors. The handwritten number recognition is done by deep learning and it's a great performance for standards of people. The deep learning algorithm provides the results and does not tell why this result produced [15]. In the point of mathematical view, deep neural network node is activated. It's a difficult task to explain how a neuron modeled, how the layers of neurons work and how the results are generated. In contrast, the machine learning provides the reason/rules explicitly for choosing an algorithm and it's an easy task to find the decision for the reason.

3.2 Steps of Machine learning method [12]:

• Feature Engineering. It is the basis for prediction choice (features, attributes).

• Choose the appropriate machine learning algorithm (like classification or regression algorithm, high or fast complexity)

• The model performance is trained and tested.
• Unknown data is classified or predicted using trained model.

The deep learning and machine learning steps are similar but the feature extraction is manual in machine learning and automated in deep learning. The different mission types require constant trial and error method for selecting machine learning/ deep learning algorithm in model selection. Supervised, unsupervised and semi-supervised are different approaches of machine learning/deep learning. In supervised learning, the occurrences consist of input instances and label. This supervised learning algorithm analyzes the trained data and how the results are mapped to new instances. Unsupervised learning is the task of machine learning that detects the hidden structure description from the data of unlabeled one. The output accuracy of algorithm could not be evaluated because of the unlabeled data and the data key features are summarized and elaborated. Semi supervised learning is the combination of supervised and unsupervised learning. In semi supervised learning, pattern recognition is done using labeled data where as it uses large amount of data in unlabeled manner. The advantage of semi supervised learning; accuracy can be high and label efforts are reduced.

The known machine learning algorithms are SVM, KNN, Bayes and decision tree. The deep learning algorithms are CNN, LSTM, DBM. How to choose a nodes and number of layers are some parameters and how the models and integrations are improved. Once training completed, it has to be evaluated on different aspects of alternative models.

IV. LITERATURE SURVEY/RELATED SURVEYS

The literature survey includes different studies of machine learning and deep learning techniques of intrusion detection system. Table 1 illustrates that the study has been categorized based on the technique used/proposed methodology, dataset used, purpose of the work, advantages, future Scope/ limitation.

Sydney et al. [17] designed an intrusion detection system for traffic of wireless network coupled with a technique wrapper based feature extraction and generated a reduced feature vector. The proposed work WFEU-FFDNN (Wrapper- Based-Feature-Extraction Unit (WFEU)Feed-Forward-Deep Neural Network (FFDNN) performed on the datasets. The intrusion detection dataset involved are UNSW-NB15 and AWID. Detection accuracy is high in this, than other approaches. The individual class detection rate of UNSW-NB15 and AWID performs better after the application of wrapper based feature extraction method.

