IJICTR
International Journal of Information & Communication Technology Research

Volume 12- Number 2 – 2020 (22 -34)

Implementation of Intrusion Detection Systems in order to Detect Phishing in the Banking Industry

Abdullah Sahifa
Science and Research Branch
Islamic Azad University
Tehran, Iran
abed.sahifeh@gmail.com

Mohsen Gerami*
Faculty member of ICT Faculty
Faculty of Post and Communications
Tehran, Iran
gerami@ictfaculty.ir

Received: 14 October 2019 - Accepted: 23 January 2020

Abstract—**Implementation of intrusion detection techniques in banking transactions in order to prevent fraudulent banking systems, especially electronic banking systems, is inevitable. The purpose of this research is to implement intrusion detection systems to detect phishing in the country's banking industry. In this regard, in this research, in order to protect banking information systems due to the combination of different IDS implementation methods in order to detect phishing and also the need to use PHISHING.IDS + ANFIS system by using Matlab programming environment, in order to increase trust. Also, the issue of the need for multiple expertise has been explored by simultaneously applying the knowledge of several experts in different fields to solve the problem of IDS implementation in order to detect phishing. In the present research, a neural-fuzzy inference system for the implementation of intrusion detection systems for phishing detection in the banking industry using the approach of artificial neural networks and fuzzy system, called PHISHING.IDS + is presented by ANIS program. In order to design a neural-fuzzy inference system and implement IDS in order to detect phishing, the most important outputs of statistical software are examined and analyzed in detail.**

Keywords—Intrusion Detection Systems (IDS); Phishing; The country's banking industry; Artificial Neural Networks; Distributed intrusion detection.

I. INTRODUCTION (HEADING 1)

Given the importance of comprehensive banking systems and in order to maintain stability in service delivery and ensure the security of their valuable data, the implementation of "intrusion detection and prevention systems (IDS / IPS)" capable of detecting, recording events and even responding to attacks [1] and [2]. It is considered as one of the main architectural solutions of bank information technology network security [3]. Also, due to the incorrect implementation of intrusion detection and prevention systems, operational risks in the field of bank information technology services, due to the deviation in identifying normal to abnormal traffic, will be accompanied by a system [4]. With banking services and systems, in addition to reducing these risks, it can contribute to greater security in the field of electronic banking [1]. In fact, in the present research, a neural-fuzzy inference system is proposed to implement intrusion detection systems for phishing detection. Considering the importance of the subject of phishing in the flaw of the security of the World Wide Web, and according to criteria such as the detection of distributed intrusion;

* Corresponding Author

Host-based intrusion detection; Signature-based recognition; Schedule network-based intrusion detection and analysis in JavaScript and HTML-based intrusion detection and features, URL-based features, address bar-based features, network-based networking features, and network-based networking features. The importance and necessity of such research can be pointed out to professors and students in the fields of network security and banking to decide on the implementation of intrusion detection systems in order to detect phishing in the country's banking industry.

II. RESEARCH BACKGROUND

Internal research background

In the research [5], after identifying the common types of fraud in the field of bank cards and simulating fraudulent transactions, using artificial neural networks, a model for classifying transactions into healthy and fraudulent transactions was created (fraudulent and fraudulent transactions). This model, which is a type of RBF neural networks, in addition to being based on the domestic banking system of the country, has been able to perform relatively well in this classification with high accuracy. The Single Value Decomposition (SVD) algorithm was also used to improve the classification performance. Comparison of performance evaluation criteria presented in this paper and the results of the base models showed that the proposed method has a much better performance than the base models.

The research [6] was conducted with the aim of increasing the accuracy of intrusion detection system using a combination of PSO and SVM algorithms. KDDCup99 data related to types of attacks were used. In the first stage, the data were classified only using the SVM algorithm. With the proposed method, we were able to increase the surroundings by reducing the feature to more than 95%.

In research [2], we have proposed an intrusion detection system with three layers of detection that uses both signature-based and anomaly-based methods. The first layer uses some rules to detect some intrusions that are very similar to normal samples. The second layer uses clustering to detect input samples that are closer to the center of the abnormal cluster than the center of the normal cluster as infiltration. The two cluster centers are calculated by a genetic algorithm. The third layer also detects intrusions using a random forest classifier. Experiments performed on the NSL-KDD dataset and compared with the recently published results using this dataset demonstrate the effectiveness of the proposed intrusion detection system.

