IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 36, No. 4, August, 2022, pp. 641-646
Journal homepage: http://iieta.org/journals/ria

A Comprehensive Analysis on Numerous Learning Models for Intrusion Detection for Security Conservation

Kurra Santhi Sri[1*], Bhargavi Peddireddy[2], Venkata Bhujanga Rao Madamanchi[3], Gottumukkala Hima Bindu[4]

[1] Department of Information Technology, Vignan's Foundation for Science Technology & Research, Guntur 522017, Andhrapradesh, India
[2] Department of Artificial Intelligence, Vidya Jyothi Institute of technology, Aziznagar Gate, Chilkur Balaji Road, Himayat Sagar Rd, Hyderabad, Telangana 500075, India
[3] Department of Information Technology, RVR & JC College of Engineering, Chowdavaram, Andhra Pradesh 522019, India
[4] Department of CSE, School of Technology, GITAM (Deemed to be University), Hyderabad 502329, Telangana, India

Corresponding Author Email: srisanthi@gmail.com

https://doi.org/10.18280/ria.360418

Received: 12 April 2022
Accepted: 12 August 2022

Keywords:
learning models, analysis, security models, intrusion detection, trust, privacy, attacker

ABSTRACT

The term intrusion refers to a series of behaviours that exposes computer networks and systems' security to compromises. Corrective action on the network cannot go on without intrusion detection. IDS and IDS is the framework used to detect network traffic intrusions, which is how the network control mechanism identifies potential intrusions. Security breaches are designed to undermine one or more of the network's three primary security goals: privacy, availability, and trust. To get access to a system, an attacker must follow a predetermined set of procedures. Once inside, they can begin gathering data such as the protocol being used and the network resources available. There are many ways for a hacker to find out what systems are available on the network and how vulnerable they are to attacks. The rapid advancement of network technology necessitated IDS to focus on the detection of assaults using contextual analysis from signature matching processes. Using machine learning to detect and prevent intrusions, the IDS is a critical part of protecting data systems. Network intrusion detection is the focus of this paper, which examines and shows various machine learning techniques.

1. INTRODUCTION

The Intrusion Detection System (IDS) [1] keeps a close eye on the system network for suspicious activity and policy violations. Malicious activity reported to the administrator or the central database is tracked by the Security Information Management (SIM) system [2]. A prevention-based approach, such as authentication and access control, will continue to be used alongside the IDS. As an additional layer of security, it is being added to enhance the framework's existing security monitoring and control measures. The IDS tracks the data passively and detects possible attack links [3]. Technically, the IDS aims at three fundamental security objectives, namely data monitoring, detection of any transactions that are potentially dangerous and ultimately reacts to suspect activity. With the enormous framework of the Internet, its presence and the absence of a central defence system, attack prevention is not possible and attacks should therefore be identified and recovered. Intrusion can be described in simple terms as an assault on any or all of the security features of the system, i.e. confidentiality, availability and integrity [4].

Machine learning is one of the best IDS approaches for detecting assaults. Machine learning deals with improvements in algorithms that enable the independent integration of information through computer systems so that their output is constantly improved to execute their tasks efficiently [5]. Using machine learning technology to detect new assaults in the last several years, high precision rates are attained. A security system for the detection of different threats is the intrusion detection system. These are a number of strategies used in the identification of suspicious behaviour in the network level. The Intrusion Detection Model is depicted in Figure 1.

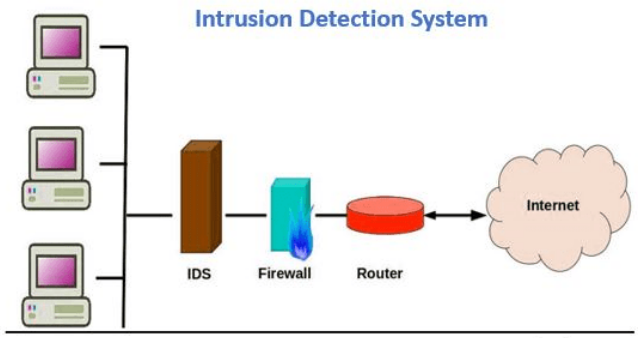

Figure 1. IDS architecture

Monitoring the system or network for policy violations or suspicious activity, an intrusion detection system (IDS) produces reports to the management system. An intrusion attempt can be prevented by a number of systems, but a monitoring system is under no obligation to do so. IDS and IPS are primarily designed to discover and log possible incidents, as well as to report efforts to do so. Organizations

also utilise IDPS to discover security policy issues, prevent employees from violating policies, and document current threats to security policies. Nearly every business now relies on IDPS as part of its overall security strategy. Intrusion detection can be accomplished using a variety of techniques, each with its own set of advantages and disadvantages [6].

