IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 47-53

Intrusion Detection Algorithm Based on Convolution Neural Network

Asst. Prof. Priti Rumao[1], Asst. Prof. Bhavna Arora[2], Asst. Prof. Nida Parkar[3], Asst. Prof. Samira Nigrel[4]

[1](Department of computer Engineering, Atharva College Of Engineering,India)
[2](Department of computer Engineering, Atharva College Of Engineering,India)
[3](Department of computer Engineering, Atharva College Of Engineering,India)
[4](Department of Information technology, Atharva College Of Engineering,India)

Abstract: *With the quick advancement of system innovation, dynamic safeguarding of the system interruption could really compare to previously. So as to improve the knowledge and precision of system interruption identification and lessen false cautions, another profound neural system (NDNN) show based interruption recognition technique is structured. A NDNN with four concealed layers is demonstrated to catch and group the interruption highlights of the KDD99 and NSL-KDD preparing information. Tests on KDD99 and NSL-KDD dataset demonstrates that the NDNN-based strategy improves the execution of the interruption recognition framework (IDS) and the precision rate can be gotten as high as 99.9%, which is higher when contrasted and different many interruption location strategies. This NDNN model can be connected in IDS to make the framework progressively secure.*

I. Introduction

Interruption recognition is to gather and break down data about the key hubs in a system to discover if there are disregarded security practices or indications of being assaulted. Interruption location framework (IDS) is an autonomous framework giving neighborhood organize administrations to guarantee the security of the system framework. With the quick improvement of system innovation, dynamic shielding of the system interruption could easily compare to previously. Thus, an increasingly wise and exact IDS is expected to address these difficulties.

There are a great deal of explores applying AI techniques in IDS to distinguish arrange interruptions in both scholarly community and industry [1– 9]. Conventional IDS first concentrates and investigations highlights of interruption and assault mode. At that point an interruption design library and a progression of separation rules are worked to identify interruption [10]. A wide range of methodologies have been attempted in investigates. Sujendran and Arunachalam [11] propose a programmed fluffy guideline age joined with a Wiener channel to recognize assaults. Yaseen et al. [2] propose a staggered half breed interruption discovery display that utilizes bolster vector machine (SVM) and outrageous learning machine to assaults. An altered K-implies calculation is likewise used to assemble new little preparing datasets speaking to the whole unique preparing dataset to diminish the preparation time and improve the execution of IDS. Kaur et al. [3] propose hybridisation of K-means and firefly calculation for peculiarity recognition. The calculation utilizes bunching to construct the preparation model and uses arrangement to assess the test set. Their test results demonstrate that K-means + firefly and K-means + bat beat different strategies by a tremendous edge. Tahir et al. [4] think about an assault framework utilizing a cross breed strategy joining K-implies with SVM. In [7], interruption was distinguished utilizing the profound certainty system, and KDD Cup 99 information was utilized to test the calculation. Contrasted and the current SVM show and the ANN display, the accuracy expanded over 6%. Lin et al. [8] propose a group focus and the closest neighbor (CANN) approach and trial results dependent on the KDD99 demonstrate that the CANN classifier not just performs superior to or like k-NN and SVM prepared technique. In [5], a tree-weighted guileless Bayesian calculation is proposed to decrease the element of unmitigated information and improve the order precision of the calculation. In [6], an IDS dependent on data gain rule is utilized to choose highlights from system traffic records and another variant of help vector area depiction is utilized to characterize the extricated highlights and to distinguish new interruptions. It can accomplish great execution in interruption discovery. In [12], infusion kinds of assaults in remote systems are distinguished by melding multi-measurements utilizing the Dempster– Shafer conviction hypothesis. The programmed and self-versatile procedure of fundamental likelihood task is viewed as when joining convictions. They don't require any earlier preparing or alignment. They said multi-layer systems perform more proficiently than other customary techniques.

These techniques, K-implies [3], SVM [2], k-NN [8], grouping [13] and relapse [14] are conventional AI strategies, for the most part rule-based techniques. Contrasted and conventional order strategies, for example, credulous Bayesian, and irregular timberland, the profound neural system (DNN) gets a higher exactness rate and discovery rate with a low false positive rate [15]. Because of the profound system structure, progressively unique highlights of interruptions can be extricated [16] and incredible identification potential is unsurprising.

