Computer Science Journal of Moldova, vol.**29**, no.2(86), 2021

Cybercrime Detection Using Semi-Supervised Neural Network

Abbas Karimi, Saber Abbasabadei, Javad Akbari Torkestani, Faraneh Zarafshan

Abstract

Nowadays, artificial intelligence is widely used in various fields and industries. Cybercrime is a concern of these days, and artificial intelligence is used to detect this type of crime. Crime detection systems generally detect the crime by training from the related data over a period of time, but sometimes some samples in a dataset may have no label. Therefore, in this paper, a method based on semi-supervised neural network is presented regarding crime types detection. As the neural network is a supervised classification system, therefore, this paper presents a pseudo-label method for neural network optimization and develops it to semi-supervised classification. In the proposed method, firstly the dataset is divided into two sections, labelled and unlabelled, and then the trained section is used to estimate the labelling of the unlabelled samples based on pseudo-labels. The results indicate that the proposed method improves the accuracy, Precision and Recall up to 99.83%, 99.83% and 99.83%, respectively.

Keywords: cybercrime, intrusion detection, neural network, semi-supervised classification.

1 Introduction

Today, with the development of information and communication technology (ICT), cybercrime has become a global concern [1]–[5]. Two factors, including time of using the computer and activity in the social

network, have been identified as the main factors and predictors of cybercrime. Cybercrime analysis is an important responsibility of the law enforcement system in every country [6]–[8]. As the crime exists in different and separable cases, the adaptability of the discovered patterns has concerns and challenges. Classification is often used to predict the process of crime, which reduces the time of offender's identification [3]–[9]. Failure to identify the crime causes and the criminal abuse make the society unsafe [2]–[10]. The best model for preventing crime is reducing the chance of crime in the society [11]. Criminal behavior is the result of an appropriate opportunity to commit a crime at a particular place and time, and eliminating or reducing those opportunities leads to reduction of crime in that situation, so it is the most important factor in preventing a crime [12]–[14]. Therefore, crime prevention has always been one of the most important issues of life that has been practiced through various ways. Intrusion was referred to is a [15]–[17]. Intrusion, that was referred to, is a series of unlawful acts that endanger the accuracy, privacy or access to a resource [16], [18], [19]. The intrusion can be divided into internal and external. External intrusion is carried out from outside a network into internal network by authorized or unauthorized persons, and internal intrusion is carried out within a network by authorized persons [20], [21]. Intruders generally use software defects, decryption and network sniffing to penetrate computers and networks. In order to deal with intrusion, several methods have been developed called intrusion detection methods that monitor the events occurred in a computer system or network [2], [22]–[24]. Due to the development of ICT and the launch of comprehensive information systems in police force and criminal intelligence registering, data mining and knowledge discovery techniques are used to analyse and detect the cybercrime, especially intrusion [25]–[27]. So, predicting, preventing and detecting the cybercrime using the data mining is a fascinating new idea performed by statistical techniques, machine learning, artificial intelligence and criminology [28]. For expanding the classification of cybercrime, we can use algorithms of supervised machine learning such as artificial neural networks. These methods are also used in data mining [29]–[32]. The basic idea of artificial neural networks is inspired

by the way the biological system uses for learning and knowledge creation [31]. A key element of this idea is creation of new structures for the information processing system. This consists of a large number of highly interconnected processing elements called neurons that work together to solve a problem and transmit information through synapses. The learning is adaptive, namely the weight of the synapses is changed by using samples to generate a correct response [34], [35]. Neural network is used in medical diagnosis [36], [37], reconstruction of digital elevation model [38], intrusion detection [39], [40], etc. This is a supervised classification, but the labelling is expensive and time consuming, so today there are various ways to provide semi-supervised methods [33]. Therefore, in this paper, an optimized semi-supervised neural network method for computer crime detection is presented. Here we propose a method called pseudo-label (PL) [41] in artificial neural network. Unlike supervised learning, our proposed method uses labelled and unlabelled samples during training. For unlabelled samples it produces predicted labels, which measure the overlap of detection probability based on probabilistic conditional entropy. Assuming the probability of detecting each type of independent class, the predicted label is calculated with the maximum probability in training process. Since the estimated label values may be erroneous, a variable coefficient called influence coefficient is used to control its impact on the classification process. Therefore, a reduction criterion is added for unlabelled samples. So, the main contribution of this paper is as follows:

- Modelling and extraction of cybercrime patterns using data mining.

- Increasing the accuracy in crime detection using semi-supervised neural networks.

- Evaluating the proposed method using evaluation parameters.

The rest of the paper is as follows: Section 2 briefly reviews related works. Section 3 provides an overview of the proposed method. In Section 4, the evaluation of the proposed method is presented and com-

pared with other methods. Conclusions and future work are presented in Section 5.

2 Literature review

In recent years, several researches on crime and intrusion detection problem have been conducted. Most of them used data mining and machine learning. Intrusion is a cybercrime, so this section is divided into two separate subsections: cybercrime detection and intrusion detection.

2.1 Cybercrime detection

Qayyum et al. (2018) investigated data mining techniques for crime detection. Crime detection is one of the hot topics in data mining, where different patterns of criminology have been identified. Its various steps include identifying the crime characteristics to identify the pattern of the crime. Data mining techniques have been widely used for crime detection. An analytical study by extracting the strengths and weaknesses of each technique is presented [6].

In 2018, Mingcheng Feng et al. analyzed big data and used data mining for crime analysis and prediction. The purpose of this study was to analyze exploratory data for criminal data analysis in the cities of San Francisco, Chicago, and Philadelphia. They examined data time series and predicted crime trends over the coming years. Experimental results indicate that the decision tree classification model fits better than k-NN and Bayesian approaches. These promising achievements will be useful for police and law forces to expedite the process of crime detection and provide insights that enable police and law forces to trace criminal activities, predict the likelihood of crime occurring, use resources effectively and make faster decisions [42]. Dutta et al. in 2017 investigated the detection of impersonation crime using data mining. This study mainly focuses on credit card related impersonation crime which is very common and costly nowadays. Current data mining techniques are not able to eliminate impersonation, and new data mining is

suggested to combat these crimes. This new method uses both public detection and Spike detection algorithms to detect fraudulent actions in programs [3]. Proffitt et al. (2018) studied the impact of cybercrime on economic crisis management. The purpose of this study was to find out how control of disaster recovery can help us to distinguish the cybercrime which disrupts the business. The results of the study are requirements of planning cyber security, aligning disaster recovery with cyber security, providing cyber security training for managers and employees, and applying the lessons learned from the experience. Implications for positive social change include the ability of organizations to return to acceptable levels of operations and continue to serve their employees, customers and other stakeholders [43].