In research [7], using data mining algorithms, we identify phishing websites. By applying the data in the UCI database, including 30 attributes of web pages such as URL and IP address, to two standard cuckoo and adaptive cuckoo evolution algorithms, we reduce the number of attributes to nine. Also, using the Bagging algorithm as a classifier and with reduced dimension data, we identify phishing websites with 93.33% accuracy. Comparing the obtained result with the existing methods in this field, the superiority of the proposed method is obvious.

In research [8], it was investigated that the techniques of reducing the alarms produced by the intrusion detection system, while attracting the attention of many researchers, have also led to many researches. The main purpose of the research is to reduce false alarms and research the root causes. In this paper, the optimal solution to reduce false alarms in intrusion detection system using support vector machine is stated. The results of this research will improve the percentage of false alarms.

In research [9], a self-learning (STL) based learning approach was proposed for the effective and flexible implementation of NIDS using deep learning based on dynamic convolution neural networks (DCNN). To test and evaluate the proposed method, the NSL-KDD standard data set was used to detect network intrusion. We also compared the performance of the proposed method with the basic methods in terms of accuracy, readability and F-measurement. Experimental results showed that the proposed method has a better performance than the basic method.

In research [10], it was investigated that intrusion detection system is used independently (such as (Snort or with various security equipment (such as Antivirus, UTM, etc.) in the network and based on two techniques of detecting abnormal behavior and detection. Signature-based detection can detect the occurrence of an attack. Currently, most research on intrusion detection systems in the field of detection is based on abnormal behavior and using various techniques (statistical, artificial intelligence, data mining, learning). In this research, we were able to achieve an effective degree of Accuracy by selecting a candidate class from the KDD dataset features and the deep learning technique.

The research [11] conducted a study entitled "Phishing detection using URL-based and anomalous features" which had two general phases. In the first phase, appropriate features are extracted and in the second phase, classification is performed. The features extracted in the first phase are divided into 4 groups based on the address bar, anomaly, domain and JavaScript. By including valid and appropriate features, the classification operation is performed in the second phase. By experimenting with stochastic forest classifiers, Bayesian, perceptron neural networks, and support vectors, they concluded that stochastic forest had the best performance.

The research [12] described several network methods in the field of intrusion detection and how such systems work, the ability and flexibility of these systems to implement a variety of neural networks without an observer. Which network is superior to other networks in terms of efficiency and accuracy? The results show that both networks are able to detect DOS and PROBE attacks well. It has a very high speed and low response time, which makes it suitable for real-time intrusion detection systems in high-traffic computer networks.

The research [13] conducted a study entitled "Classification and identification of phishing websites using a set of fuzzy rules and a modified slope optimization algorithm". First, it defines a mechanism

based on the design of a change threshold to flexibly reduce the features being evaluated in identifying phishing websites. Then, by memorizing the sloping page optimization algorithm, softly reducing the effect of memory on the algorithm performance in high iterations, and defining 12 fuzzy rules in a fuzzy inference system, we can intelligently effective this algorithm in order to classify and classify it according to web classification. .

The research [14] presented a research with an approach to identify and predict phishing websites using classification algorithms based on web page characteristics, which has a lower error rate than other similar techniques against phishing scams. . In this approach, the features that can be used to identify phishing pages are weighted based on the effect of identifying these attacks. Compared to other similar methods before.

The research [15] presented a research to identify phishing websites in electronic banking with fuzzy logic. And states that in general the information marketing process consists of two stages. The first step is probabilistic retrieval models that calculate the relationship between the user's need for information and each of the documents in the collection. The second stage focuses on how to rank the calculated documents.

In research [1], it was investigated that the customization of Snort intrusion detection system is described by determining the correct signature of detection of attacks related to the vulnerability of existing systems and known attacks with the purposes of online banking services. The Darpa1999 dataset is used as a standard data to evaluate accepted intrusion detection systems to adjust the results of the analysis of test data, the performance of the Snort intrusion detection system recommended for banking systems in comparison with the default Snort system.