II. Deep neural systems

As of late, profound learning has been utilized for interruption identification. Ceaseless layers progressively are utilized to do include learning and example order. Its incredible component graphic capacity has pulled in individuals' consideration quickly. Individuals additionally utilize profound learning in interruption location. Some related techniques have been finished up in Table 1. Fiore et al. [17] recommend the appropriation of AI procedures to execute semisupervised oddity discovery frameworks where the classifier is prepared with 'typical' information just, so learning about irregular practices can be developed and advance progressively. They utilize the discriminative confined Boltzmann machine (RBM) to join the expressive intensity of generative models with astounding grouping capacities to gather some portion of its information from deficient preparing information. The exactnesses are around 94%. In [18], MIXMAD is proposed for MIXed information Multilevel Anomaly Detection. They build a troupe of profound conviction nets (DBNs) with changing profundities. The outcomes show that MIXMAD is better than well known unsupervised location strategies for both homogeneous and blended information. Alrawashdeh et al. [19] likewise use RBM, together with DBNs, and they accomplish an identification rate of 97.9% on the complete 10% KDDCUP'99 test dataset. In [20], an interruption discovery strategy utilizing DBNs and probabilistic neural system (PNN) is proposed. The technique incorporates measurement decrease with DBN, molecule swarm advancement and PNN based arrangement. Investigation result demonstrates that the technique performs superior to the customary PNN, PCA-PNN and unoptimised DBN-PNN. Javaid et al. [16] utilize self-educated learning (STL) on NSL-KDD dataset for system interruption and accomplish an order exactness rate higher than 98% for a wide range of characterization.

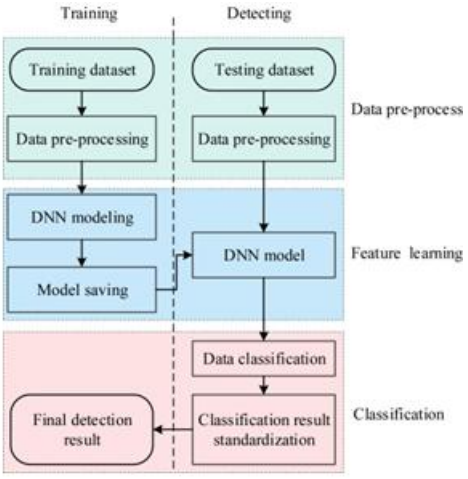

Fig. 1*Proposed IDS structure*

[21], a quickened DNN engineering is created to recognize variations from the norm in system information. NSL-KDD dataset is utilized to register the preparation time and examine the adequacy of the identification system. Roy et al. [22] check the potential ability of DNN as a classifier for various kinds of interruption assaults. Their relative examination demonstrates that DNN works superior to SVM in interruption location. Yin et al. [15] propose a methodology utilizing intermittent neural systems (RNN-IDS). They contrast it and those of J48, a counterfeit neural system, irregular woods, SVM and other AI strategies proposed by past scientists on the benchmark dataset. The exploratory outcomes demonstrate that RNN-IDS is appropriate for displaying an order show with high precision and that its execution is better than that of conventional AI arrangement techniques.

With the improvement of innovation and size of web, an ever increasing number of dangers and conceivable outcomes showed up on web interruptions. To improve the precision of interruption discovery further, another DNN (NDNN) show is assembled and tried in this paper. The IDS can be separated into three modules: information pre-handling, highlight learning module and interruption type arrangement module. The IDS demonstrate is displayed in Fig. 1. The left side demonstrates the preparation procedure and the correct side

demonstrates the discovery procedure. The prepared DNN demonstrate is spared and utilized in identification. Subtleties of the three modules will be clarified beneath.

III. Data pre-handling

In this paper, KDD99 and NSL-KDD datasets are utilized as our preparation and testing datasets. Insights concerning the KDD99 and NSL-KDD datasets can be found in [2]. There are four kinds of interruption in the dataset [23], as appeared Table 2.