Solak et al. (2015) studied the analysis of cybercrime perceptions among computer science students. Computer technology is growing rapidly and has become an inevitable part of modern life. While technology simplifies social life, at the same time it brings some security issues. So, it is easier to commit a crime and we are facing cybercrime. This study distinguishes the differences between broad perceptions of undergraduate students at Trakya University in terms of demographic factors. The research method was a questionnaire that was given to teachers and students in the Trakya University sample and was designed to measure and evaluate the level of interest in technology, the severity of cybercrime and people's perceptions of cybercrime in terms of ethics and law. The findings of this study can help us to identify the level of general understanding of cybercrime and the significant differences between groups [44].

Rosellini et al. (2017) investigated the use of data mining to identify US Army soldiers committing violent crimes. The purpose of this study was to use machine learning methods, stepwise regression and random forests, to develop models of predicting violent crime and crime among the US Army soldiers. Results indicated that using this method we can prevent the dangers which might happen to soldiers [45].

Li et al. (2017) researched the development of crime in England by using data mining with selforganized maps (SOM). The aim of this study was to study criminal phenomena in the United Kingdom and its

relationship with different crime factors. Data are collected by the SOM method. Clustering and properties are evaluated using the Scooter algorithm. Machine learning is applied to confirm the clustering result with SOM. As a result, 96.2% accuracy is achieved for crime prediction [46].

Chauhan and Sehgal (2017) studied crime analysis by using data mining techniques. With the rise of computer systems, crime intelligence analysts can help law enforcement officials speed up the process of solving crimes. Using the concept of data mining, we can analyze unknown and useful information of unstructured data. Using analytical and predictive techniques for criminal identification is very effective. Given the increasing crime rate over the years, we have to handle a huge amount of data and it will be extremely difficult to access. Criminals are progressing with the technology. Therefore, it is necessary to use advanced technologies to prevent crime. They focus on examining the algorithms and techniques used to identify criminals [25].

David and Suruliandi (2017) investigated crime analysis and use of data mining techniques at police stations and other similar criminal organizations. Databases contain a great deal of data that can be used to predict or analyze criminal movements and criminal interference in the society. Criminals can be predicted based on crime information. The main purpose of this study was conducting a survey on learning techniques of criminal identification. They investigated the method of crime analysis and its prediction using data mining techniques [47].

Hassani et al. (2016) investigate the use of data mining in crime. The main purpose of this paper is to present data mining applications in crime detection. It covers more than 100 applications of data mining in crime. Data mining techniques including data extraction, clustering, associated rules, decision tree, support vector machines, naive Bayesian, neural networks were applied and the desired results were significant for crime prediction [8].

2.2 Intrusion detection

Meera Gandhi et al. presented an intrusion detection model using decision trees. A 10-fold cross-validation metric was used to evaluate the proposed method. According to this metric, the proposed method detected known intrusion better than unknown intrusion [48]. Lakhina et al. [49] reduced the number of features taken from NSL-KDD dataset using PCA algorithm. In this study, they used principal component analysis and back propagation algorithm. Another research [38] used data mining to extract associated rules for attacks [50]. This framework produced a large number of rules, thereby increased the complexity of the system. Also, Dempster-Shafer and adaptive boosting (AdaBoost) [51] was used for intrusion detection. Meena et al. also presented a review paper on several classification algorithms with KDD CUP 99 and NSL-KDD datasets [52]. Elmasry et al. investigated a multiclass classification for intrusion detection. This is an empirical study, and it uses particle swarm optimization and deep learning to classify various datasets (KDD CUP 99, NSLKDD, CIDDS, and CICIDS2017) [16]. Verma et al. proposed a machine learning method for network intrusion detection. They used CIDDS-001, and the results show that accuracy in this method is 99.60% [53]. A system for HTTP DDoS Attacks detection was investigated in [54] based on information theory and Random Forest.

As it is shown above, most research has focused on cybercrime detection and intrusion detection using supervised methods. Therefore, the aim and main novelty of this paper is to improve the artificial neural network to use semi-supervised classification for intrusion detection.

3 Proposed method

In this section the proposed method is introduced. Initially, the methods used for data pre-processing are introduced, which include data normalization. The standard neural network is presented, and then the proposed method for using unlabelled data in the neural network is introduced.

3.1 Normalization

The goal of normalization is to normalize the elimination of data redundancy and maintain the dependency between related data. This process reduces the size of the database and guarantees improvement of data efficiency. Normalization by standard deviation works well in most cases by measuring the distance between intervals [55]. For sample i, the given value is converted using the following equation: If F is the feature, $\bar{F}$ is F mean, Std is standard deviation, and F' is the normalized value of the feature as follows:

$$\overline{F} = \frac{\sum F_i}{n}; \tag{1}$$

$$Std(F) = \sqrt{\frac{\sum (F_i - \overline{F})^2}{n-1}}; \tag{2}$$

$$F'_i = \frac{F_i - \overline{F}}{Std(F)}. \tag{3}$$

3.2 Artificial Neural Network

Artificial Neural Network (ANN) classification is one of the most effective methods in data classification, but this method has a critical problem which is getting stuck in local optimum [33], [34]. The purpose of network in training process is to minimize the total error of the network based on the weight of the network. We show ANN model as a function (4).

$$y' = M(F'). \tag{4}$$

Here y' is a predicted label, F' is an input feature vector extracted from equation (3), and M is a model of ANN. The back-propagation (BP) training algorithm is used. In layers (except input layer) we use a linear function like equation (5):

$$x = \sum F' \cdot W + b, \tag{5}$$

where W is a weight vector. We used tan as an activation function (equation (6)) to calculate outputs:

$$\text{Activation function} = f(\cdot) = \frac{1 - e^{-x}}{1 + e^{-x}} = y'; \tag{6}$$

$$\text{Error} = y - y'. \tag{7}$$

In this algorithm, after calculating the error in the output layer (equation 7), the values of the weights in the hidden layer are adjusted to reduce the error. Therefore, we need to have a differential of activation function according to the following equation:

$$\frac{d}{dx}\frac{1 - e^{-x}}{1 + e^{-x}} = 1 - \tanh^2 x = (1 - y')(1 + y'). \tag{8}$$

BP Error algorithm, which is an iterative gradient descent algorithm, is a simple way to train multilayer feed forward neural networks. The BP algorithm is based on the gradient descent rule:

$$W(n+1) = W(n) + \eta G(n) + \alpha[W(n) - W(n-1)], \tag{9}$$

where W is the weight vector, n is the iteration number, η is the learning rate, α is the momentum factor, and G is the gradient of error function that is given by 10:

$$G(n) = -\nabla E_p(n). \tag{10}$$

Here E_p is the sum squared error and calculated using equation (8).

