Designing an Intelligent Intrusion Detection System in the Electronic Banking Industry Using Fuzzy Logic

Adel Jahanbani
Department of computer, Lamerd Branch, Islamic Azad University, Lamerd , Iran
Email: jahanbani_adel@yahoo.com

Abstract

One of the most important obstacles to using Internet banking is the lack of Stability of transactions and some misuse in the course of transactions it is financial. That is why preventing unauthorized access Crime detection is one of the major issues in financial institutions and banks. In this article, a system of intelligence has been designed that recognizes Suspicious and unusual behaviors for users in the Internet banking system. Because the behavior of different users is accompanied by ambiguity and uncertainty, this system is designed based on fuzzy logic to identify user behavior and categorize suspicious behaviors of varying severity. The system applies a diagnostic process based on KDD data. The results show that in all validation algorithms, 2 to 5 percent improvement in detection is provided.

Keywords: Intrusion, fuzzy logic, detection system, data mining

1. Introduction

With the advent of e-commerce, many economic and industrial sectors have been more or less affected by this promising technology. However, the influence of e-commerce in any industry has not been as tangible as the banking industry. Today, the use of Internet banking is more than an asset, and banks are inevitably required to provide their services electronically to survive and reduce costs. But it seems that it has not been welcomed due to the lack of trust in this service. Considering this point and by studying the factors affecting the adoption of Internet banking [1], it was found that security and trust in the services of these types of banks could have an impact on the intention of using customers from Internet banking services. In fact, these two factors increase the trust of customers, so that trust is a crucial factor in accepting Internet banking. The trustiness of the protection of information refers to unauthorized parties, meaning that no data is available to unauthorized persons [2]. Therefore, one of the key factors in the success of e-banking adoption is to build trust among users through security. On the other hand, the existence of different security models is considered to be the most important obstacle in the technical structure of the electronic banking system. Security in e-banking is important not only for delivering services but also for building trust in users [3]. The importance of easier access to communications without the need for any physical and physical attachment to anyone is unobtainable. The use of wireless internet, mobile phone and its applications in e-commerce, e-banking, e-health, e-judgments, electronic police, information, entertainment and the like are the applications of mobile technologies. Given the widespread use of these technologies, the importance of their security needs will be more evident. Meanwhile, users also need more confidentiality and commitment than ever [4].

Considering the widespread and deep impact of e-commerce on global markets, given the importance of monetary and credit exchanges in every business-economic activity, the tools and platforms for secure and secure exchange of money should also be synchronized with the development of e-commerce. Meanwhile, banks have not been idle for more customers and the expansion and diversification of their services, and they have quickly coordinated with technology and information. Banks in the field of trade developments have paid serious attention to structural changes in secure payment systems and paying the money and creating facilities in the process of service to the customer. In fact, it can be claimed that one of the reasons why public e-commerce has become e-commerce has been the attention of bank managers to the importance and necessity of this phenomenon, which has resulted in their keen interest in providing a safe and secure electronic banking structure.

As a result, one of the essential tools for the realization and expansion of e-commerce is the existence of a secure electronic banking system, which, in keeping with global financial and financial systems, operations and e-business activities will be facilitated. Therefore, detection of crime and improving the level of security in the e-banking industry is far more important than before. Using Machine Learning Algorithms A fuzzy news system is designed to diagnose suspicious behaviors of Internet banking users, and the type of user's performance when confronted with the Internet banking system is considered as the input of the fuzzy system and the output is to classify user behavior so that One of the five categories of normal behavior, a little suspicious, suspicious, very suspicious and dangerous customer.

2. Related Work

There are several methods for detecting crime, unusual behaviors and conflicts with users' laws, and similar investigations have been carried out in various industries, such as healthcare, telecommunications [5], e-mail [6], etc. In addition, various ways to deal with fraudulent practices in Internet banking are noted, which are briefly mentioned below. Electronic banks use different methods for detecting offenses and screening customer transactions.