One record of the information interruption is a component vector with 41 components. Portrayal of the component vector is appeared Table 3. Subtleties can likewise be found in http://www.kdd.org/kdd-glass/see/kdd-container 1999/Task.

A case of the first interruption information record is
x = {0, icmp, ecr_i, SF, 1032, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0,
0, 0, 0, 0, 0,

References	Methods	Performance
Fiore *et al.* [17]	RBM	accuracy: around 94%
Do *et al.* [18]	an ensemble of DBNs Khaled *et al.* [19]	RBM together with DBNs detection *F*-score on mixed data is around 72% detection rate is 97.9%
Zhao *et al.* [20]	DBNs with PNN	detection accuracy is about 99%. Detection rate is about 90%
Javaid *et al.* [16]	STL	accuracy rate is more than 98%, a little lower than 99%. *F*-measure can achieve 98.84%
Potluri and Diedrich [21]	accelerated DNN	highest detection accuracy is 97.7%
Roy et al. [22]	DNN	better than SVM in interruption identification
Yin et al. [15]	RNN-IDS	superior to conventional AI

Table 2: Description of five labels

Intrusion type	Description	Label
Probe	scanning and detection	1
Dos	denial of service attack	2
U2R	illegal access to local super users	3
R2L	unauthorised remote access	4
Normal	normal record	5

Initial step of information preparing is information separating (In genuine caught information, loads of interruption records are same, so de-duplication would be utilized to diminish the measure of information entering the IDS to take out the data excess. KDD99 dataset has just been de-copied and sifting isn't important in this paper.). A portion of the highlights are numerical and others are representative. At that point institutionalization is utilized to change all information caught from various IDS sources into numerical organization to rearrange the information preparing. Emblematic highlights are changed over to numerical marks. Guidelines are as per the following:

(i) Protocal type: 1 icmp; 2 tcp; 3 udp; 4 others.

(ii) Service: 1 space u; 2 ecr_i; 3 eco_i; 4 finger; 5 ftp_data; 6 ftp; 7 http; 8 hostnames; 9 imap; 10 login; 11 mtp; 12 netstat; 13 other; 14 private; 15 smtp; 16 systat; 17 telnet; 18 time; 19 uucp; 20 others.

(iii) Flag: 1 REJ; 2 RSTO; 3 RSTR; 4 SO; 5 S3; 6 SF; 7 SH; 8 OTHERS.
Highlights including land, logged_in, is_host_login, is_guest_login are images with esteem 0 or 1. Diverse highlights have distinctive measurements and the range is wide. To maintain a strategic distance from the vanishing of little numerical traits and lessen the measure of computation cycles, numerical information is standardized to [0,1] with a direct capacity given in the accompanying condition:
y = (x − xmin/xmax − xmin (2)
0, 0, 511, 511, 0.00,
0.00, 0.00, 0.00, 1.00, 0.00,
0.00, 255, 255, 1.00, 0.00,
1.00, 0.00, 0.00, 0.00, 0.00,
0.00, smur f } (1)

xmin and xmax are the base and most extreme estimations of the considerable number of components. One-hot encoding is utilized to exhibit the 42th characteristic of x. It is a gathering of bits among which the legitimate mixes of qualities are just those with a solitary high (1) bit and all the others low (0) [24]. The one-hot code of 2 is 01000, as appeared (3). The upside of utilizing this code is the majority of the five codes have the equivalent .There are 42 qualities in x, 41 highlights and a name. Smurf is the name of the record x. weight and it is impartial for the classifier.
For example, the interruption information x is a 41-dimensional element vector. After institutionalization and standardization, x′ is

IV. NDNN Model Structure

4.1 NDNN Structure Building

DNN is an essential structure of profound learning system with no less than one shrouded layer. DNN can give displaying to complex non-straight frameworks. Additional layers give an a lot larger amount of unique highlights to upgrade the ability of the model.
NDNN has a straightforward system structure. It is made out of three sections: input layers, concealed layers and yield layers. The structure is appeared, incorporating an information layer with 41 neurons, 4 shrouded layers and 100 neurons for every layer, 1 completely associated (FC) layer with 5 neurons, a softmax layer and a yield layer with 5 neurons. The
In NDNN, amended direct unit (ReLU) is utilized as the enactment capacity of the concealed layer neurons. ReLU is a non-straight initiation work communicating the perplexing characterization limit superior to anything direct actuation work [26]. Due to ReLU, the angle evaporating brought about by sigmoid capacity can be avoided
Table 3 Forty one highlights of a unique interruption information record Description Feature Data properties preparing consequence of each layer is treated as the contribution of the following layer (Fig. 2).