This network can be defined as an information processing system consisting of a set of layers and mapping inputs (F') to a suitable set of outputs (y'). The neurons in each layer are fully connected with the neurons in the next layer. In ANN, each neuron has a nonlinear activation function except the input nodes. Updating weights continues to get the given level of error. Finally, ANN uses an appropriate gradient learning algorithm to train.

3.3 Proposed semi-supervised neural network

The main problem in ANN is getting stuck in local minima. Also, because this method is a supervised classification, therefore it is not usable for unlabelled data. We propose a method using pseudo-label (PL) [41] in the neural network. Based on the proposed method, the semi-supervised learning framework is used to train labelled and unlabelled samples. Unlabelled samples are labelled using equation (11).

$$y'_{Unlabelled} = \min d(M(F'), y), \tag{11}$$

where, d is a distance function. In fact, this relationship states that at each stage of training in the neural network the label of unlabelled data is estimated. The unrealistic label y' is calculated with the minimum distance. Since the estimated label values can be accompanied by an error, a coefficient is used to control its impact on the classification process. In this view, a reduction criterion is added for unlabelled samples. This criterion is shown in the equation (12).

$$E = \operatorname{argmin}\big[\text{norm2}_{lable}(y', y) + \alpha(t)\text{norm2}_{Unlabelled}(y'_{Unlabelled}, y)\big]. \tag{12}$$

In this equation, α is the influence coefficient for control the error between labelled and unlabelled samples in the training process. The equation (13) is used here to calculate the value of α.

$$\alpha(t) = \begin{cases} 0 & t \leq \varepsilon_1 \\ \left(\frac{t-T_1}{T_2-T_1}\right)^2 & \varepsilon_1 < t < \varepsilon_2 \\ 1 & \varepsilon_2 \leq t \end{cases} \tag{13}$$

where ε_1 and ε_2 are errors in the training process. Equation (13) represents the current iteration, T_1 is the first iteration with error equal to ε_1, and T_2 is the second iteration with error equal to ε_2 in the training process. We proposed three conditions as follows:

Condition 1: If $t \leq \varepsilon_1$, then in training process, equation (7) is used without unlabelled samples.

Condition 2: If $\varepsilon_1 < t < \varepsilon_2$, then in training process, equation (12) is used with labelled and unlabelled samples. In each epoch, updating $y'_{Unlabelled}$ is performed using equation (11).

Condition 3: If $\varepsilon_2 < t$, then in training process, equation (12) is used with labelled and unlabelled samples.

Pseudocode for the proposed method is illustrated in Table 3. Flow chart is shown in Figure 1.

Algorithm 1 Pseudocode for the proposed back propagation algorithm

Input: η:learning rate α:momentum value and designing multilayer network
Output: A trained neural network Method:

1: Create the initial amount of weights and bias in the network
2: Repeat loop until desired condition {
3: Repeat loop according to number of samples {
4: // feed forward
5: Repeat loop for each j of input layer {
6: $O_j = I_j$ // The output of an input unit is equal to its actual value.
7: Repeat loop for each j of the hidden layer or the output layer {
8: $I_j = \sum_i W_{ij} O_i + \theta_j$ // Calculating the unit network input j compared to i in the previous layer
9: $O_j = \frac{1-e^{-I_j}}{1+e^{-I_j}}$}// Calculate the output of each j
10: // back propagation {
11: If $t \leq \varepsilon_1${
12: Do line 22-31}
13: Elseif $\varepsilon_1 < t < \varepsilon_2${
14: Error = equation 12
15: updating $y'_{Unlabelled}$ using equation 11
16: Do line 22-31}
17: Else {
18: Combine labelled and unlabelled samples
19: Do line 22-31}
20: Repeat loop for each j in the output layer
21: Error = Target −Output // calculating error
22: $\Delta_O^{ij} = error \times (1 - y_{ij}) \times (1 + y_{ij})$ // calculating corrected error
23: Repeat loop for each unit j in the hidden layer from the last to first hidden layer
24: $\Delta_H = (1 + y_{ij}) \cdot (1 - y_{ij}) \cdot (\overline{\Delta_O} \times \overline{W})$
25: Repeat loop for W_{ij} weight and bias in the network {
26: $W_{ij}^{k+1} = W_{ij}^k + \eta G + \alpha[W_{ij}^k - W_{ij}^{k-1}]$}
27: $G = -\nabla E_p$}
28: If end of training = false go to line 10}

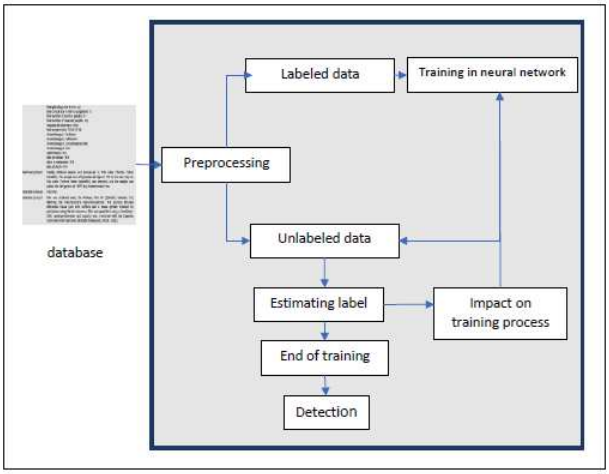

Figure 1. Flow chart for the proposed algorithm

4 Results and discussion

To prepare this paper, a computer with specific characteristics has been used, including:

Processor: Intel Pentium (R) CPU G620, 2.60 GHz 2.60GHz

Installed memory (RAM): 4.00 GB

System type: 32-bit Operating system

The operating system installed is Microsoft's Windows 10. MATLAB version R2017a 64-bit was used for modelling.

4.1 Database

In this paper we used Coburg intrusion detection dataset (CIDDS) to examine the proposed method. CIDDS is available in network-based intrusion detection system dataset. CIDDS has two versions called CIDDS001 and CIDDS-002, and we used CIDDS-001 version. This includes 12 features and 5 labelled classes. Class name and distribution

of dataset is Normal (32 000), DoS (32 000), brute force (32 000), port scan (32 000), and ping scan (32 000). Number of attacks and protocols are 92 and 5, respectively [16].

4.2 Evaluation Metrics

Confusion matrix [16],[56] is one of the criteria for evaluating each classifier. This matrix is a square matrix $N \times N$, where N is the number of classes in the classifier. The main diagonal in this matrix shows the number of correct diagnoses, and the other elements in this matrix show the wrong diagnoses. Table 1 illustrates an example of confusion matrix. Using this matrix, we obtain such metrics as Sensitivity, Specificity, Precision, Recall, F_1, and G-Means.