There are two distinct types of IDS methods. Anomaly detection and signature-based identification are two of the methods. In order to distinguish attacks that take the form of signatures or patterns, misuse detection is employed [7]. The main drawback of using a proven pattern to detect attacks is that it is unable to recognise any unknown attacks on the network or device that it has not been trained with. To distinguish between legitimate and suspicious attacks, intrusion detection is employed [8]. Anomalies can be discovered in a variety of methods. Several machine learning approaches are used to look for anomalies. A review of significant works on intrusion detection systems was conducted in this paper.

2. LITERATURE SURVEY

Salih et al. [1] proposed a model that uses NSL-KDD dataset for performing analysis on the data records. Issues in the intrusion detection models are analysed and a adaptive ensemble learning model is proposed. In the proposed work, multiple base classifiers are introduced to enhance the overall detection effect. The efficiency of the data characteristics is examined for improved results in order to identify detection impacts. The proposed model only includes balanced data for identifying network intrusions, but the accuracy rate can be improved on imbalanced data considerations. Regardless of weight, the model proposed takes account of features. The allocation of weights for the features and consideration of relevant features enhances the level of safety through correct intrusion identification. Ensuring the advantages of several algorithms is the core principle of the model. To improve the detection effect, an ensemble learning method is applied. Compared to other research papers, the proposed ensemble model effectively increases the precision of detection.

El Boujnouni et al. [3] proposed a model that uses a group of 6 machine learning techniques (Decision Tree, Random Forest, K Nearest Neighbor, Adaboost, Gradient Boosting, and Linear Discriminant Analysis) are implemented with a updated dataset (CSE-CIC-IDS2018). Unbalanced data for intrusive detection is considered in the suggested model. The complexity of the model is significant since all features for intrusion detection are taken into account. The studied the efficacy of profoundly trained algorithms for sample assault detection in datasets. Deep learning models can therefore be utilised in future projects. The reliability of the device should improve with the use of a fresh design approach.

Machine learning has been employed in the previous decades to improve intrusion detection, and an up-to-date, detailed taxonomy and survey of latest work is currently required. Many related studies have been conducted utilising both the KDD-Cup 99 and DARPA 1999 datasets for validating IDS development, but the question is to which data mining approaches are more effective is not obvious. It is not obvious. Secondly, although the time required for the construction of IDS is a key element for 'on-line' IDSs, the evaluation of certain IDSs methodologies is not examined.

Bhosale et al. [4] discussed a model in which most of the model interpretation work focuses on other areas, such as machine vision, processing of natural languages. It adds to the assumption that cybersecurity specialists can hardly refine their options according to the decisions of the model of realistic usage. In order to resolve these problems, a structure is suggested to provide an interpretation for IDSs. using SHapley Additive exPlanations (SHAP). The proposed model is applied with only a single dataset with less records. The false positive rate of the proposed model is high which gives less accuracy. The model considers neighbour system data for intrusion detection which increases delay. There are comparisons between the interpretation between two different classifying agents, one vs-all and multi-class. To test the frame feasibility, the NSL-KDD data set is used. The proposed framework improves the clearness of any IDS and allows cyber security staff to better understand the judgments of IDSs.

Intrusion detection systems for signature based intruder detection (SIDS) are designed to match patterns in order to locate an attack known as the detection of knowledge or mismanagement. Mating strategies for finding a previous intrusion are employed in SIDS [5]. In other words, an alarm signal is triggered when an intrusion signature matches the previous intrusion signature already in the signature database. The host logs for SIDS are checked to see sequences of previously recognised malware commands or actions.

Some scientists have used the Bayesian method to solve the problem of intrusion detection. The principal notion underlying this technique is the Bayesian methodology's distinctive property. For a certain outcome, Bayesian technique can retreat in time and discover the source of the events by utilising probability estimates. This feature is appropriate to determine why the network behaviour has had a particular anomaly. The system can somehow go back in time and discover the reason of the occurrences via Bayesian algorithm.