4.1.1 Input and concealed layers: The unpredictable mapping connection between info vector X and yield vector Y is built in the system display. The information vector X is a 41-dimensional component vector of one interruption record. The yield vector Y is a 5-dimensional likelihood vector with qualities somewhere in the range of 0 and 1. Each esteem demonstrates the likelihood which sort of interruption (four kinds of assault and one typical information) the info has a place with. Aggregate of the five yields (y1, y2,… ,y5) is 1. Limit of the yield is viewed as the grouping consequence of the present information.
For instance of a solitary concealed layer coordinate with 100 neurons, there are N tests (xi, yi) (i = 1,2,… ,N). Yield of the shrouded layer neurons is communicated in the accompanying condition [25]:
h = g(wx + b) (4)
Yield of all associated layer neurons is communicated in the accompanying

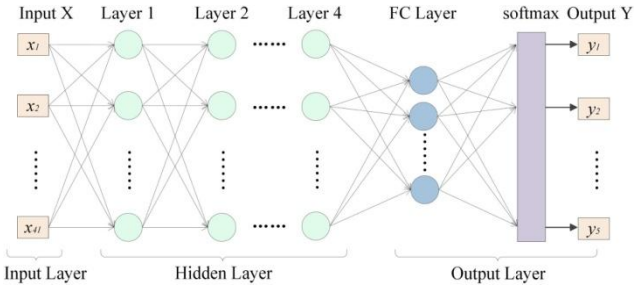

Fig. 2 *Designed NDNN model for IDS*

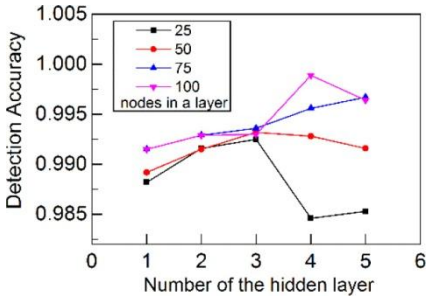

Fig. 3 *Network layer number, network node number and detection accuracy test of the proposed NDNN on KDD99 dataset*

4.2 Network parameter choice

Various component learning tests have been done to locate the best system structure which has the best element learning execution [15]. Fig. 3 demonstrates a few test exactnesses of system structure with various system layer number, organize hub number.

Trials demonstrate that regardless of what number of hubs are set in a layer, as the layer number increments from 1 to 3, the precision of testing is expanding (display structure is recorded as layer number-hubs number in a layer). While when the layer number increments to 4, show with 25 hubs a layer (demonstrate 4-25) and model with 50

Interruption class Number of preparing information

Number of testing information hubs a layer (demonstrate 4-50) are overfitting and the precision begins to drop. The exactness of the model 4-75 and model 4-100 is still

Probe	3723	384
DoS	356,691	34,767
U2R	41	11
R2L	1024	102
Normal	88,515	8763

effectively, and the inference is simple. The ReLU work is appeared in the accompanying condition:

$g(x) = \max(0, x)$ (9)

In [15], three diverse learning rate (LR) values have been tried lastly they pick 0.1. Here a randomized streamlining technique, Adam (versatile minute estimation) [27], is utilized as the stochastic inclination plunge optimiser in NDNN. The benefit of Adam is after inclination revision, every iterative LR has an unmistakable range, which makes the parameters increasingly steady. The underlying estimation of LR is 0.001. The esteem is powerfully changed by the Adam optimiser. Figuring distinctive versatile LRs for various parameters requires less memory. Contrasted and other versatile learning calculations, the union rate is expanded and increasingly viable, and the issues existed in other streamlining methods, for example, the vanishing of LR, the moderate combination or the misfortune work fluctuating brought about by extensive difference parameter refresh, can be amended.