Table 1. Confusion matrix

True Positive (TP) crimes that are correctly identified as an intrusion	False positive (FP) Correct activity that has been wrongfully detected as an intrusion
False Negative (FN) intrusions that has been wrongfully detected as a correct activity	True Negative (TN) Correct activity that is correctly identified as a correct one

Mathematically speaking, Sensitivity through equation (14), consists of dividing the true positive into the sum of the true positive and false negative.

$$\text{Sensitivity} = \frac{TP}{TP + FN}. \tag{14}$$

Similarly, the Specificity through equation (15), is the result of dividing the true negatives into the sum of the true negatives and false positives.

$$\text{Specificity} = \frac{TN}{TN + FP}. \tag{15}$$

The Precision parameter, through the equation (16), is the result of dividing the true positives into the sum of the true positives and false

positives.

$$\text{Precision} = \frac{TP}{TP + FP}. \tag{16}$$

The Recall parameter through equation (17) is the result of dividing the true positives into the sum of the true positives and the false negatives.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{17}$$

And the F_1-measure and G-mean [56] are also obtained through equations (18) and (19):

$$F_1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}; \tag{18}$$

$$\text{G-mean} = \sqrt{\text{Precision} \times \text{Recall}}. \tag{19}$$

It should be mentioned that since the dataset used here is multiclass, so each parameter is first separately calculated for each class. Then the average results are obtained.

Another tool for performance measure used here is the Receiver operating characteristic (ROC) [16]. To use the ROC curve in an evaluation, the area under the curve is suggested. This area is the probability that whenever the diagnostic classification variable is randomly measured for a negative response and a positive response, the value obtained is correct. Whenever the test is able to identify accurately, then the values will be low for positive responses and high for negative responses (or vice versa depending on status). The greater the test detection power, the more the ROC curve is above the diagonal, and the closer it is to the ideal (region 1) ROC curve. Inversely, if the ROC curve is under the diagonal or just at the bottom of the square, then the test is with low detection capabilities or useless.

4.3 Comparison of results

Figure 2 shows the mean square error for each epoch of the proposed algorithm in training process. Since one of the problems in neural network is getting stuck in local optimal, so here we use data for validation

as shown in Figure 2 with the green line to decide on the number of iterations of the training process. This figure shows that the lowest difference exists between training and validation data in epoch 20. From the curves, the training error is descending, and these three curves are increased in epoch 3. This is because the unlabelled samples are joined to training process.

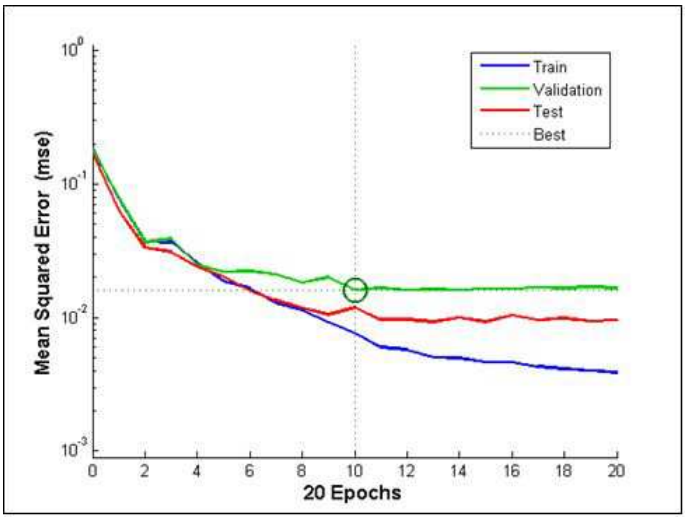

Figure 2. Mean square error in training process

Table 2 illustrates confusion matrix for Test set in the proposed method, called Semi-Supervised Neural Network (SSNN). Number of true predicted labels for Normal class (15976) and Ping scan class (15974) is more than for other classes. Table 3 shows evaluation metrics for SSNN method in each class separately. Precision metric for Normal (0.999) class and Ping scan (0.999) is more than for other classes in SSNN. Precisions for other classes such as DoS, Brute force and Port scan are 0.998, 0.998 and 0.997, respectively. Other evaluation metrics, such as Recall, F_1-measure, Sensitivity, Specificity and G-means are more than 0.99, and this means that SSNN can predict each class with high accuracy.

Tables 2 and 3 showed just the evaluation metrics for SSNN. There-

Table 2. Confusion matrix for each class

	Actual Classes				
	Normal	DoS	Brute force	Port scan	Ping scan
Normal	15976	8	2	10	2
DoS	6	15970	5	12	6
Brute force	5	9	15972	7	5
Port scan	9	10	13	15970	13
Ping scan	4	3	8	1	15974

Table 3. Performance evaluation of SSNN in terms of Precision, Recall, F_1-measure, Sensitivity, Specificity, and G-means for each class

Classes	Normal	DoS	Brute force	Port scan	Ping scan
Metrics					
Precision	0.999	0.998	0.998	0.997	0.999
Recall	0.999	0.998	0.998	0.998	0.998
F_1-measure	0.999	0.998	0.998	0.998	0.999
Sensitivity	0.999	0.998	0.998	0.998	0.999
Sensitivity	1.000	1.000	1.000	0.999	1.000
G-means	0.999	0.998	0.998	0.998	0.999

fore SSNN is compared with 7 other methods: ANN, SVM [53], NB [53], DT [53], VR [53], IAB [54], DBN [16]. ANN is a standard neural network explained in Section 3.1. SVM is support vector machine with Radial Basis Function (RBF) as a kernel function. NB and DT represent Naive Bayes and Decision Tree (J48), respectively. VR was investigated by Verma and Ranga using machine learning techniques to statistical analysis of dataset [53]. IAB was proposed by Idhammad et al. for attack detection in cloud environment [54]. DBN is deep belief networks and was explained by Elmasry et al. [16].

Accuracy is shown in Table 4. This metric for SSNN is equal to 99.83, and its value is greater than for ANN and other methods. Us-

ing of unlabelled samples in training process causes this improvement. After SSNN, VR and IAB have the greatest accuracy than in other methods, respectively. Another characteristic used here is AUC. The AUC for the SSNN (0.9987) shows better results.

Table 4. Accuracy and AUC

	SSNN	ANN	SVM	NB	DT	VR	IAB	DBN
Accuracy	99.83	95.71	98.19	98.70	98.90	99.60	99.54	94.66
AUC	0.9987	0.9571	0.9823	0.9871	0.9891	0.9961	0.9955	0.9625

Figure 3 shows the average of Precisions for all classes. As it is shown above, the SSNN method performs better than others. Precision is the ratio of classified samples by the classifier in a given class, to the total number of samples the classifier has classified in that class, either correctly or incorrectly. As it turns out from equation (16), the Precision shows in what proportion the detected positives are really positive. Precision in SSNN is equal to 99.83% and in ANN = 96.25%. DBN, VR and IAB have Precision 99.71%, 99.61% and 99.53%, respectively.