Wang et al. [6] proposed a model that concentrates on using deep learning methods using optimization technique to study the lower level characteristic to the higher level definition. In this paper, the Network Intrusion Detection System (NIDS) was proposed for improved Genetic Algorithm (GA-IFS) technology. In order to easily distinguish normal and inadequate network traffic, GA-IFS tracks and analyses simulated network behaviour using a DARPA KDD Cup 99 dataset. GA is a search heuristic ideal for large population issues, but has a time limit for convergence, often resulting in optimum locality, if there is no population diversity. The Genetic Algorithm (GA) helps to learn functions that translate from input to output due to the abstraction of several layers for extraction of features. The learning model should not depend on attributes that are man-made. DBN uses the Restricted Boltzmann Machine (RBM) for each sheet that is an unregulated learning algorithm. The proposed model identifiers intrusions in the network and the time for identification is more. The delay in the network is very high that degrades the system performance. The data review procedure is not taken into account in the model proposed. The GA fitness value is calculated by the system trust weights. This technique is much like how the problem of uncertainty in the expert systems is handled. The guidelines for regular and aberrant conduct have later been compared in their models.

Pham et al. [8] discussed on Auto Encoder (AE) and its variants for selection of features. The main goal of the model is to analyse and summarise the working model of in-depth learning used with machine security monitoring for identification of intrusions in the system.

Important trainings of data features can decline IDS performance and level of accuracy. The results show that selection of features will substantially increase IDS' efficiency even if it improves the inaccuracy of the function [9]. The analysis of selecting features on the NSL-KDD dataset is performed that does not consider attacks of multiple types [10]. Features are selected for identification of attacks of only one type in the network [11]. All kinds of attacks in the network is not detected in this model.

Desale et al. [12] explored and described the mechanism that emerged from their artificial neural network Feed-Forward neural algorithm + Probabilistic Algorithm + Particle Swarm are used to train a neural model. The numerous IDS techniques designed for the model are all used to reduce model overhead and thus the entire system cost. the standard NSL-KDD dataset works well with other intrusion models, but there is still some room for improvement with the RB and OPSN model. This model is like PSO, PSR, and NSL. It has a higher detection and specificity. In comparison, the PSO-PNN is more sophisticated. Its identifying rate is higher, and the error rate is lower than average. It should be noted that only the binary classification was completed in this study. The optimizer utilised for the optimization of particulate swarm method is concepted to be similar to the crossover operation of the genetic algorithms, while making adjustments to "local" and "global" best particles. In addition, fitness function includes particle swarm optimisation, which quantifies the closeness of the appropriate solution to the optimum. The fundamental distinction from the evolutionary computing notion of particle swarm optimization is that flying potential solutions across hyper-space accelerate towards "better" solutions, but in evolutionary calculation systems, potential solutions are directly represented as physical locations.

Zhang et al. [13] took inspiration from the Extreme Learning Machine (ELM) in creating their new intrusion detection system, which draws on findings from the DBN algorithm. a facial recognition algorithm, pedestrian identification, and cyber intrusion experiments were conducted using the ELM algorithm Using the ELM algorithm, the author distinguished machine learning with the Deep Belief Network (DBN) to classify each of these algorithms on the NSL dataset. the training set of the two algorithms on the NSL-K dataset consists of four lakh documents and the testing set of the remaining two lakhs are shared documents It is deduced that the ELM algorithm is more accurate, since it closely compares various correct, stable, and aesthetically-similar models.

The usage of the Naive Bayesian classifier is one of the most interesting elements of this research. Dirichlet distribution is used in the description of the classifier to obtain the probability density function [14]. A decent choice for this kind of problem is the Dirichlet distribution. Time is associated with the distribution of Dirichlet and Gamma.

Algorithms presented by Dong et al. [15] outlined Smart Grid IDS data mining algorithms have been presented here. Algorithms are calculated on the basis of several different parameters, including the likelihood of discovery, the possibility of error, the processing time, and the length of the result the latest research finds that Random Forest significantly outperforms other classifies to detect attacks with higher sensitivity and lower false-positive rate. These four IDS classifiers were experimentally analysed using the Random Forest, SVM, Bayesian Network, Naïve Bayes, and other techniques: Many measurements were used, including the likelihood of identification, the efficacy of treatment, and the likelihood of false alarm. In this study, some algorithms demonstrated high accuracy but required much time, while others were more precise but fast.