4.1.2 FC layer – characterization: NDNN arrange demonstrate is utilized to distinguish and group obscure interruption information. Yields of neurons of shrouded layers speak to abnormal state includes in the information and these information should be arranged into five kinds of interruptions. A FC layer is intended to delineate highlights into five classes. There are five hubs in the FC layer. The 100-dimensional highlights from the fourth layer are mapped into five classes with this layer.

The last layer of the NDNN show is a softmax classifier. Softmax actuation work is commonly utilized for a system with more than one yield neuron. softmax classifier is a sort of various yield aggressive characterization calculation. Each yield speaks to an order classification likelihood. Preparing softmax is a directed procedure and named information is required. To diminish the bogus positive, realized assaults should be characterized into various classifications in preparing. Ordinary information and obscure assaults are additionally added into the preparation dataset to improve the speculation execution of the calculation.

The softmax work is appeared in the accompanying condition: expanding. At the point when the layer number is added to 5, exactness of the model 5-100 starts to drop. It demonstrates that 4-layer might be the best decision for the model with 100 hubs a layer. It tends to be treated as a neighborhood streamlining esteem. As the precision is as of now 0.998, we think it is sufficiently high in test tests and the model 4-100 is chosen. The exactness of the model with 75 hubs a layer is as yet expanding, while the precision is dependably not as high as a model with 100 hubs in a layer. Because of the fulfilled model 4-100, no more investigations are done to

investigate the exactness with more layers. A few parallel analyses likewise demonstrate that when there are 4 concealed layers and 100 hubs in each layer, the NDNN show has its best execution. So at last model 4-100 is picked as the NDNN structure.

In the preparation method, NDNN arrange demonstrate is worked to extricate highlights from countless interruption information. Parameters of each system layer are advanced to make the later interruption acknowledgment execution better. At that point the prepared NDNN demonstrate with the best parameters and system structure is spared to order the obscure system interruption. In identification methodology, testing information is input the prepared NDNN to do interruption arrangement.

V. Experiment

KDD Cup 1999 dataset [23] and NSL-KDD dataset [28] are utilized in this examination. The planned system is kept running in tensorflow 1.0 on a PC with an Intel Core i7– 5820k (R) focal handling unit (3.70 GHz), 16 GB memory and a GeForce GTX1060 GPU.

5.1 Dataset

The KDD99 dataset [23] and NSL-KDD dataset are generally utilized as a dataset to perform different execution tests on the planned IDS. There are four sorts of interruption in the dataset: Probe, Dos, U2R and R2L. In KDD99 dataset, just 10% of the absolute dataset are chosen, the dataset from 'kddcup.data_10_percent' contains 494021 association records. About 90% of them are arbitrarily chosen as the preparation set, and the staying 10% are utilized as the test set. The test set contains not just kind of assault that has happened in the preparation set, yet additionally sorts of assault never happened. In addition, the execution of NDNN has additionally been tried on NSL-KDD. Comparative activities of information preparing have been done on this dataset. Traffic records dissemination in the preparation and test information for ordinary and assault dataset is given in Tables 4 and 5.

5.2 Analysis of the trial results

For the assessment of IDS execution, five assessment records

y(z) j ezj K zk k = 1 , j = 1, … , K (10)

have been utilized: precision (Acc), review (R) [or discovery rate (DR), registering strategies for R and DR are the same], F-measure, false location rate (FDR, which can likewise be treated as the bogus caution)

z is the yield of the FC layer. Every class has a z, and the softmax work is utilized to compute the likelihood of the classification. K is the quantity of interruption classes, and here K is 5. Softmax layer gives five likelihood esteems. At last, the biggest what's more, missing caution rate (MAR).

The particular meanings of the five measurements are appeared in conditions (11)– (15). Clarification of True Positive (TP), False Negative(FN), False Positive (FP), True Negative (TN) utilized in these conditions are portrayed.