Vijayanand et al.[18] performed the approach on the standard dataset CICIDS2017 and ADFA-LD. The wrapperbased approach using modified whaleoptimization algorithm (WOA) detects intrusions accurately by selecting the network data informative feature and has detection rate better than other WOA and evolutionary algorithm. The work can be further optimized by modifying the filter based WOA feature selection method (information gain). Mohammad Mehedi Hassan et al.[19] proposed hybrid deep learning model with deep CNN(deep CNN–WDLSTM IDS) to evaluate the intrusion detection dataset. Dataset used are UNSW-NB15 and a comparison is made with ISCX2012 dataset. To avoid the problem of over fitting; a technique of drop connect with hidden to hidden weight matrices used with LSTM and use LSTM to avoid gradient vanishing problem by retaining the extracted features of long term dependencies. The real time intrusion detection system can be obtained by further analyzing the complex and bigger datasets. R. Vinayakumar et al.[20] had worked on KDDCup 99 dataset by performing Deep neural network (DNN) that Scale-Hybrid-IDS-AlertNet (SHIA) used to monitor network traffic effectively and proactively uses host level events to alert the cyber-attacks. The unpredictable and unforeseen cyberattacks can be detected and classified. Further the performance of deep neural network architecture can be improved through advanced hardware distributed approach. Mengmeng Ge et al.[21] proposed a model that differentiate high accuracy in traffic of normal and malicious node and achieves low false positive and false negative predictions. The FeedForward neural networks model (FNN) classification of binary and multiclass was performed over BoT-IoT dataset and has High Classification Accuracy. The DDoS/DoS and reconnaissance attack binary classification capability demonstrated the result close to 0.99 against the evaluation criteria like accuracy,F1score, recall and precision can be further improved by developing the classifier for the attack of each subcategory and includes the timestamp into as a new feature and develops a new model of deep neural network. Time series data can be modeled using long short term memory network. Nagaraj Balakrishnan et al.[22] proposed Deep Belief Network-Deep Learning algorithm performs intelligent intrusion detection on anomaly dataset and scrutinizes the active malicious activity in the network and creates a diversion/breaching on it. It creates a secure way to drive the network in the uncertain situation and improves the rate of detection and accuracy. More anomaly datasets are trained for promising outcomes of Deep Belief network. Fahimeh Farahnakian et al.[23] had trained a model to avoid the problem of over fitting and local optima and handled the Deep-Auto-Encoder based- Intrusion Detection System- (DAE-IDS) model in greedy layer fashion. The input can be classified into normal /attack using soft-max layer after training four autoencoders. The further work can be explored on autoencoder, how sparse to design the constraints of deep autoencoder and how to improve the effectiveness of intrusion detection. M. Al-Qatf et al.[24] has developed intrusion detection network model for binary and multiclass data for predicting accurately the intrusion of network using Pre-learned sparse autoencoder with SVM(SAE-SVM). The NSL KDD dataset used 5 category classification and shows high accuracy rate. Further, the improvement for good feature representation and dimensionality reduction using STL multiple stages and hybrid feature learning model. The training and testing times of model can be reduced by implementing parallel platform/GPU acceleration in a system. Weiwei Chen et al.[25] has proposed new ensemble clustering(NEC) technique that perform on NSL-KDD 2009 to detect novel anomalies and the detection rate is high and lowers the false positive rate. As the model shows greater robustness, high rate of detection and low false positive rate and is suitable for real system. Weiwei Chen et al.[26] A novel anomaly detection can be efficiently detected using clustering and KDD. High rate of detection and less rate of false positive is produced by unsupervised anomaly.

It's an appropriate way to detect anomaly and solve problem, which does not require labeled dataset. The model uses NSLKDD 2009 dataset. In preprocessing all features are transformed into real numbers and datasets are normalized at the evaluation end component and compare the predicted result to the accurate result.

Manoj et al.[27] confirmed that the proposed method uses the advanced way for intrusion detection is to use machine learning ranking and Voronoi clustering to improve security by identifying and attacker tracking. It ensures the reduced size of dataset and high accuracy in detection. ISOT dataset used for processing this machine learning model and it has a delay in large scale network of UDP and TCP. To help the system delay,a DNA based botnet technique developed under deep neural network. The botnet intrusion detection is done using the network characteristics in spite of payload packet content (helps to encrypt packets.

Panagiotis I et al.[28] Android operating system uses Artificial Neural Network to detect the flow based anomaly behavior of android mobile devices. The rate of accuracy and detection reaches 85% and 81% respectively. To address public attacks, the CPU, memory, battery power endeavors the light weight, efficient scalable IDS for android environment. Machine learning algorithm analyses data streams of this model. The rate of accuracy and detection improvement is considered as future scope.