Yusufzai et al., On the factors influencing e-trust in using e-banking, have presented a study and model for this issue. The model of these researchers focuses on the two perceived security and perceived confidentiality factors, which are effective on the efficiency of the customer's trust. Of course, these researchers have characteristics the credible Bank acceptance, which includes compassion, truthfulness and competence has a positive effect on these two key factors in building trust in customers, which ultimately leads to the desire of users to use e-banking services [7]. In a study on key indicators in electronic banking, the factors influencing e-trust, including perceived security, perceived confidentiality, and perceived service quality are presented [8]. In [9], using neural network for detecting crime in Internet banking has been provided with the help of a learning process and the use of learning collections to construct models of fraudulent Internet banking transactions. In [10], a neuro-fuzziness system has been proposed to find invalid accounts and to predict these accounts, which has made it possible to identify such accounts with a relatively high accuracy. In this article, the history of violations committed in the system as well as information about individuals which have been used to repay their loans.

The main goals of this research are:

- Possibility to establish and maintain appropriate and sustainable security in the sense that all communications are necessary.
- Definition of new abnormalities in the electronic banking network.
- Strengthening the electronic banking network against a variety of suspicious behavior.
- Avoid unnecessary barriers to unsustainable behavior in electricity banking.
- Reduce E-Banking Network with less processing.

3. Fuzzy System Theory

The theory of fuzzy sets provides a method for calculating uncertain and vague data and information, while providing the inference mechanism for reasoning based on a set of rules "if-then"[11]. These rules are defined with the aid of fuzzy sets in which each member of the set of degrees of conscience is between zero and one. A real example of the uncertainty is the ambiguity in the natural language of humans. Fuzzy systems combine the concepts of fuzzy set and fuzzy logic together and provide a framework for providing linguistic knowledge with uncertainty and have two main features that have increased their popularity: one that they have for approximate reasoning, especially for systems It is appropriate to extract a mathematical model from them, and the other is that fuzzy logic allows decisions to be made using incomplete and uncertain information with the help of linguistic variables 2 that can easily be understood by humans.

Fuzzy logic systems consist of four main components are:

- **Fuzzification**: In the process of fuzzing, relations between inputs and linguistic variables are defined using membership functions. In this step, the input values are converted to the degree of belonging to the corresponding linguistic variables. In fact, the input variables become fuzzy numbers through the fuzzy unit.
- **Knowledge base:** The knowledge base comes from the combination of knowledge of the experts in the area under discussion and is formed in the form of rules of linguistic variables. These rules are used to express the connection between input and output fuzzy sets. The grammatical form of a fuzzy rule is expressed as: If (input conditions exist) then (the output result set can be deduced)

- **Inference engine:** This unit is the decision maker of the fuzzy system. An inference engine has the capability of deducing outputs using fuzzy rules and operators, that is, extracting operators such as: minimum, maximum, or sum of fuzzy combinations and outputs from fuzzy sets of inputs and fuzzy relations, and thereby, the ability to make decisions Simulates in humans.
- **Defuzzification:** This is the reverse phase of the fuzzification process. The defuzzifier produces an output with a definite amount of fuzzy sets that output the inference engine.

In this paper, we use a fuzzy inference intelligence system to diagnose suspicious behaviors of Internet banking customers. The design and architecture of the fuzzy system is described in the next section.

4. Fuzzy System Design

In this section, we will introduce an intrusion detection system in E-Banking using fuzzy inference system (figure 1) then we will evaluate this method in a variety of ways.