In research [16], the results show that using a machine learning algorithm such as ART neural networks is an efficient method in detecting phishing emails using URLs, but it is not practical, also in recognizing and using text. Email also has a better performance than the genetic algorithm, but because the decision tree is legal if it works then and there are no ambiguous steps, the implementation of the decision tree is preferred.

In research [17], it was investigated that fraudsters use the password and username of the user to enter the site. This article first examines the cases of phishing that have occurred so far in financial institutions and banks. Then, by examining the challenges in the security of online systems, solutions in three areas of customer, financial and credit institutions and the use of new technologies are presented. As a result, the necessary training and implementation of new technologies will reduce phishing crimes.

In research [18], the intelligent system for faster and more efficient detection of these websites has been studied using fuzzy set classification and AHP_TOPSIS combination decision-making method. First, a brief description of information retrieval and data mining is given, and finally a comparison is made between decision-making methods and fuzzy logic techniques to detect these attacks using fuzzy rules and layers, as well as their criteria and components.

In research [19], a new and innovative framework for dealing with phishing websites based on random networks has been presented. If both random networks are available, the security image can be restored to its original state.

In research [20], using the distinguishing parameters of a secure website from a phishing website, an expert system has been developed to detect these types of attacks in e-banking. Parameters are categorized into six different sections, including website domain characteristics, security and encryption used, script code on the page, page content and appearance, web page address, and site behavioral features. By combining different extractable values, forming a knowledge base, and evaluating all possible scenarios, the system is able to reason about the degree to which a website is suspicious of a phishing website. In order to check the validity and efficiency of the system, the output was evaluated based on real values from the PhishTank site, and acceptable results were obtained to identify this type of attack in comparison with other existing systems in this field.

In research [21], it was investigated that due to the recent developments in today's port banks, banks have become more and more dependent on information technology, which has led to its risks related to network security risks. This paper tries to provide a conceptual framework for managing network security in this convergent environment between allied and stakeholder banks. Also, at the end, the relationship between the issues raised and the strategic document on space security of the country's information exchange (EFTA) is examined.

External research background

The research [3] found that although software banks are launching new products that use a blacklist of exploratory, visual, and machine-learning methods, these products cannot prevent all attacks. In this paper, a real-time anti-phishing system, which uses seven different classification algorithms and features based on natural language processing (NLP), is proposed. This system has the following distinctive features from other studies in the literature: language independence, use of large-scale legal data, real-time implementation, identification of new websites, independence from third-party services, and use of feature-rich classifiers. To measure system performance, a new data set is created and experimental results are tested on it. Based on the experimental results and comparisons of the implemented classification algorithms, the random forest algorithm with only NLP-based features provides the best performance with 97.98% accuracy for detecting phishing Internet addresses.

The research [22] found that we've all heard stories that start with someone receiving an email that requires an immediate invoice review or password change, and breaking information that compromises personal information and loses money. It ends. Although many of us may open our eyes to the idea of falling because of such an internet scam, we must acknowledge that if that internet scam does not work, malicious actors will

not prevent many people from e-mailing their bank details. Take action, education is clearly still needed for the silent majority who still click on it. People continue to respond to the deception of the Internet and the hackers who still benefit from it. This research provides Internet deception guidelines on how not to get caught.

The research [23] found that to examine phishing emails, we used a social impact framework and used phishing emails to scale persuasion strategies within the persuasion process model. A total of 985 participants participated in this research. The results showed that emails using the principles of scarcity and social proof were the least successful, while those that used the principles of coordination and reciprocity were more successful. The same principles were considered according to the scale of persuasion strategies. For the most part, participants who were prone to a particular principle were significantly more likely to receive emails containing that principle. The results further revealed that age; Percentage of time spent by the computer; Sensitivity to the principle of social proof; And, co-location are significant predictors of individuals' ability to detect non-phishing emails. The practical implications of these findings are also discussed for the future.