Table 1

Article No	Technique Used/ Proposed Methodology	Dataset used	Purpose of the work	Advantages	Future Scope/ Limitation
17	WFEU-FFDNN (Wrapper Based Feature-Extraction Unit (WFEU)-FeedForward Deep Neural Network – (FFDNN)	UNSW-NB15 and AWID datasets	Designed Intrusion detection system for traffic of wireless network coupled with a technique wrapper based feature extraction and generated a reduced feature vector.	Detection accuracy is high than other approaches.	The individual class detection rate of UNSW-NB15 and AWID performs better after the application of wrapper based feature extraction method.
18	wrapperbased approach using modified whaleoptimization algorithm (WOA)	CICIDS 2017 and ADFA- LD standard datasets	The method detects intrusions accurately by selecting the network data informative feature and has better detection rate.	The detection rate is better than WOA and other evolutionary algorithms. The accuracy is good in the wireless mesh topology network.	The work further optimized by modifying the filter based WOA feature selection method (information gain).
19	Hybrid Deep Learning Model with Deep CNN(deep CNN–WDLSTM IDS)	UNSW-NB15	The hybrid deep learning model with deep CNN(deep CNN–WDLSTM IDS) to evaluate the intrusion detection dataset. Dataset used are UNSW-NB15 and a comparison is made with ISCX2012 dataset.	To avoid the problem of over fitting; a technique of drop connect with hidden to hidden weight matrices used with LSTM and use LSTM to avoid gradient vanishing problem by retaining the extracted features of long term dependencies.	The real time intrusion detection system can be obtained by further analyzing the complex and bigger datasets.
20	Deep Neural Network (DNN)	KDDCup 99 dataset	Scale-Hybrid-IDS-AlertNet (SHIA) used to monitor network traffic effectively and proactively uses host level events to alert the cyber-attacks.	Detect and classify unforeseen and unpredictable cyber-attacks.	The performance of deep neural network architecture can be improved through advanced hardware distributed approach.
21	Feed-forwardNeural Networks model(FNN)-for classification of binary and multi-class.	BoT-IoT dataset	A model that differentiate high accuracy in traffic of normal and malicious node and achieves low false positive and false negative predictions.	High Classification Accuracy- The DDoS/DoS and reconnaissance attack binary classification capability demonstrated the result close to 0.99 against the evaluation criteria like accuracy,F1score, recall and precision	Further improved by developing the classifier for the attack of each subcategory and includes the timestamp into as a new feature and develops a new model of deep neural network. Time series data can be modeled using long short term memory network.

22	Deep Belief Network-Deep Learning algorithm.	Anomaly dataset	The algorithm performs intelligent intrusion detection on anomaly dataset and scrutinizes the active malicious activity in the network and creates a diversion/breaching on it.	It creates a secure way to drive the network in the uncertain situation and improves the rate of detection and accuracy.	Improves the rate of detection and accuracy. More anomaly datasets are trained for promising outcomes of Deep Belief network.
23	Deep Auto-Encoder based Intrusion Detection System (DAE-IDS)	KDD-CUP'99 dataset	Trained a model to avoid the problem of over fitting and local optima and handled the Deep-Auto-Encoder based-Intrusion Detection System-(DAE-IDS) model in greedy layer fashion.	The input classified into normal /attack using soft-max layer after training four autoencoders.	Further work can be explored on autoencoder, how sparse to design the constraints of deep autoencoder and how to improve the effectiveness of intrusion detection.
24	SAE-SVM (Pre-learned-sparse-autoencoder with SVM)	NSL-KDD Dataset	Developed intrusion detection network model for binary and multiclass data for predicting accurately the intrusion of network using Pre-learned-sparse autoencoder with SVM-(SAE-SVM).	The NSL KDD dataset used 5 category classification and shows high accuracy rate.	Further, the improvement for good feature representation and dimensionality reduction using STL multiple stages and hybrid feature learning model. The training and testing times of model can be reduced by implementing parallel platform/GPU acceleration in a system.
25	New-Ensemble-Clustering(NEC)	NSL-KDD 2009	To detect novel anomalies and the detection rate is high and lowers the false positive rate.	NEC model shows high positive rate and low rate of false positive.	The model shows greater robustness, high rate of detection and low false positive rate and is suitable for real system.
26	Clustering and KDD.	NSL-KDD 2009	Novel anomaly detection (NEC) can be efficiently detected using clustering and KDD.	An appropriate way to detect anomaly and solve problem, which does not require labeled dataset.	High rate of false positive and high detection rate.
27	Machine Learning, Ranking, Voronos clustering.	ISOTdataset	The method uses the advanced way for intrusion detection is to use machine learning ranking and Voronoi clustering to improve security by identifying and attacker tracking. ISOT dataset used for processing this machine learning model and it has a delay in large scale network of UDP and TCP.	It ensures the reduced size of dataset and high accuracy in detection.	To help the system delay,a DNA based botnet technique developed under deep neural network. The botnet intrusion detection is done using the network characteristics in spite of payload packet content (helps to encrypt packets).
28	Artificial Neural Network (ANN)-IDS.	Android Operating system	Android operating system uses Artificial Neural Network to detect the flow based anomaly behavior of android mobile devices.	The rate of accuracy and detection reaches 85% and 81% respectively.	To address public attacks, the CPU, memory, battery power endeavors the light weight, efficient scalable IDS for android environment. Machine learning algorithm analyses data streams of this model. The rate of accuracy and detection improvement is considered as future scope.