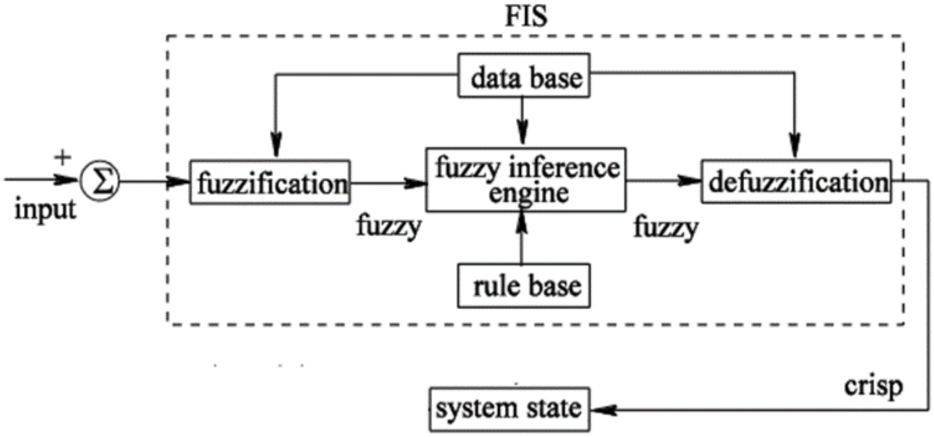

Fig.1. Proposed model

4-1. Electronic banking data set

The study uses the KDD Cup's 99 data set, a standard data set for assessing intrusion detection systems that was provided in 1999[12]. This collection includes information on the connections of the US Air Force's local network, including a wide range of simulated intruders. For each connection in this data set, 41 attributes are defined, which are grouped into four categories of TCP primary attributes, content characteristics, time-based traffic characteristics, and host-based traffic characteristics. Each connection has a label indicating that the connection is normal or one of a variety of attacks. All of these attacks can be divided into four categories:

- Denial of Service attacks (DOS): in which legitimate user requests are not met by the system.
- Remote Raids (R2L): Where a remote machine provides inaccessible access to a local system.

- User-to-root attacks (U2R): In which root user privileges are handled by unauthorized or unauthorized access.
- Probe attacks: which involves scanning and scanning on the system to find ways to penetrate it.

4-2. Types of Derived Features

Among the many features available in the actual connections to the Internet Banking environment, seven effective featuers based on the test and error for our proposed system have been selected as follows.

- User Behavior: Normal behavior refers to those user behaviors that are intruder detection, search, surfing, and doing normal work on the web. If the user is out of the routine and attempts to access the protection pages, it is defined as a user with maladaptive behavior. This feature, which is used as a system output, is divided into Normal, Little Fishy, Fishy, Very Fishy and Abnormal categories to fuzzy it.
- Usage Time: This feature shows the night and day times the user enters the bank's site and intends to use the bank's services, which are divided into ordinary, Usual, Little Unusual, Very Unusual and much Unusual categories in order to fuzzy it.
- Familiarity Level: This feature indicates the level of user familiarity with the site, which is calculated from the time the user is familiar with the bank's site. A user who has long been familiar with the bank's site and uses its services is less mistakenly expected. We divided it into three Unknown, Half-Known and Known categories.
- IP Number: This feature represents the number of different IPs of the user until logged into the registered bank. However, this number indicates the user's suspicion that we divide into three categories, Low, Medium and High.
- Transaction Number: The number of financial transactions that the user has ever performed. This attribute can indicate the amount of user credit on the site. Low, Medium, and High three categories of this parameter are in the direction of its fuzzation.
- Transaction Value: This attribute represents the value of the financial transactions performed by the user so far. Also we have divided it into low, medium and high categories to fuzzy it.
- Login Error: This feature represents the number of errors made by the user when logging in to the site, the more that logically indicates anomalies in the site. To fuzzy it to categories No Error, Low Error, Medium Error, Very Error and Much Error.
- Browser Type: The type of browser used by the user to use the services of the bank as unusual is likely to indicate more suspicion of the user of the site, because today most hackers use misleading intrusion detection systems from unfamiliar browsers. To fuzzy This entry is divided into three Unusual, Half Usual and Usual categories.

These seven parameters are calculated on the basis of the running process calls and the finite state machine (FSM) extracted rules and entered into the fuzzy intrusion detection system. The fuzzy system also creates an alert after executing fuzzy calculations that output the behavior of the user.

4-3. Specifications of the proposed fuzzy system

Below is a summary of the main features of the proposed method implemented in MATLAB software.