The research [4] found that the limitation of this approach is that it breaks down when the server host phishing page is compromised. In addition, this leads to low negative rates when new domains are registered or unpopular. Therefore, in this paper, we present an application called Jail-Phish that improves the accuracy of search engine-based methods by being able to detect phishing sites hosted on common servers (PSHCS) as well as identifying newly registered legitimate sites. . Jail-Phish compares the suspicious site and the synchronous domain in the search results to calculate the similarity score between them. On some pages of the same website, there are some similarities such as logos, favions, images, scripts, styles and links, while on the other hand, the differences in pages on PSHCS are very large. Therefore, we use the similarity score between the suspicious site and the matched domain as a parameter to diagnose PSHCS. From the experimental results, it has been observed that Jail-Phish with 98.61% accuracy, 97.77% positive real rate and less than 0.64% false positive rate.

In the research [24], it was investigated that we present an accumulation model for identifying web pages using Internet address and HTML attributes. In terms of features, we design a lightweight, HTML URL and, without the use of third-party services, introduce HTML strings without the use of third-party services, allowing for the development of real-time tracking programs. In addition, we design an accumulation model combining GBDT, XGBoost, and LightGBM in multiple layers that enable different models to complement each other, thus improving phishing authentication performance. Specifically, we collect two real datasets for evaluation: 50 K - PD and 50 K - IPD, respectively. 50 K - PD includes 49, 947 web pages with Internet and HTML code. 50K - IPD contains pages 53, 103 with screenshots in addition to web and HTML code. The proposed method operates on multiple criteria compared to several machine learning models, with 97.30% on accuracy, 4.46% on missed warning rate, and 1.61% on 50 K-PD false alarm rate. In the 50K IPD data set, the proposed method achieves 98.60% on accuracy, 1.28% on missed alarm rate, and 1.54% on false alarm rate.

In research [25], it was found that these days phishing is done by real-time tools (RT) and control relays (CR) in intermediate attacks (MITM) or by malicious extensions. User authentication schemes are either unable to control phishing attacks or are complex to learn and use, or require users to use and purchase additional hardware such as a security key. In this article, we propose a new anti-phishing security authentication scheme that uses the Bluetooth address of the user's smartphones to identify the user along with the user password for authentication. Analysis of our test results shows that the proposed design is safe against RT and CR air strikes and attacks carried out through malicious extensions. It is also effective in memory usage and CPU usage. Comparison of the proposed design with existing designs in the field of usability and implementation shows that it is better than other designs.

The research [26] found that many anti-phishing solutions have been proposed for mobile devices to date, but there is still a lack of a complete fledge solution. The main purpose of this article is to make a detailed analysis of attack techniques and defense mechanisms. We present this article in four sections. First, we talk about mobile phishing attacks, their history, attackers' motives, and smartphone security concerns. Second, we analyze phishing attacks and provide a similar classification. Third, we provide a taxonomy of the recently proposed solutions that detect and protect users from mobile phishing attacks. Fourth, we talk about the different issues and challenges that researchers face when confronted with phishing attacks. In addition, we have discussed the evaluation and evaluation matrices used by researchers to evaluate their approaches.

In the research [27], it was investigated that in this research, a new framework has been presented that combines neural networks with amplifier learning to detect phishing attacks online for the first time. The proposed model demonstrates its ability to create a new phishing email recognition system that demonstrates changes in newly studied behaviors, which is done by adopting the idea of reinforcing learning to dynamically enhance the system over time. The proposed model solves the problem of limited data sets by automatically adding more emails to the offline data set online. A new algorithm is proposed to detect any new phishing behavior in the new dataset. By careful testing using known datasets, we show that the proposed technique can achieve zero-day phishing attacks with high performance levels of high accuracy, TPR and TNR of 98.63%, 99.07% and 98.19%, respectively. FPR and FNR are low at 1.81% and 0.93%, respectively. Comparison with other similar techniques in a data set shows that the proposed model is superior to the existing methods.

In the research [28], in order to analyze the effect of deterrents and norms related to resistance to information systems security, it was examined that non-compliance is mainly due to resistance to information

security policies. Much of this research, based on the theory of rational practice, examines whether employees' intention to comply with information systems security policies is a good predictor of their behavior. This research argues that employees' compliance with information systems security policies is usually enforced within banks, and that non-compliance is primarily due to resistance to these policies. This research examines the role of banking sanctions and banking norms in influencing employee resilience to information systems security policies. Data were collected from 133 people from 10 banks in four industries and the hypotheses were tested and confirmed using PLS-SEM analytical method. The results show that ethical and descriptive norms are useful for reducing resistance.