V.CONCLUSION AND FUTURE SCOPE:

An effective design of intrusion detection system-IDSs has attractions in lot and there's a huge increase in various types of attacks and network traffic. To secure a network, there are many protocols, software and algorithms; even then, the system appears vulnerable to the cyber-attacks. From the survey it is observed that to improve the detection and accuracy rates of the IDS, a classifier can be developed for differentiating the attack types in detail and the timestamp information can be added as a new feature. A self-taught learning (STL) based IDS can be used for learning the features and dimensionality reduction. The training and testing period can be reduced considerably and efficiently increases the detection and rate of accuracy of the deep learning approach with respect to attacks. A method has to be proposed to select the most informative features from the network data and thereby improves the detection and accuracy of the model. In future, the optimization of other parameters of the deep network can be considered for dimensionality reduction.

REFERENCES

1. B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ``Network intrusion detection," IEEE Netw., vol. 8, no. 3, pp. 26_41, May 1994.
2. K. Scarfone, P. Mell, P. Mell, Guide to intrusion detection and prevention systems (IDPS), NIST special publication, (2007).
3. A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne,"Evaluating Computer Intrusion Detection Systems:A Survey of Common Practices," Acm Comput. Surv., vol. 48, no. 1, pp. 1–41, 2015
4. F. A. Khan, A. Gumaei, A Comparative Study of Machine Learning Classifiers for Network Intrusion Detection, In International Conference on Artificial Intelligence and Security, pp. 75-86. Springer, Cham, 2019.
5. S. Pouyanfar et al., "A Survey on Deep Learning: Algorithms, Techniques, and Applications," ACM Comput. Surv., vol. 51, no. 5, p. 92, 2018.
6. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning. nature 521 (7553): 436," Google Sch., 2015.
7. Lazarevic, Aleksander, Yipin Kumar and Jaideep Srivastava, "Intrusion Detection: A Survey", managing cyber Threats, Springer US, 2005, pp 19-78, 2005.
8. G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," in Digital Forensic and Security (ISDFS), 2018 6th International Symposium on. IEEE,2018, pp. 1–6.
9. G. Karatas¸, "Genetic algorithm for intrusion detection system," in Signal Processing and Communication Application Conference (SIU), 2016 24th. IEEE, 2016, pp. 1341–1344.
10. O. Can and O. K. Sahingoz, "An intrusion detection system based on neural network," in 2015 23nd Signal Processing and Communications Applications Conference (SIU), May 2015, pp. 2302–2305.
11. R. G. Smith and J. Eckroth, "Building AI Applications: Yesterday, Today, and Tomorrow," Ai Mag., vol. 38, no. 1, pp. 6–22, 2017.
12. P. Louridas and C. Ebert, "Machine Learning," IEEE Softw., vol. 33, no. 5, pp. 110–115, 2016.
13. M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," Science, vol. 349, no. 6245, pp. 255–260, 2015.
14. L. Deng and D. Yu, "Deep learning: methods and applications," Found. Trends® Signal Process., vol. 7, no. 3, pp. 197–387, 2014.
15. Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.
16. I. M. Coelho, V. N. Coelho, E. J. D. S. Luz, L. S. Ochi, F. G. Guimarães, and E. Rios, "A GPU deep learning metaheuristic based model for time series forecasting," Appl. Energy, vol. 201, no. 1, pp. 412–418, 2017.
17. Sydney Mambwe Kasongo, Yanxia Sun, A Deep Learning Method With Wrapper Based Feature Extraction For Wireless Intrusion Detection System, Computers & Security (2020), doi: https://doi.org/10.1016/j.cose.2020.101752
18. R. Vijayanand and D. Devaraj, "A Novel Feature Selection Method Using Whale Optimization Algorithm and Genetic Operators for Intrusion Detection System in Wireless Mesh Network," in *IEEE Access*, vol. 8, pp. 56847-56854, 2020
19. Mohammad Mehedi Hassan , Abdu Gumaei , Ahmed Alsanad , Majed Alrubaian , Giancarlo Fortino , A Hybrid Deep Learning Model for Efficient Intrusion Detection in Big Data Environment, Information Sciences(2019)
20. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in *IEEE Access*, vol. 7, pp. 41525-41550, 2019.
21. Mengmeng Ge, Xiping Fu, Naeem Syed, Zubair Baig, Gideon Teo, Antonio Robles-Kelly, "Deep Learning-based Intrusion Detection for IoT Networks", *2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, Kyoto, Japan, 2019, pp. 256-25609.
22. Nagaraj Balakrishnan, Arunkumar Rajendran, Danilo Pelusi, Vijayakumar Ponnusamy, "Deep Belief Network enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things, Internet of Things (2019), doi: https://doi.org/10.1016/j.iot.2019.100112
23. F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 178-183.
24. M. Al-Qatf, Y. Lasheng, M. Al-Habib and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," in *IEEE Access*, vol. 6, pp. 52843-52856, 2018.
25. W. Chen, F. Kong, F. Mei, G. Yuan and B. Li, "A Novel Unsupervised Anomaly Detection Approach for Intrusion Detection System," 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 69-73
26. Weiwei Chen, Fangang Kong, Feng Mei, GuiginYuan, Bo Li, "a novel unsupervised Anamoly detection Approach for Intrusion Detection System", 2017 IEEE 3rd International Conference on big data security on cloud, May 16-18,2017, Zhejiang, China.
27. Manoj s. Koli, Manik K. Chavan, "An Advanced method for detection of botnet traffic using Internal Intrusion Detection", 2017 International Conference on (ICICCT), March 10-11, 2017, Sangli, India.
28. Panagiotis I. Radogloa-Grammatikis; Panagiotis G. Sarigannidis, "Flow anamoly based Intrusion Detection System for Android Mobile Devices", 2017 6th International Conference on MOCAST, May 4-6, 2017, Kazani, Greece.