- The number of fuzzy sets: eight sets (seven sets for input variables and one for output variables).
- Fuzzification : Triangular and Trapezoid.
- Defazzification: Mean center of gravity
- Fuzzy Detection Engine: Mamadani
- -Fuzzy rules base: Search table.

Based on the specification, the main codes of the fuzzy inference engine of the proposed system in MATLAB software are as follows:

```
[System]
Name='intrusion'
Type='mamdani'
Version=2.0
NumInputs=7
NumOutputs=1
NumRules=295
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
```

4-3-1. Fuzzification

In this step, for each input and output variable, we consider membership functions to convert definite inputs to fuzzy and to be in the fuzzy inference system. Membership functions have several types, such as triangular, trapezoidal, Gaussian, and so on. The fuzzy function used in this experiment is a triangular and trapezoidal fuzzification. In the design of the intrusion detection system for electronic banking, these seven input parameters and one output are fuzzified according to the table 1.

4-3-2. Fuzzy Rules Generation

Fuzzy rules are linguistic IF-THEN-constructions that have the general form "IF A THEN B" where A and B are (collections of) propositions containing linguistic variables. Fuzzy rules are used within fuzzy logic systems to infer an output based on input variables. There are two main methods for determining fuzzy rules: one is to use expert knowledge and the other to use self-organization training, such as modern methods and the neural network, where we use the first method to determine the fuzzy rules.

Of all the existing rules, five different laws have been selected and are presented in Table 2.

4-3-3. Aggregation of Outputs

Since decisions are made on the basis of all rules in fuzzy inference systems, it is necessary to combine the rules in a way to make decisions for decision making. The community is a method by which all sets of outputs of each base are combined into a single fuzzy set.

The input process of the community is a list of output functions that are cut off by the implication process for each rule, and the output is a fuzzy set of outputs. There are different methods of social gathering, most important of which are maximization and aggregation, which is used here in aggregate method.

4-3-4. Defuuzification

Defuzzification is the process of producing a quantifiable result in fuzzy logic, given fuzzy sets and corresponding membership degrees. It is typically needed in fuzzy control systems. Some process of defuzzification is required to convert the resulting fuzzy set description of an action into a specific value for a control variable. There are many different methods of defuzzification available, such as Adaptive integration, basic defuzzification distributions and constraint decision defuzzification that

Table 1. Input and Output Fuzzification

	Range	The membership Function name	Fuzzy Membership Function	Fuzzy values
Login Time (Input)	[0-24]	Usual	Trapezoidal	[7/30, 9,15,19]
		Little-Unusual	Triangular	[17/5, 19/2,22/5]
		Very-Unusual	Trapezoidal	[21,22/15,24, 24]
		Much-Unusual	Trapezoidal	[0, 0, 6, 8/15]
Familiarity Level (Input)	[0-10]	Unknown	Trapezoidal	[0, 0, 1/7, 3/3]
		Half-Known	Triangular	[2, 5 ,8]
		Known	Trapezoidal	[6/4, 8/1, 10,10]
IP Number (Input)	[0-10]	Low	Trapezoidal	[0, 0, 2, 3/5]
		Medium	Triangular	[1/8, 5/2 ,7/9]
		High	Trapezoidal	[5/9, 8, 10,10]
Transaction Number (Input)	[0-100]	Low	Trapezoidal	[0, 0, 19/1, 40/14]
		Medium	Trapezoidal	[14, 32 ,59, 79]
		High	Trapezoidal	[64/7, 82/2, 100,100]
Transaction Value (Input**)**	[0-500]	Low	Trapezoidal	[0, 0, 55/5, 125]
		Medium	Triangular	[76/1, 199/1, 332]
		High	Trapezoidal	[200, 306/9, 500,500]
Login Error (Input**)**	[0-100]	No-Error	Triangular	[0, 2, 4]
		Low-Error	Triangular	[4, 6, 8]
		Medium-Error	Triangular	[8, 18, 20]
		Very-Error	Trapezoidal	[18, 23/8, 32/6, 40]
		Much-Error	Trapezoidal	[30/2, 52, 100, 100]
Browser Type (Input)	[0-10]	Unusal	Trapezoidal	[0, 0, 2, 3/5]
		Half-Usual	Triangular	[2, 4/3 ,6/9]
		Usual	Trapezoidal	[6, 8/2, 10,10]
User Behavior (Output)	[0-100]	Normal	Trapezoidal	[0, 0, 10, 5, 24]
		Little-Fishy	Triangular	[18/6, 28/6, 39]
		Fishy	Triangular	[34/5, 44/5, 54]
		Very-fishy	Triangular	[50/3, 60/3, 70/3]
		Abnormal	Trapezoidal	[64/1, 74, 100, 100]