In the research [29] with the aim of analyzing personal data management systems from a security and performance perspective was examined. we do. From this analysis, we derive a general set of security features and security requirements that any personal data management system (PDMS) should consider. We then identify the challenges of implementing such a system and propose a preliminary design for a complete and comprehensive reference architecture that meets the requirements. Finally, we discuss several important research challenges to explore for a mature PDMS ecosystem.

The research [30] aimed at providing a built-in, service-based system for information security applications. To provide a complete data protection mechanism, we propose an embedded service-based system (ASOS) design. Access control policies are implemented as protection matrices and are designed in hardware; therefore, the method of accessing information is specific and not public, so that the risks of illegal access to information can be reduced. A layered and layered design method has also been introduced to increase its scalability. In addition, it has a system compliance manager who can dynamically adapt its hardware functions to support application requirements. Experiments show that compared to a pure software-based design, it can have an access time of 8.75. Compared to a built-in system design that contains 13 hardware functions, ASOS can reduce 26.42% cuts and 25.81% cuts in a Virtex.

The research [31] aimed to analyze the impact of the relationship between internal auditing and information security performance on the consequences of information security, which has become vital for banks to manage network security risk due to the increasing financial impact of cybercrime. The professional literature has long argued that the practice of internal auditing (IAF) can play an important role both in ensuring respect for network security and in providing insights on how to improve bank network security. However, there is little empirical evidence to support this belief. Using a unique data set, this research examines how the quality of the relationship between internal auditing and information security performance affects the objective criteria for the overall effectiveness of the bank's information security efforts. The quality of this relationship has a positive effect on the number of reported internal control weaknesses and incidents due to non-compliance, as well as the number of security incidents revealed before and after the material damage to the bank. In addition, we found that higher levels of management support for network security and having a senior information security officer (CISO) report independent of IT performance had a positive effect on the quality of the relationship between internal audit and information security performance.

In research [32] aimed to analyze the acceptance of the Electronic Document Management System (EMRS) in network security management awareness and perceived service quality, since network security management (ISM) awareness enables health workers to act on security breaches. This research investigates the effect of perceived service quality on the relationship between knowledge of network security management and perceived service quality on improving service quality in the post-acceptance phase. In particular, the results show that with sufficient technical support and high awareness, the quality of information system features can be increased, which in turn increases the desire of users to continue to use the system to advance their therapeutic work, but must with knowledge and Knowledge of network security management policy formulation and its effective implementation should be considered. Therefore, a successful adoptive parent should be well-connected with the network security management policy and adequate technical support, and both technical and managerial aspects should be fully considered and effectively integrated for the best outcome.

The research [33], presented, stated that many intrusion detection models do not offer a real-time solution to the barrier. And proposed a light intrusion detection system to detect DOS and DOS attacks. The most important feature set was selected using the Enhanced Use of Information (IG) feature selection filters, and the Correlation Based Feature Selection (CFS) filter. In addition, four machine learning methods, C4.5, NB, and Random Forest (RF), show good detection results and false-positive rates for probe attacks. Processing time is also optimized when it is evaluated using the best set of features.

The research [26] presented and provided solutions for users to identify and dispose of them. They also studied the data set and evaluation used by researchers to evaluate approaches.

In research [34] used a matrix to assess the realistic quality of an intrusion detection system. Their results show that the realistic attack behavior and natural dynamics of real-world networks are included in NGIDS -DS. NGIDS-DS is a marked network that generally shows the critical cyber infrastructure of various banks in both normal and abnormal states.

The research [35] presented and developed phishing attacks and anti-phishing techniques not only in traditional environments such as emails and websites but also in new environments such as mobile sites and social networks. And proposed a classification that includes attacking techniques, countermeasures, targeted environments, and communication media. Classification not only provides guidance for designing effective techniques for detecting and preventing

phishing in different environments, but also helps practitioners evaluate and select tools, methods, and features to address specific types of phishing problems.

The research [36] conducted a study entitled "Providing an efficient neural-fuzzy approach to detect phishing" and stated that they presented a new and effective method for identifying phishing sites. In this proposed method, neural-fuzzy and exploratory networks have been used. And the results show that it can detect more than 99% of phishing sites. It can also be used more with large data sets and exploratory parameters.