Figure 4 shows the value of average of Recall for classes. This parameter for SSNN is 99.83%, and in other methods, e.g., VR = 99.59% and IAB = 99.55%. So, it indicates that the proposed algorithm performs better than other methods. The Recall shows the ratio of true classification of samples in given classes by the classifier to the number of samples in that class. So, the Recall shows in what proportion true positives are correctly identified as positive. Therefore, Figure 4 shows that the SSNN predicts intrusion detection better.

F_1-Measure is proposed to compare Precision and Recall, in fact, F_1-Measure shows the harmonic mean between Precision and Recall (Figure 5). F_1-metric for SSNN is 99.83, and it is greater than for other methods like VR (99.60%). Increasing the number of training examples in the proposed method with the semi-supervised approach in it has improved the global search in NNSS.

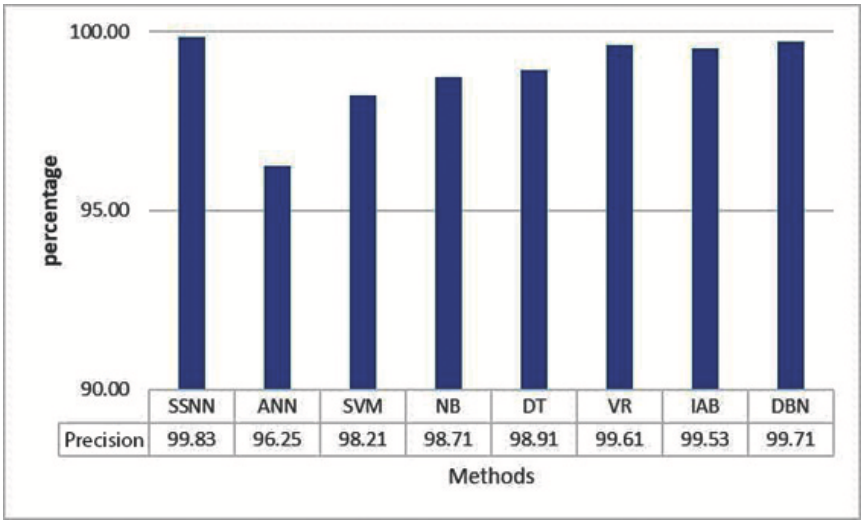

Figure 3. Comparison of Precision

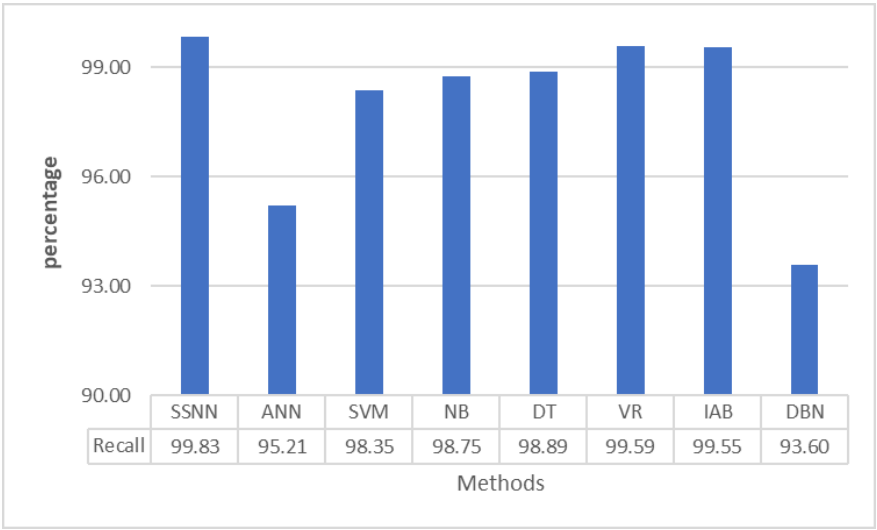

Figure 4. Comparison of Recall

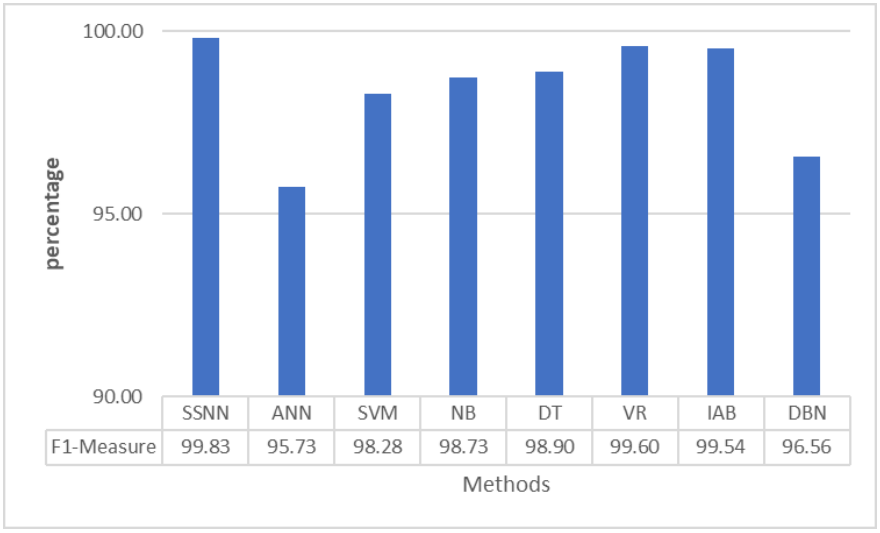

Figure 5. Comparison of F_1-measure

Figure 6 shows the values of the average Sensitivity parameter for all classes. The Sensitivity of SSNN is greater than 99.83%, which is better than for ANN (95.21%). The ability of a classifier to find the true positive of a class is called Sensitivity. According to equation (14), Sensitivity is ratio of true positives to the sum of true positives and false negative. So, the Sensitivity here shows what proportions of the intrusions are correctly identified. Therefore, this parameter also confirms that the SSNN predicts intrusions better than other methods.

Figure 7 shows the average Specificity value for all classes. The Specificity value for SSNN (99.96%) is greater than for the other methods. It indicates that the proposed method has performed well in Normal class. Figure 8 indicates average G-mean for all classes. G-mean in SSNN is 99.83% and proves that SSNN with higher accuracy predicts normal situation and attacks situation rather than ANN (97.21%), VR (99.60%), IAB (99.54%), DBN (98.90%), etc.