Table 2. Some fuzzy rules are designed

1	If (Login-Time is Normal) and (Familiarity-level is Half-know) and (IP-Number is Low) and (Transactin-Number is Medium) and (Transaction-Value is Low) and (Login_Error is Low-Error) and (Browser-Type is Normal) then (User-Behavior is Normal) (1)
2	If (Login-Time is Little-Unusual) and (Familiarity-level is Half-know) and (IP-Number is Medium) and (Transactin-Number is Medium) and (Transaction-Value is Low) and (Login_Error is Medium-Error) and (Browser-Type is Normal) then (User-Behavior is Low-Fishy) (1)
3	If (Login-Time is Little-Unusual) and (Familiarity-level is Unknow) and (IP-Number is Medium) and (Transactin-Number is Medium) and (Transaction-Value is Medium) and (Login_Error is Medium-Error) and (Browser-Type is Half-Usual) then (User-Behavior is Fishy) (1)
4	If (Login-Time is Very-Unusual) and (Familiarity-level is Unknow) and (IP-Number is Medium) and (Transactin-Number is Medium) and (Transaction-Value is Medium) and (Login_Error is Very-Error) and (Browser-Type is Half-Usual) then (User-Behavior is Very-Fishy) (1)
5	If (Login-Time is Very-Unusual) and (Familiarity-level is Unknow) and (IP-Number is High) and (Transactin-Number is Medium) and (Transaction-Value is Medium) and (Login_Error is Very-Error) and (Browser-Type is Unusual) then (User-Behavior is Abnormal) (1)

5. Experimental Work

In order to evaluate the electronic banking intrusion detection systems, an evaluation method has been used in which tcpdump files are used within 7 weeks of the DARPA2000 data aggregation data [12].

Each file has been infiltrated as input to detection systems, these systems are configured to have all preprocessors, and their rules activated. An alert file is created for each tcpdump file. Using a help file, the alert file is mapped to the attack list in the tcpdump file. The aid program also reports the negative error rate for each attack and the positive error rate for each base law.

In summary, sensitivity and specificity are in the statistics of two indicators to evaluate the result of a binary classification (double-ended) test [13]. When data can be divided into positive and negative groups, the accuracy of the results of an experiment dividing information into these two categories is measurable and descriptive using sensitivity and attribute indicators. A true positive rate means a proportion of the positive cases, which will test them correctly as positive. A true negative rate means the proportion of negative cases that tests them correctly as negative.

- True Positive (TP): The number of penetration examples that are classified as infiltration.
- True Negative (TN): The number of normal samples categorized as normal.

- False Positive (FP): The number of normal samples classified as infiltration.
- False Negative (FN): The number of penetration samples categorized as normal.

The criteria for assessing the intrusion detection system are based on the following formulas[14]:

$$\text{Sensitivity} = \frac{TP}{TP + FN} \qquad (1)$$

$$\text{Specifity} = \frac{FP}{TN + FP} \qquad (2)$$

$$\text{OverallAccuracy(OA)} = \frac{TP + TN}{TP + FN + \ TN + FP} \qquad (3)$$

In the following, important algorithm s for categorizing the flow of data and the approaches of each of them with different methods and the proposed method for solving the problem of intrusion detection in electronic banking will be evaluated.