In research [37] categorized an exploratory method that uses only address information. It first uses a number of scripts to collect secure and phishing addresses. Then, it uses machine learning methods to build models for educational data. Considers classes as binary, with phishing addresses belonging to the positive class and harmless addresses belonging to the negative class.

In research [38] worked on features such as spelling errors, long URLs, prefixes and suffixes. The use of multi-class classification algorithm based on association rules was one of the strengths of this method.

The research [39] focused on phishing detection using fuzzy data mining in e-banking. First, fuzzy sets are formed using the extraction of rules. Then, fuzzy is performed and the corresponding classifier is used. The final step is the fuzzy return of exact values instead of fuzzy values.

III. THEORETICAL FRAMEWORK

The following variables will be used in the implementation of intrusion detection systems for phishing detection. The following table presents the theoretical framework of the research in order to design a neural-fuzzy inference system for the implementation of intrusion detection systems in order to detect phishing in the country's banking industry using the approach of artificial neural networks and artificial systems.

TABLE I. THEORETICAL FRAMEWORK OF THE RESEARCH

Phishing [11],[13], [36] and [14] and [26], [35] and [3] and [27] and [4] and [7]	Infiltration detection systems [40], [41], [12], [33] and [34]. And [3] and [27]
JavaScript and HTML based features	Distributed intrusion detection
URL-based features	Host-based intrusion detection
Address bar based features	Signature-based recognition
Abnormal features	Schedule analysis and diagnosis
Behavioral features of the site	Network-based intrusion detection

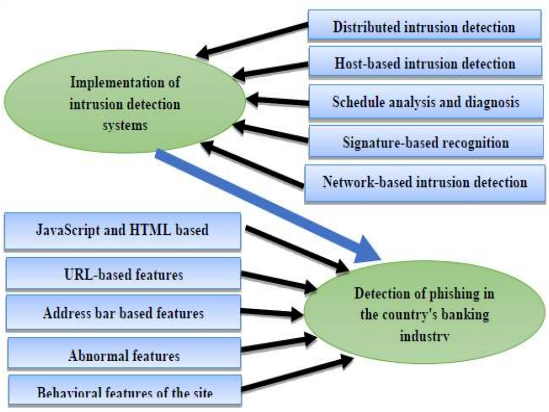

Figure 1. Conceptual model of implementation of intrusion detection systems in phishing detection inspired by research [41], [12], [33] and [34] And [3] and [27] and [11], [13], [36] and [14] and [7].

In fact, after reviewing the theoretical foundations of the research and reviewing the research background, it was found that conducting this research to prevent network security problems in the banking industry on scheduling issues of penetration analysis and detection, signature-based detection, penetration-based penetration detection. And host-based intrusion detection, as well as the lack of a system to provide advice to the manager to decide on the implementation of intrusion detection systems to detect phishing, can lead to the innovation of the present research to bridge the gap. In fact, given the weaknesses in the implementation and application of intrusion detection systems in the banking industry, we can hope for results and innovations in such research.

IV. STATISTICAL ANALYSIS OF RESEARCH DATA

Here, mean, standard deviation, skewness (asymmetry) and correlation were used to statistically describe the research data. The table of descriptive information shows the variables and indicators of the research, based on the number of data, minimum, maximum, average, standard deviation and skewness. Among the answers of experts in the field are:

TABLE II. DESCRIPTIVE INFORMATION ON THE IMPORTANCE OF RESEARCH VARIABLES

Research Indicators	Number of	minimum	maximum	mean	standard deviation	statistic skewness
Signature Detection (X1)	60	3	7	5.10	.838	.165
Specify signature image noises	60	4	7	5.43	.767	.464
Remove signature image noise	60	3	7	5.23	.963	.214
Identify fake signatures	60	4	7	5.57	.810	.568
Network-based intrusion detection (X2)	60	3	7	5.50	1.097	.000