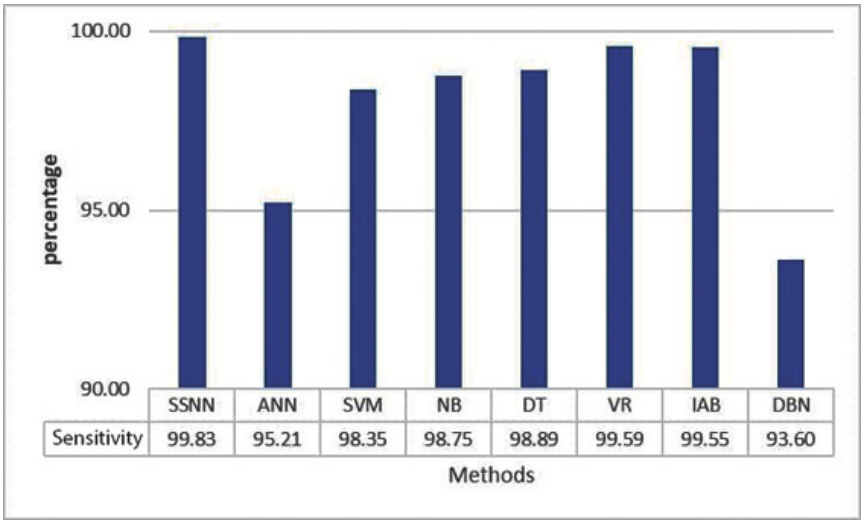

Figure 6. Comparison of Sensitivity

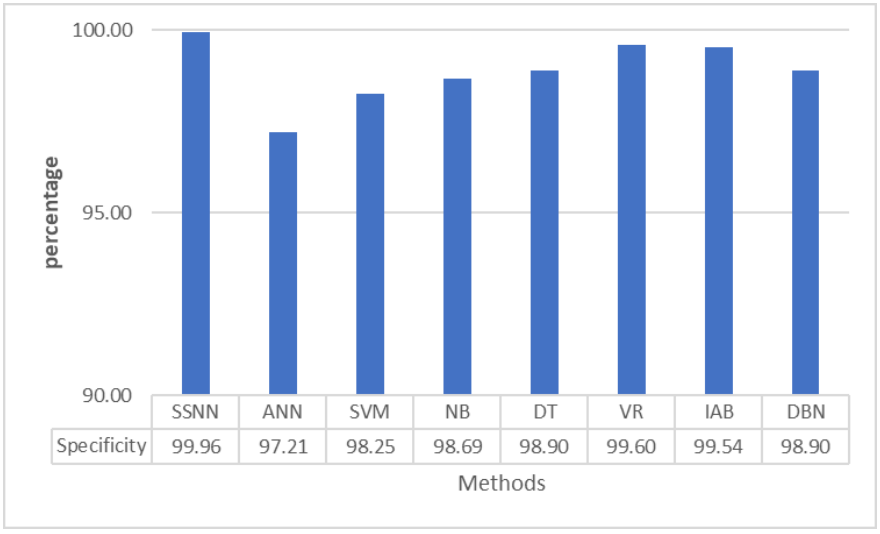

Figure 7. Comparison of Specificity

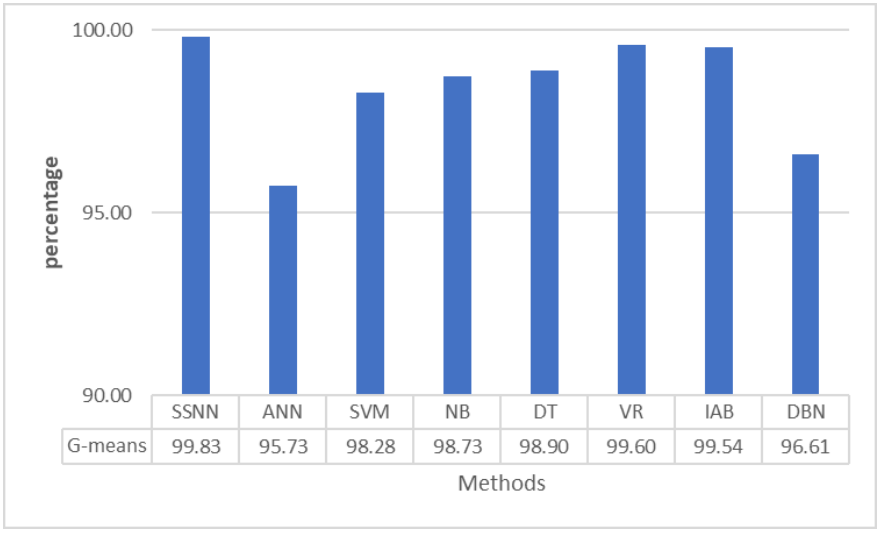

Figure 8. Comparison of G-means

5 Conclusion

Data mining techniques, including descriptive and predictive tools, have been introduced in various fields and a tremendous number of researches have been conducted on this issue. Data mining applications include business, management, medical, sports, econometrics, financial management, web business. One of the areas that has been the focus of data mining in recent years is the police enforcement, and one of the topics that has attracted a great deal of research is crime modelling. Therefore, this paper presents a semi-supervised method for detecting cybercrimes. The neural network is used here to classify the crimes. Since the neural network is a supervised classification technique, it is only usable for labelled data. On the other hand, it is a cost of fortune and time consuming to create labelled data. Thus, here the neural network is optimized so that it can be used in unlabelled data. Here the pseudo-labelling technique is used to estimate the labelled data during the neural network training process. The Precision, Recall, Sensitivity and Specificity values for the proposed network are obtained and

represent values of 99.83%, 99.83%, 99.83% and 99.96%, respectively. However, other researches have reported lower values.

We suggest for the future work, first, the detection of the probability of a crime before it happens, and this issue has not been addressed here. Second, a specific dataset is used here for crime detection, while many crimes occur today on social networks and data in the networks are a combination of text and images, so a hybrid method for crime detection is suggested.

Conflict of interest

We wish to inform that there is no known conflict of interest associated with this paper.

Acknowledgements

The authors are grateful for the support from Islamic Azad University and Atiye Andishan Group.

References

[1] A.-Z. Ala'M, J. f. Alqatawna, and H. Faris, "Spam profile detection in social networks based on public features," in *2017 8th International Conference on information and Communication Systems (ICICS)*, IEEE,2017, pp. 130–135.

[2] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Computational Science*, vol. 25, pp. 152–160, 2018.

[3] S. Dutta, A. K. Gupta, and N. Narayan, "Identity Crime Detection Using Data Mining," in *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*, IEEE, 2017, pp. 1–5.