VI. Conclusion

In this paper, a DNN-based IDS is fabricated. Examination results demonstrate that ability and execution of the NDNN-based IDS are superior to anything strategies dependent on customary AI technique. Utilizing NDNN arrange model to do interruption identification is practical, particularly in this multi-include dataset. Be that as it may, there are still a few issues should be tackled later on. To start with, if there are an excessive number of parameters and hard to tune, for example, the quantity of hubs and layers, the expansion of the system structure will prompt the exponential movement of registering time and different issues. In this paper, a portion of the parameters are chosen by tests. This is additionally utilized in some related papers [15]. While the hazard is that possibly it isn't the worldwide best arrangement. So related advancement calculations and programmed parameter tuning techniques will be concentrated to improve the execution. Second, the IDS ought to be tried in a genuine system condition. High identification rate on dataset does not mean the comparable execution in genuine recognition. In this way, more system recreation tests should be done later on. Third, it is discovered that with bigger preparing information scale, the location execution is better. Including more U2R and R2L interruption records in the dataset is required.

References

[1]. Dong, H.S., An, K.K., Choi, S.C., *et al.*: 'Malicious traffic detection using *K*- means', *J. Korean Inst. Commun. Inf. Sci.*, 2016, **41**, (2), pp. 277–284

[2]. Al-Yaseen, W.L., Othman, Z.A., Nazri, M.Z.A.: 'Multi-level hybrid support vector machine and extreme learning machine based on modified *K*-means for intrusion detection system', *Expert Syst. Appl.*, 2017, **67**, pp. 296–303

[3]. Kaur, A., Pal, S.K., Singh, A.P.: 'Hybridization of *K*-means and firefly algorithm for intrusion detection system', *Int. J. Syst. Assur. Eng. Manage.*, 2017, **9**, (4), pp. 1–10

[4]. Tahir, H.M., Hasan, W., Said, A.M., *et al.*: 'Hybrid machine learning technique for intrusion detection system'. 'Computer science for improving the quality of life'. Int. Conf. Computing and Informatics, Icoci, Istanbul,