Zhao et al. [16] created a comprehensive survey of all existing intrusion detection systems in order to aid end users to better comprehend the device. The network is expanding worldwide and growing increasingly every day. The model includes a combination of static, dynamic and control techniques for signatures.

If the effort to mitigate device interference is to be minimised [17], we have recommended the use of network content based computer training to differentiate between non-harmful and malicious data and behaviour [18]. This is done with many methods of machine learning like algorithms. The data utilised in this simulation is the UNSW-NB dataset [19]. Modern machine learning techniques allow high-lower false-positive network intrusion detection systems as well as well as greater-precision systems for pattern recognition.

Alrawashdeh et al. [18] proposed a hybrid detection method that employs Classification and Boosting algorithms. The process uses three different classifiers to fine-tune performance. On review, the Random Tree comes out with an average accuracy of 99.98%, an average false-positive rate of 0.21%, and a 0.78% misidentification rate. Random is one of the strongest combinations of 98.7% and above. Millions of computer users around the world do diverse things with their systems. It has become ever more important to provide strong protection in networks. using all intrusion detection systems and computers One of the principal functions of intrusion detection techniques is to help the organisation reduce the fear of future intrusions. Delays in model training increase as the time required to process data for intrusion detection data grows.

A series of machine learning studies analysed by Cordero et al. [20] includes a comprehensive review of several other studies. Authoring included a simple flowchart for processing anomalies based on similar studies. A core part of security-monitoring mechanism is an intrusion detection strategy. Many aspects of the defence have been improved with the advent of computer technology. Innovative protection mechanisms use machine learning to discover even unknown intruders. In this paper, anomaly-based intrusion detection is done with the NSL KDD project database. He used a common methodology to explain and define the study process. Simplifying the procedures in the early stages of the generic phase should be primary; new researchers should focus on increasing the early detection rate. Since pre-processing impacts classification, it's important to perform it first. Using an ANN for pre-derived characteristics will reveal the highest detection speeds.

Tang et al. [21] performed a multi-machine learning study on the issue of irregular problems. Several machine learning mining methods in the study were applied, as well. Two or more standards that are appropriate to the application of a detection model which, but don't always, seriously impact the measurement of the structure. Although there have been numerous subsets developed since the DARPA subsets, the

latest subsets, such as DAR8, ISC15, and KDD12, have improved greatly. This article undertakes a comprehensive survey of the available databases, summarising the requirements and results from IDSs. IDS was the most instrumental in the development and evolution of the framework in which several attacks are simultaneously interrupted. A lot of machine learning algorithms have been created on creative and novel techniques. Even though all types of crime can be detected, however, detection is not 100% accurate. The speed of detection is another key problem in this field of research. In order to constantly change information and data, computer networks are dynamic. Consequently, the system must operate in real time if an incursion is detected precisely and quickly. Real-time operations are not only intended for real-time detection, but to react to new network dynamics. IDS is a current area of research analysed by numerous scientists in real time. The main research projects are designed to introduce approaches that are the most time efficient. The objective is to ensure that the implemented methods can be used in real time.

Mane et al. [22] suggested three separate approaches. the first, gaining information Furthermore, the Gain Ratio. More importantly, range correlation. To begin, these methods are employed, followed by the highest ranking features. Of the 41 possible features, only six were considered interesting enough to implement. Ten processes of cross-validation were used to analyse the accuracy of the model applied to the KDD results. The identification of numerous plays an important part in an intrusion detection system. When you have several features in the traffic dataset, the task of deciding which features are most important and which are not will lead to an improvement in the classifier's accuracy.

Kumar et al. [23] used regulated and unsupervised approaches are considered. Using this approach, the author first selected and weighed features and then applied a feature-by-value analysis to them. The weights of the K-Means classifier are then used to give the classifier its overall distribution. Using the K-Means to select the closest and farthest neighbours ensures that the classification is less reliant on the K scale, which minimises bias. Experimental KDD data shows that the proposed solution detects DoS, Probe, R2L, and overflow and denial of service attacks while greatly improve its ability to discover U2R attacks.