[4] L. Y. Chang, L. Y. Zhong, and P. N. Grabosky, "Citizen co-production of cyber security: Self-help, vigilantes, and cyber-

crime," *Regulation & Governance*, vol. 12, no. 1, pp. 101–114, 2018.

[5] N. L. Piquero, "Causes and prevention of intellectual property crime," in *Combating Piracy*, Routledge, 2017, pp. 57–84.

[6] S. Qayyum and H. Dar, "A Survey of Data Mining Techniques for Crime Detection," *University of Sindh Journal of Information and Communication Technology*, vol. 2, no. 1, pp. 1–6, 2018.

[7] H. Benjamin Fredrick David and A. Suruliandi, "Survey on Crime Analysis and Prediction Using Data Mining Techniques," *ICTACT Journal on Soft Computing*, vol. 7, no. 3, pp. 1459–1466, 2017.

[8] H. Hassani, X. Huang, E. S. Silva, and M. Ghodsi, "A review of data mining applications in crime," *Statistical Analysis and Data Mining: The ASA Data Science Journal*, vol. 9, no. 3, pp. 139–154, 2016.

[9] T. Tantawutho, "The computer crime incidents and the future of countermeasures in Thailand," in *2017 Third Asian Conference on Defence Technology (ACDT)*, IEEE, 2017, pp. 97–103.

[10] H. Fatima, G. Dash, and S. K. Pradhan, "Soft Computing applications in Cyber crimes," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, IEEE,2017, pp. 66–69.

[11] J. D. Hawkins and J. G. Weis, "The social development model: An integrated approach to delinquency prevention," in *Developmental and Life-course Criminological Theories*, Tara Renae McGee and Paul Mazerolle, Eds. London: Routledge, 2017, pp. 3–27.

[12] R. F. Sparks, "Criminal opportunities and crime rates," *Indicators of crime and criminal justice: Quantitative studies*, vol. 1, pp. 18–28, 1980.

[13] K. Land, *Criminal circumstance. A dynamic multi-contextual criminal opportunity theory* (New Lines in Criminology Series), Taylor and Francis, 2018, 264 p. ISBN: 9781351524940.

[14] J. Li et al., "Signal-noise identification of magnetotelluric signals using fractal-entropy and clustering algorithm for targeted denoising," *Fractals*, vol. 26, no. 2, p. 1840011 (18 pages), 2018. DOI: https://doi.org/10.1142/S0218348X1840011X.

[15] E. E.-D. Hemdan and D. Manjaiah, "Cybercrimes Investigation and Intrusion Detection in Internet of Things Based on Data Science Methods," in *Cognitive Computing for Big Data Systems Over IoT* (Lecture Notes on Data Engineering and Communications Technologies), Arun Kumar Sangaiah, Arunkumar Thangavelu, and Venkatesan Meenakshi Sundaram, Eds. Springer International Publishing, 2018, pp. 39–62.

[16] W. Elmasry, A. Akbulut, and A. H. Zaim, "Empirical study on multiclass classification-based network intrusion detection," *Computational Intelligence*, vol. 35, no. 4, pp. 919–954, 2019.

[17] P. Mali, J. Sodhi, T. Singh, and S. Bansal, "Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study," *International Journal of Mechanical Engineering and Technology*, vol. 9, no. 2, pp. 110–124, 2018, Article ID: IJMET_09_02_012.

[18] J. Zhao et al., "An "End-Network-Cloud" Architecture Key Technology with Threat Perception and Collaborative Analysis," in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 452, no. 3, IOP Publishing, p. 032091 (6 pages). DOI: 10.1088/1757-899x/452/3/032091.

[19] R. Gifty, R. Bharathi, and P. Krishnakumar, "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection," *Neural Computing and Applications*, vol. 31, no. 1, pp. 23–34, 2019.

[20] D. A. Ziegler, J. R. Janowich, and A. Gazzaley, "Differential impact of interference on internally-and externally-directed attention," *Scientific reports*, vol. 8, no. 1, Article number 2498 (10 pages), 2018. DOI: 10.1038/s41598-018-20498-8.

[21] A. F. Sidiq, R. Umar, and A. Yudhana, "Research on Secure Virus Trojan in Cybersecurity Platform," *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, vol. 5, no. 2, pp. 8–13, 2018. DOI: https://doi.org/10.35968/jsi.v5i2.247.

[22] P. A. A. Resende and A. C. Drummond, "A survey of random forest based methods for intrusion detection systems," *ACM Com-*

puting Surveys (CSUR), vol. 51, no. 3, Article No. 48 (36 pages), 2018. DOI: 10.1145/3178582.

[23] A. Tomlinson, J. Bryans, and S. A. Shaikh, "Towards viable intrusion detection methods for the automotive controller area network," in *2nd Computer Science in Cars Symposium - Future Challenges in Artificial Intelligence Security for Autonomous Vehicles (CSCS 2018)*, (Munich, Germany, 13-14 September 2018), 2018, United States: ACM. DOI: 10.1145/3273946.3273950.

[24] W. Wang, J. Liu, G. Pitsilis, and X. Zhang, "Abstracting massive data for lightweight intrusion detection in computer networks," *Information Sciences*, vol. 433, pp. 417–430, 2018.

[25] C. Chauhan and S. Sehgal, "A review: Crime analysis using data mining techniques and algorithms," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, (5-6 May 2017), 2017, pp. 21–25. DOI: 10.1109/CCAA.2017.8229823.

[26] O. E. Isafiade and A. B. Bagula, *Data mining trends and applications in criminal science and investigations*, IGI Global, 2016, 386 p. DOI: 10.4018/978-1-5225-0463-4, ISBN13: 9781522504634, ISBN10: 152250463X.

[27] J. Lin et al., "Automatic Knowledge Discovery in Lecturing Videos via Deep Representation," *IEEE Access*, vol. 7, pp. 33957–33963, 2019.

[28] S. Caneppele and M. F. Aebi, "Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes," *Policing: A Journal of Policy and Practice*, vol. 13, no. 1, pp. 66–79, 2017.

[29] A. V. Mbaziira and D. R. Murphy, "An empirical study on detecting deception and cybercrime using artificial neural networks," in *Proceedings of the 2nd International Conference on Compute and Data Analysis*, ACM,2018, pp. 42–46.

[30] K. Gajera, M. Jangid, P. Mehta, and J. Mittal, "A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection," in *2019 3rd International con-*

ference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2019, pp. 196–200.

[31] D. Peraković, M. Periša, I. Cvitić, and S. Husnjak, "Artificial neuron network implementation in detection and classification of DDoS traffic," in *2016 24th Telecommunications Forum (TELFOR)*, (Belgrade, Serbia, 22-23 Nov. 2016), IEEE, 2016, pp. 1–4. DOI: 10.1109/TELFOR.2016.7818791.