Network Security Management Gap Analysis	60	1	7	5.17	1.278	-.928
Creating a strategy to facilitate the network security management program	60	3	7	5.43	.998	.084
Detect intra-network attacks	60	4	7	5.57	.851	.297
Detection of extranet attacks	60	3	7	5.27	.936	.202
Distributed Intrusion Detection (X3)	60	3	7	5.20	.840	-.043
Influence process distribution	60	3	7	5.10	.838	.165
Distribution of influence data	60	4	7	5.43	.767	.464
Influence temporal distribution	60	3	7	5.20	.798	-.380
Infiltration hardware distribution	60	4	7	5.60	.887	.290
Host-based intrusion detection (X4)	60	3	7	5.47	1.033	.092
Recognize the behavioral characteristics of the site	60	4	7	5.53	.853	.401
Identify abnormal features	60	3	7	5.43	1.064	.093
Recognize features based on JavaScript and HTML	60	4	7	5.80	.917	.142
Identify attributes based on address bar and URL	60	4	7	5.53	.853	.401
Intrusion Analysis and Detection Schedule (X5)	60	4	7	5.60	.867	.245
Licensing methods	60	4	7	5.77	.890	.186
Authentication methods	60	4	7	5.78	.885	.143
Prevention methods (resistance)	60	4	7	5.77	.890	.186
Response methods	60	3	7	5.43	.998	.084

As can be seen, based on the opinions and professional experience of managers and senior experts of the country's banking industry as well as the opinions of university professors, the most important criteria related to signature recognition processes (X1), network-based intrusion detection (X2), intrusion detection (X3)), Host-based intrusion detection (X4) and intrusion analysis and intrusion detection (X5) scheduling are: Detection of forged signatures with an average of 5.57; Detection of intra-network attacks with a mean of 5.57; Detection of extranet attacks with a mean of 5.57; Intrusion hardware distribution with an average of 5.60; Recognize features based on JavaScript and HTML with an average of 5.80; And authentication methods with an average of 5.78; Were calculated. Ranking of research variables based on the weighted average of their indicators are: Host-based intrusion detection with a weighted average of 5.5863, Mohawk analysis and intrusion detection with averaged 5.5325, Mohsen-centered intrusion 5.3325 and detected distributed intrusion with a weighted average of 5.306. Other analyzes related to descriptive statistics of research data can be examined in the table above. In fact, the data of this research are in good condition in terms of symmetry and aggregation. In fact, the main reason for analyzing the reliability of the data collection tool of this research is to what extent the measurement tool gives the same results under the same conditions and that the correlation between one set of answers and another set of answers in an equivalent test that How much is an independent form obtained on a group of subjects? The table related to the reliability statistics of research variables according to the number of items of measurement tools, shows high reliability of the measurement tools of this research:

TABLE III. INFORMATION ON THE RELIABILITY STATISTICS OF RESEARCH VARIABLES

Reliability of IDS implementation variables for phishing detection	Cronbach's alpha	Number of items
	0.935	24

Here, Cronbach's alpha for the research variables is greater than 0.9, indicating that the reliability of the IDS implementation modeling tool for phishing detection is excellent. Then, in order to investigate the effect and effectiveness between the function (dependent) variable and the independent variables, the correlation coefficient based on the research variables is used:

TABLE IV. CORRELATION BETWEEN RESEARCH VARIABLES

Correlation between research variables		**Signature-based detection (X1)**	**Network-based intrusion detection (X2)**	**Distributed intrusion detection (X3)**	**Host-based intrusion detection (X4)**	**Analysis scheduling and intrusion detection (X5)**
Signature-based detection (X1)	Correlation	**1**	**.646**	**.887**	**.572**	**.476**
	Sig.		**.000**	**.000**	**.000**	**.000**
Network-based intrusion detection (X2)	Correlation	**.646**	**1**	**.589**	**.209**	**.178**
	Sig.	**.000**		**.000**	**.108**	**.173**
Distributed intrusion detection (X3)	Correlation	**.887**	**.589**	**1**	**.438**	**.298***
	Sig.	**.000**	**.000**		**.000**	**.021**
Host-based intrusion detection (X4)	Correlation	**.572**	**.209**	**.438**	**1**	**.477**
	Sig.	**.000**	**.108**	**.000**		**.000**

Analysis scheduling and intrusion detection (X5)	Correlation	.476	.178	.298 *	.477	1
	Sig.	.000	.173	.021	.000	