Clustering, which is based on distance measurements on objects and on the classification into clusters of items. Classification is a non-conscious learning process because there is no information on the label of learning data. Euclidean distance may be defined as the square root of the entire difference between the same vector size [24]. Finally, methods of grouping and classification must be efficiently channelled, and the dimensions of network data and heterogeneity must be handled massively [25]. One of the widely recognised clustering tools is the K-means algorithm. K-means the data to be grouped into a user given number of different K clusters according to their characteristic values. Data classified into the same cluster have the same values. K, the number of cluster must be indicated in advance by a positive entirely

Sajana et al. [25] developed a new IDS to extract network parameters from network traffic data and a new feature description of attacks to classify attacks. Another use of machine learning and data mining techniques is to detect anomalies in the network, which can reveal possible attacks. It was proposed as a new way of identifying vulnerabilities that addressed concerns about intrusion detection using an approach based on anomalies. Symbolic network attributes are converted to numeric, and normality is used to deduce additional information is included.

3. PROPOSED METHODOLOGIES

The purpose of the IDS is to identify the intrusions in the system or the computer network by analysing the actions of the user in relation to their intended usage [26]. It includes fraud, accessing data on the network, trying to prevent the system from working properly or actually crashing the software. On the basis of the shortcomings found in the survey, there is a strong need to propose an IDS model that uses machine learning techniques as a whole and reinforces the neural learning network. In order to enhance detection accuracy, the necessary IDS model needs to integrate individual basic classification and Machine Learning paradigms to minimise computational complexity using the Ensemble Approach and Enhancing the Neural Learning Network. The model needed is to set up a network and choose the shortest fixed route for data communication and to set up a clustering model that selects a group head in the network to track a device activities during data transmission and to identify attacks and detect a wide range of network attacks during data communication. The model to be developed must reduce the number of false IDS alerts to increase the accuracy of attack detection and avoid network intrusions on the basis of trained data to function efficiently in real time.

4. CONCLUSIONS

NIDS is the most commonly used protection model in the area of network security. With the rapid growth of the network, network protection has become one of the most critical issues, as it directly affects the interests of the public organizations, companies and individuals. Furthermore, with the increasing awareness of attacks, dynamic and varied attack tools and techniques, the latest simple firewall technology has not been able to meet people's needs. Intrusion detection and prevention technologies are bound to become one of the primary technologies for security auditing. In computer network protection, NIDS is a type of intrusion detection system that aims to detect unauthorised access to a network by analysing network traffic for malicious behaviour. Many methods for the intrusion detection method have been introduced in recent years. This paper provides a brief survey on various models for detecting intrusions.

REFERENCES

[1] Salih, A.A., Abdulrazaq, M.B. (2019). Combining best features selection using three classifiers in intrusion detection system. In 2019 International Conference on Advanced Science and Engineering (ICOASE), Zakho - Duhok, Iraq, pp. 94-99.https://doi.org/10.1109/icoase.2019.8723671

[2] Wang, H., Han, B., Su, J., Wang, X. (2018). A high-performance intrusion detection method based on combining supervised and unsupervised learning. In

2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, pp. 1803-1810.https://doi.org/10.1109/smartworld.2018.00304

[3] El Boujnouni, M., Jedra, M. (2018). New intrusion detection system based on support vector domain description with information gain metric. International Journal of Network Security, 20(1): 25-34.

[4] Bhosale, K.S., Nenova, M., Iliev, G. (2018). Data mining based advanced algorithm for intrusion detections in communication networks. In 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), Belgaum, India, pp. 297-300. https://doi.org/10.1109/ctems.2018.8769173

[5] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Systems with Applications, 39(1): 424-430. https://doi.org/10.1016/j.eswa.2011.07.032

[6] Wang, Z. (2018). Deep learning-based intrusion detection with adversaries. IEEE Access, 6: 38367-38384.https://doi.org/10.1109/ACCESS.2018.2854599

[7] Ahmad, I., Basheri, M., Iqbal, M.J., Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE access, 6: 33789-33795.https://doi.org/10.1109/access.2018.2841987

[8] Pham, N.T., Foo, E., Suriadi, S., Jeffrey, H., Lahza, H. F.M. (2018). Improving performance of intrusion detection system using ensemble methods and feature selection. In Proceedings of the Australasian Computer Science Week Multiconference, pp. 1-6.https://doi.org/10.1145/3167918.3167951

[9] Kumari, U., Soni, U. (2017). A review of intrusion detection using anomaly based detection. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 824-826.https://doi.org/10.1109/cesys.2017.8321199