[5]. Turkey, 2015
[6]. Yang, Q., Lou, J., Liu, S., *et al.*: 'Naïve Bayes decision tree hybrid approach for intrusion detection system', *Bul. Tek. Elektro Dan Inform.*, 2013, **2**, (3), pp. 2477–2487
[7]. Boujnouni, M.E., Jedra, M.: 'New intrusion detection system based on support vector domain description with information gain metric', *Int. J. Netw.*
[8]. *Secur.*, 2018, **20**, (1), pp. 25–34
[9]. Gao, N., Gao, L., Gao, Q., *et al.*: 'An intrusion detection model based on deep belief networks'. Second Int. Conf. Advanced Cloud and Big Data,
[10]. Huangshan, People's Republic of China, 2014, pp. 247–252
[11]. Lin, W.-C., Ke, S.-W., Tsai, C.-F.: 'CANN: an intrusion detection system based on combining cluster centers and nearest neighbors', *Knowl.-Based Syst.*, 2015, **78**, pp. 13–21
[12]. Zhu, W., Deng, M., Zhou, Q.: 'An intrusion detection algorithm for wireless networks based on ASDL', *IEEE/CAA J. Autom. Sinica*, 2018, **5**, (1), pp. 92– 107
[13]. Wang, W., He, Y., Liu, J., *et al.*: 'Constructing important features from massive network traffic for lightweight intrusion detection', *IET Inf. Sec.*, 2015, **9**, (6), pp. 374–379
[14]. Sujendran, R., Arunachalam, M.: 'Hybrid fuzzy adaptive wiener filtering with optimization for intrusion detection', *ETRI J.*, 2015, **37**, (3), pp. 502–511
[15]. Kyriakopoulos, K.G., Aparicio-Navarro, F.J., Parish, D.J.: 'Manual and automatic assigned thresholds in multi-layer data fusion intrusion detection system for 802.11 attacks', *IET Inf. Sec.*, 2014, **8**, (1), pp. 42–50
[16]. Costa, K.A.P., Pereira, L.A.M., Nakamura, R.Y.M., *et al.*: 'A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks', *Inf. Sci.*, 2015, **294**, pp. 95–108
[17]. Bamakan, S.M.H., Wang, H., Shi, Y.: 'Ramp loss *K*-support vector classification-regression; a robust and sparse multi-class approach to the intrusion detection problem', *Knowl.-Based Syst.*, 2017, **126**, pp. 113–126
[18]. Yin, C.L., Zhu, Y.F., Fei, J.L., *et al.*: 'A deep learning approach for intrusion detection using recurrent neural networks', *IEEE. Access.*, 2017, **5**, pp. 21954–21961
[19]. Javaid, A., Niyaz, Q., Sun, W., *et al.*: 'A deep learning approach for network intrusion detection system'. Eai Int. Conf. Bio-Inspired Information and Communications Technologies, New York City, NY, USA, 2016, pp. 21–26
[20]. Fiore, U., Palmieri, F., Castiglione, A., *et al.*: 'Network anomaly detection with the restricted boltzmann machine', *Neurocomputing*, 2013, **122**, pp. 13– 23
[21]. Do, K., Tran, T., Venkatesh, S.: 'Multilevel anomaly detection for mixed data', 2016, arXiv:1610.06249
[22]. Alrawashdeh, K., Purdy, C.: 'Toward an online anomaly intrusion detection system based on deep learning'. IEEE Int. Conf. Machine Learning and Applications, Anaheim, CA, USA, 2017, pp. 195–200
[23]. Zhao, G., Zhang, C., Zheng, L.: 'Intrusion detection using deep belief network and probabilistic neural network'. IEEE Int. Conf. Computational Science and Engineering, Guangzhou, People's Republic of China, 2017
[24]. Potluri, S., Diedrich, C.: 'Accelerated deep neural networks for enhanced intrusion detection system'. IEEE Int. Conf. Emerging Technologies and Factory Automation, Berlin, Germany, 2016
[25]. Roy, S.S., Mallik, A., Gulati, R., *et al.*: 'A deep learning based artificial neural network approach for intrusion detection', 2017, pp. 44–53
[26]. Stolfo, S.J., Stolfo, S.J.: 'KDD cup 1999 dataset', 1999, available at: http:// kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[27]. Harris, D.M., Harris, S.L.: 'Digital design and computer architecture',
[28]. *Microelectron. Reliab.*, 2012, **44**, pp. 1279–1280
[29]. Ding, S., Guo, L., Hou, Y.: 'Extreme learning machine with kernel model based on deep learning', *Neural Comput. Appl.*, 2017, **28**, (8), pp. 1975–1984
[30]. Dahl, G.E., Sainath, T.N., Hinton, G.E.: 'Improving deep neural networks for LVCSR using rectified linear units and dropout'. IEEE Int. Conf. Acoustics,
[31]. Speech and Signal Processing, 2013, pp. 8609–8613
[32]. Kingma, D.P., Ba, J.: 'Adam: a method for stochastic optimization',
[33]. Computer Science, 2014
[34]. Chae, H.S., Jo, B.O., Choi, S.H., *et al.*: 'Feature selection for intrusion detection using NSL-KDD', Proceedings of the 6th WSEAS World Congress: Applied Computing Conference (ACC'13), Nanjing, China, 2013, pp. 184– 187
[35]. Dong, C., Zhou, G., Liu, Y. J., *et al.*: 'The detection of network intrusion based on improved adaboost algorithm', Journal of Sichuan University, 2015
[36]. Chun-Lin, L.I., Huang, Y.J., Wang, H., *et al.*: 'Detection of network intrusion based on deep learning', in Ding, S. (Ed.): '*Information security & communications privacy*' (Beijing, China, 2014), pp. 68–72
[37]. Chebrolu, S., Abraham, A., Thomas, J.P.: 'Feature deduction and ensemble design of intrusion detection systems', *Comput. Secur.*, 2005, **24**, (4), pp. 295–307
[38]. Chen, Y., Abraham, A., Yang, B.: 'Feature selection and classification using flexible neural tree', *Neurocomputing*, 2006, **70**, (1-3), pp. 305–313
[39]. Chandrasekhar, A.M., Raghuveer, K.: '*An effective technique for intrusion detection using neuro-fuzzy and radial SVM classifier*' (Springer New York, 2013)
[40]. Ambusaidi, M.A., He, X., Nanda, P., *et al.*: 'Building an intrusion detection system using a filter-based feature selection algorithm', *IEEE Trans. Comput.*, 2016, **65**, (10), pp. 2986–2998