[32] L. O. Batista et al., "Fuzzy neural networks to create an expert system for detecting attacks by sql injection," arXiv:1901.02868 [cs.AI], 2019.

[33] D. Hassabis, D. Kumaran, C. Summerfield, and M. Botvinick, "Neuroscience-inspired artificial intelligence," *Neuron*, vol. 95, no. 2, pp. 245–258, 2017.

[34] M. Van Gerven and S. Bohte, "Editorial: Artificial neural networks as models of neural information processing," *Frontiers in Computational Neuroscience*, vol. 11, Article number: 114 (2 pages), 2017. DOI: 10.3389/fncom.2017.00114.

[35] I. N. Da Silva, D. H. Spatti, R. A. Flauzino, L. H. B. Liboni, and S. F. dos Reis Alves, *Artificial neural networks. A Practical Course*, Switzerland: Springer International Publishing, 2017, XX+307 p. ISBN: 978-3-319-43161-1.

[36] S. Gong, W. Gao, and F. Abza, "Brain tumor diagnosis based on artificial neural network and a chaos whale optimization algorithm," *Computational Intelligence*, vol. 36, no. 1, pp. pp. 259–275, 2020. First Published: 20 November 2019, DOI: 10.1111/coin.12259.

[37] J. Mendoza and H. Pedrini, "Detection and classification of lung nodules in chest X-ray images using deep convolutional neural networks," *Computational Intelligence*, vol. 36, no. 2, pp. 370-401, 2020. First Published: 04 November 2019, doi: 10.1111/coin.12241.

[38] P. M. Buscema, G. Massini, M. Fabrizi, M. Breda, and F. Della Torre, "The ANNS approach to DEM reconstruction," *Computa-*

tional Intelligence, vol. 34, no. 1, pp. 310–344, 2018. First published: 28 November 2017, DOI: 10.1111/coin.12151.

[39] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, vol. 11, no. 6, ID: e0155781, 2016.

[40] E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, (Yasmine Hammamet, Tunisia, 11-13 May 2016), IEEE, 2016, pp. 1–6. DOI: 10.1109/ISNCC.2016.7746067.

[41] A. Rasmus, M. Berglund, M. Honkala, H. Valpola, and T. Raiko, "Semi-supervised learning with ladder networks," in *Advances in neural information processing systems*, 2015, pp. 3546–3554.

[42] M. Feng, J. Zheng, Y. Han, J. Ren, and Q. Liu, "Big Data Analytics and Mining for Crime Data Analysis, Visualization and Prediction," in *International Conference on Brain Inspired Cognitive Systems*, Springer, 2018, pp. 605–614.

[43] T. G. Proffitt, "The Effects of Computer Crimes on the Management of Disaster Recovery," Ph.D. dissertation, Scholar Works Walden Dissertations and Doctoral Studies, Walden University, 2018. https://scholarworks.waldenu.edu/dissertations/5252.

[44] D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes in View of Computer Science Students," *Procedia - Social and Behavioral Sciences*, vol. 182, pp. 590–595, 2015. DOI: https://doi.org/10.1016/j.sbspro.2015.04.787.

[45] A. J. Rosellini et al., "Using administrative data to identify US Army soldiers at high-risk of perpetrating minor violent crimes," *Journal of psychiatric research*, vol. 84, pp. 128–136, 2017.

[46] X. Li, H. Joutsijoki, J. Laurikkala, and M. Juhola, "Development of crime in England and Wales 1898–2001: Data mining using self-organising map," in *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, IEEE, 2017, pp. 1–8.

[47] H. B. F. David and A. Suruliandi, "Survey on Crime Analysis and Prediction Using Data Mining Techniques," *ICTACT Journal on Soft Computing*, vol. 7, no. 3, pp. 1459–1466, 2017.

[48] G. MeeraGandhi, K. Appavoo, and S. Srivasta, "Effective network intrusion detection using classifiers decision trees and decision rules," *Int. J. Advanced network and application*, vol. 2, no. 3, pp. 686–692, 2010.

[49] S. Lakhina, S. Joseph, and B. Verma, "Feature reduction using principal component analysis for effective anomaly–based intrusion detection on NSL-KDD," *International Journal of Engineering Science and Technology*, vol. 2, no. 6, pp. 1790–1799, 2010.

[50] J. Song, H. Xie, and Y. Feng, "Fast association rule mining algorithm for network attack data," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 20, no. 6–7, pp. 1465–1469, 2017. DOI: 10.1080/09720529.2017.1392464.

[51] P. Natesan and P. Balasubramanie, "Multi Stage Filter Using Enhanced Adaboost for Network Intrusion Detection," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 4, no. 3, pp. 121–135, 2012.

[52] G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, IEEE, 2017, pp. 553–558.

[53] A. Verma and V. Ranga, "On evaluation of network intrusion detection systems: Statistical analysis of CIDDS-001 dataset using machine learning techniques," *Pertanika Journal of Science & Technology*, vol. 26, no. 3, pp. 1307–1332, 2018.

[54] M. Idhammad, K. Afdel, and M. Belouch, "Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest," *Security and Communication Networks*, vol. 2018, Article ID 1263123, 2018. DOI: https://doi.org/10.1155/2018/1263123.

[55] H. Schwarzenbach, A. M. Da Silva, G. Calin, and K. Pantel, "Data normalization strategies for microRNA quantification," *Clinical chemistry*, vol. 61, no. 11, pp. 1333–1342, 2015.

[56] R. Abdulhammed, M. Faezipour, A. Abuzneid, and A. AbuMallouh, "Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic," *IEEE sensors letters*, vol. 3, no. 1, pp. 1–4, 2018.

Abbas Karimi, Saber Abbasabadi,
Javad Akbari Torkestani, Frane Zarafshan

Received April 04, 2020
Revised April 16, 2021
Accepted April 20, 2021

Abbas Karimi
Assistant Professor, Department of Computer Engineering,
Islamic Azad University, Arak Branch,
Arak, Markazi Provience, Iran.
E–mail: Akarimi@iau-arak.ac.ir

Saber Abbasabadei
PhD student, Department of Computer Engineering,
Islamic Azad University, Arak Branch,
Arak, Markazi Provience, Iran.
E–mail: saber.abbasabadey1@gmail.com

Javad Akbari Torkestani
Associate Professor, Department of Computer Engineering,
Islamic Azad University, Arak Branch,
Arak, Markazi Provience, Iran.
E–mail: j-akbari@iau-arak.ac.ir

Faraneh Zarafshan
Assistant Professor, Department of Computer Engineering,
Islamic Azad University, Arak Branch,
Arak, Markazi Provience, Iran.
E–mail: fzarafshan@aiau.ac.ir