AUTHORS PROFILE

S. Kavitha received her B.Tech-Information Technology and M.E Computer Science and Engineering from Anna University, Chennai,India in 2010 and 2012. She is pursuing her Ph.D. in Information and Communication Engineering, Anna University, Chennai. Currently, she is working as an Assistant Professor in the Department of Computer Science and Engineering at Velammal College of Engineering and Technology, Madurai, India. She has 8 years of teaching experience. She has published various papers in International and National conference and journal.

Dr. N. Uma Maheswari received her M.E in Computer Science and Engineering from the Madras University, Chennai, India in 2002 and Ph.D. in Information and Communication Engineering in 2011 from Anna University, Chennai. Currently, she is working as a Professor in the Department of Computer Science and Engineering at the P.S.N.A. College of Engineering and Technology, Dindigul, India. She has totally 16 years of teaching experience which includes 12 years of research experience. Her research interests include Biometrics, Image processing, Compiler design, Artificial Intelligence, Speech Processing, and Wireless Sensor Networks. She has published 50 papers in International journals, 2 papers in National journals, and presented 30 papers at International conferences, and 20 papers at National conferences. She has co-authored a book entitled ''Compiler Design'' and " Theory of Computation" published by Yes Dee Publishing. She is a recognized Ph.D. supervisor in Anna University of Technology in the area of Image processing, Cloud computing, Network security and Networks. Acted as a reviewer for various referred journals, acted as a Coordinator for various seminars, conferences etc.

Dr. R. Venkatesh received his M.E in Computer Science and Engineering from Anna University Chennai in India, in 2007 and Ph.D. Computer Science and Engineering in 2010 at Alagappa University, Karaikudi. Currently, he is working as a Professor in the Department of Information Technology in PSNA College of Engineering and Technology, Dindigul, India. He has totally twenty five years of teaching experience which includes 15 years of research experience. He has published 60 papers in International journals, 2 papers in National journals, and presented 32 papers at International conferences and 10 papers at National conferences. His research interests include Networks , Network security ,Biometrics, Artificial intelligence, Compiler design, Neural Networks and Soft computing. He has co-authored a book entitled ‘‘Compiler Design’’ published by Yes Dee Publishing and Object Oriented Programming published by notion press. He has also co-authored a book chapter published by Advances in Computer Science.