5-1. Results based on Ensemble-base algorithm and 8 features selection (seven inputs and one output)

Ensemble learning helps improve machine learning results by combining several models. This approach allows the production of better predictive performance compared to a single model [15]. Ensemble methods are meta-algorithms that combine several machine learning techniques into one predictive model in order to decrease variance (bagging), bias (boosting), or improve predictions (stacking).

The first algorithm examined is the Ensemble-base algorithm. The accuracy of each of the proposed methods is based on 8 characteristics.The table 3 shows different methods. In this table, each of the methods of neural network, data mining, social networking and fuzzy logic has been investigated.

Table 3. Comparison of proposed model with intrusion detection systems based on Ensemble-base algorithm and 8 features.

	Overall Accuracy	***Sensitivity***	**Specifity**	**Duration of Training**	**Duration of Forecast**
Neural Network	89/54	89/35	89/91	/768 741	16/22
Data Mining	88/65	88/12	37/37	560/67	13/33
social networking	88/91	50/44	39/59	341/19	12/009
Fuzzy logic (proposed System)	90/09	91/66	89/55	/334 389	14/97

According to the above table, the accuracy of the proposed method is better than other methods. In the context of the sensitivity of the percentage of the social network, the percentage of data mining and social networking are very low, while the proposed method has earned a decent percentage relative to those methods.

5-2. Results based on On-Demand algorithm

The On-Demand classification method divides the classification process into two components. A component continuously stores statistical information about the flow of data, and the second component continuously uses this statistical information to perform the classification function. Statistical information is presented in the form of microcrystals with specified class labels. This means that each of the microcrystals has a label that defines and delineates the label inside the microcluster. It should be noted that both of the mentioned approach can be used in an online way, and for this reason, this approach can be called an On Demand classification method.

This algorithm applied to any of the methods resulted in a very bad result, which seems to be due to the lack of selection of important features at run-time.

Table 4. Comparison of the proposed model of intrusion detection systems based on the on-Demand algorithm and 8 features

	Overall Accuracy	Sensitivity	Specifity	Duration of Training	Duration of Forecast
Neural Network	87/33	87/10	88/94	678/39	16/44
Data Mining	55/45	57/12	59/33	555/241	17/17
social networking	60/53	58/77	61/62	400/26	16/73
Fuzzy logic (proposed System)	88/00	89/172	90/01	433/19	17/003

Table 5. Comparison of proposed model with intrusion detection systems based on Rule-base algorithm and 8 features

	Overall Accuracy	Sensitivity	Specifity	Duration of Training	Duration of Forecast
Neural Network	91/55	91/39	91/54	800/31	15/676
Data Mining	82/08	81/49	82/26	551/48	14/57
social networking	83/33	82/69	82/92	357/12	16/8
Fuzzy logic (proposed System)	92/59	92/09	92/37	397/73	15/15

According to the table 4, the accuracy of the proposed method is better than other methods. In the context of accuracy and specificity and sensitivity, the percentage of the method introduced by the data mining and social networking method is about 20% better.

In accordance with the table 5, the precision of the proposed method yields better results than other methods, as well as other algorithms. The results of the social network and data mining are very suitable and can be used in the field of detection.

5-3 Results based on Rule-based algorithm

In this algorithm, in order to deal with the concept change problem, it has been attempted to use a classifier that can be subdivided into smaller class floors so that when the concept changes, updating the classifier and adapting it to the new concept has a shorter overhead time [16]. The smallest possible size for a classifier can be a rule only. When the change of concept is due to the change in the concept of a particular area of data, among the existing rules are only certain rules that need to be updated and changed.

This algorithm obtained the best result for the introduced model, so that up to 92% for the result precision section is presented. Due to the use of this algorithm, other methods have also produced appropriate results.

6. Result and Conclusion

The results indicate that the proposed system is capable of detecting normal traffic and unusual traffic and the appropriateness of the proposed structure for a network-based anomaly detection system in electronic banking and the positive effect of using fuzzy logic in improving the performance of systems Diagnosis is abnormal.