[10] Lee, H., Kim, Y., Kim, C.O. (2016). A deep learning model for robust wafer fault monitoring with sensor measurement noise. IEEE Transactions on Semiconductor Manufacturing, 30(1): 23-31.https://doi.org/10.1109/tsm.2016.2628865

[11] Ozgur, A., Erdem, H., Nar, F. (2016). Sparsity-driven weighted ensemble classifier. arXiv preprint arXiv:1610.00270. https://arxiv.org/abs/1610.00270

[12] Desale, K.S., Kumathekar, C.N., Chavan, A.P. (2015). Efficient intrusion detection system using stream data mining classification technique. In 2015 International Conference on Computing Communication Control and Automation, pp. 469-473. https://doi.org/10.1109/iccubea.2015.98

[13] Zhang, J., Zulkernine, M., Haque, A. (2008). Random-forests-based network intrusion detection systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 38(5): 649-659.https://doi.org/10.1109/tsmcc.2008.923876

[14] Javaid, A., Niyaz, Q., Sun, W., Alam, M. (2016). A deep learning approach for network intrusion detection system. Eai Endorsed Transactions on Security and Safety, 3(9): e2. https://eprints.eudl.eu/id/eprint/2057.

[15] Dong, B., Wang, X. (2016). Comparison deep learning method to traditional methods using for network intrusion detection. In 2016 8th IEEE international conference on communication software and networks (ICCSN), Beijing, China, pp. 581-585.https://doi.org/10.1109/ICCSN.2016.7586590

[16] Zhao, R., Yan, R., Chen, Z., Mao, K., Wang, P., Gao, R. X. (2019). Deep learning and its applications to machine health monitoring. Mechanical Systems and Signal Processing, 115: 213-237. http://arxiv.org/abs/1612.07640

[17] You, L., Li, Y., Wang, Y., Zhang, J., Yang, Y. (2016). A deep learning-based RNNs model for automatic security audit of short messages. In 2016 16th International Symposium on Communications and Information Technologies (ISCIT), Qingdao, China, Anaheim, CA, USA, pp. 225-229.https://doi.org/10.1109/iscit.2016.7751626

[18] Alrawashdeh, K., Purdy, C. (2016). Toward an online anomaly intrusion detection system based on deep learning. In 2016 15th IEEE international conference on machine learning and applications (ICMLA), pp. 195-200.https://doi.org/10.1109/icmla.2016.0040

[19] Potluri, S., Diedrich, C. (2016). Accelerated deep neural networks for enhanced intrusion detection system. In 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, pp. 1-8. https://doi.org/10.1109/etfa.2016.7733515

[20] Cordero, C.G., Hauke, S., Mühlhäuser, M., Fischer, M. (2016). Analyzing flow-based anomaly intrusion detection using replicator neural networks. In 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, pp. 317-324.https://doi.org/10.1109/pst.2016.7906980

[21] Tang, T.A., Mhamdi, L., McLernon, D., Zaidi, S.A.R., Ghogho, M. (2016). Deep learning approach for network intrusion detection in software defined networking. In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, pp. 258-263.https://doi.org/10.1109/wincom.2016.7777224

[22] Mane, P.M., Rani, C.S. (2019). High data availability with effective data integrity and user revocation using ABE scheme for cloud storage. International Journal of Innovative Technology and Exploring Engineering, 8(4S2).

[23] Kumar, S.A., Vidyullatha, P. (2019). A comparative analysis of parallel and distributed FSM approaches on large-scale graph data. International Journal of Recent Technology and Engineering. 7: 642-648.

[24] Sai Meghana, S., Amulya, P., Manisha, A., Rajarajeswari, P. (2019). A deep learning approach for brain tumor segmentation using convolution neural network. International Journal of Scientific and Technology Research, 8(12): 1697-1702.

[25] Sajana, T., Krishna, K.S., Dinakar, G., Rajdeep, H. (2019). Classifying diabetic retinopathy using deep learning architecture. International Journal of Innovative Technology and Exploring Engineering, 8(6S4): 1273-1277.

[26] Balaraju, J., Prasada Rao, P.V.R.D. (2019). Innovative secure authentication interface for Hadoop cluster using DNA cryptography: A practical study. In International Conference on Soft Computing and Signal Processing, pp. 17-29. https://doi.org/10.1007/978-981-15-2475-2_3