The structure and method that we have proposed for the anomaly detection system have all the features presented for a good intrusion detection system:

- We find in the various experiments using the proposed fuzzy logic capability and the use of low-performance network connectivity for the evaluation data set, the sensitivity criterion, the property criterion, and the percentage accuracy in detecting a very acceptable maladaptation.
- The proposed method is less robust than other methods and does not have much processing power, since a small number of features are used for detection.
- The proposed method utilizes the fuzzy logic of the entire automatic and intelligent detection process.
- Also, since in the proposed structure, the decision is made on the basis of a predetermined threshold value, it is possible, with changes in this value, to determine the position of the compromise between the negative and the positive, as desired.

References

[1] Leyla Sarokhi, G. Ali Montazer, “ Designing and Implementing the Smart System for Identifying Suspicious Behavior in Internet Banking Using the Theory of Fuzzy Collections”, Iran Information and Communication Technology Association, 2008.

[2] T. G. Dietterich, Ensemble methods in machine learning, in: Multiple classifier systems, Springer, 2000, pp. 1–15.

[3] Farhad Soleymanian, "Designing and implementing an intelligent system for detecting the behavior of the Internet agent in reducing the fuzzy sets", National Conference on Information Technology and Economic Jihad, 2002.

[4] K. B. Bignell, "Authentication in an InternetBanking Environment; Towards Developing aStrategy for Fraud Detection," in InternetSurveillance and Protection, ICISP'06.International Conference on, Cote d'Azur, 2006, pp.23-33.

[5] G. Kumar, K. Kumar, "Design of an evolutionary approach for intrusion detection", The Scientific World Journal 2013.

[6] G. Folino, C. Pizzuti, G. Spezzano, "An ensemble-based evolutionary framework for coping with distributed intrusion detection", Genetic Programming and Evolvable Machines 11 (2) (2010) 131–146.

[7] L. Lin, R. Zuo, S. Yang, Z. Zhang, "SVM ensemble for anomaly detection based on rotation forest", in: Intelligent Control and Information Processing (ICICIP), 2012 Third International Conference on, IEEE, 2012, pp. 150–153.

[8] A. J. Malik, W. Shahzad, F. A. Khan, "Binary pso and random forests algorithm for probe attacks detection in a network", in: Evolutionary Computation (CEC), 2011 IEEE Congress on, IEEE, 2011, pp. 662–668.

[9] S. Axelsson, "Intrusion detection systems: A survey and taxonomy", Tech. rep., Technical report Chalmers University of Technology, Goteborg, Sweden (2000).

[10] P. P. Angelov, X. Zhou, "Evolving fuzzy-rule-based classifiers from data streams", Fuzzy Systems, IEEE Transactions on 16 (6) (2008) 1462–1475.

[11] A.Angel Cerli and Dr.S.Ramamoorthy, "Intrusion Detection System by Combining Fuzzy Logic with Genetic Algorithm", Global Journal of Pure and Applied Mathematics (GJPAM), 11(1), 2015.

[12] Ozge Cepheli, Saliha Buyukçorak and GuneG Karabulut Kurt," Hybrid Intrusion Detection System for DDoS Attacks", Hindawi Publishing Corporation Journal of Electrical and Computer Engineering, 2016.

[13] Mohamad Nazrin Napiah , Mohd Yamani Idna Idris , Roziana Ramli , Ismail Ahmedy "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol" IEEE Access, 2018.

[14] Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, Robert Atkinson, and Xavier Bellekens, "A Taxonomy and Survey of Intrusion Detection System Design Techniques", Network Threats and Datasets. 1(1) (2018).

[15] K. Remya, J. Ramya, Using weighted majority voting classifier combination for relation classification in biomedical texts, in: Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, IEEE, 2014, pp. 1205–1209.

[16] H. H. Pajouh, G. Dastghaibyfard, S. Hashemi, Two-tier network anomaly detection model: a machine learning approach, Journal of Intelligent Information Systems (2015) 1–14.