As can be seen in the table above, the correlation between the research variables. Since the correlation coefficient sign is the slope of the regression line, there is a positive and relatively significant relationship between signature-based detection (X1) and host-based intrusion detection (X4). The correlation coefficient between them is calculated to be 0.572. On the other hand, there is a positive and significant relationship between signature-based detection (X1) and distributed intrusion detection (X3), because the correlation coefficient between them is calculated to be 0.887. There is a positive and significant relationship between signature-based detection (X1) and network-based intrusion detection (X2), because the correlation coefficient between them is calculated to be 0.646. On the other hand, there is a positive and significant relationship between distributed intrusion detection (X3) and network-based intrusion detection (X2), because the correlation coefficient between them is calculated to be 0.589. In fact, due to the high correlation between the variables and research indicators, ie the signature recognition variable based on (X1) includes indicators such as: identifying signature image noise, removing signature image noise and the existence of fake signatures; Network-based intrusion detection variable (X2) includes indicators such as: analysis of network security management gaps, creating a strategy to facilitate network security management program, intra-network attack detection and extranet attack detection; Distributed intrusion detection variable (X3) includes indicators such as: intrusion process distribution, intrusion data distribution, intrusion time distribution and intrusion hardware distribution; Host-based intrusion detection variable (X4) includes indicators such as: site behavioral features detection, JavaScript and HTML based feature detection, address bar and URL based feature detection; And Intrusion Analysis and Detection Schedule (X5) includes indicators such as: licensing methods, authentication methods, prevention methods (resistance), response methods (reactive), can be the management of the network industry in the bank network Improved the country's banking.

V. PHISHING.IDS + ANFIS SYSTEM DESIGN

In the present research, the neural-fuzzy inference system for implementing IDS to detect phishing using Matlab programming environment, called PHISHING.IDS + ANFIS is presented for the first time in a related research field. In fact, the PHISHING.IDS + ANFIS system is a system whose input information can be inaccurate, ie the input information of a fuzzy system is in the form of fuzzy sets or fuzzy numbers. On the other hand, the processing of a fuzzy system can be done inaccurately. One of the most famous and practical inaccurate processes in fuzzy systems is the use of fuzzy law database. In the fuzzy law database, each law is defined by an "if-then" structure. Considering the application of neural-fuzzy inference system designed in this research, at the end of the five steps for designing neural-fuzzy inference system to implement IDS in order to detect phishing were considered, which are:

Step 1: Identifying the input and output variables of the system - After finalizing the conceptual model of the neural-fuzzy inference system of the research, the input and output variables of the neural-fuzzy inference system were defined. The input variables of the neural-fuzzy inference system for implementing IDS to detect phishing are: First input variable: Signature-based signature detection status (X1); Second input variable: network-based intrusion detection (X2); Third input variable: Distributed intrusion detection (X3); Fourth input variable: host-based intrusion detection (X4); Fifth input variable: Schedule analysis and intrusion detection (X5); And the output variable of the neural-fuzzy inference system of the research is the status of "bank network security management in detecting phishing attacks (Y)" in the country's banking industry. According to the conceptual model of the research and also applying the opinions of experts to evaluate that model, the input and output variables of the neural-fuzzy inference system can be shown as follows:

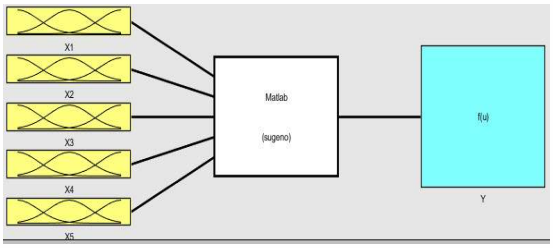

Figure 2. Model of input variables of the module "Improving Bank Network Security Management in Detecting Phishing Attacks".

Step 2: Define qualitative variables by using linguistic constraints and assigning fuzzy numbers and sets and membership functions to them - Table and form of language variables, fuzzy values as well as membership functions of triangular numbers and trapezoids related to input variables and output variables The research is presented in threes and fifties:

TABLE V. LINGUISTIC VARIABLES RELATED TO THE OUTPUT VARIABLE OF THE MODULE "IMPROVING BANK NETWORK SECURITY MANAGEMENT IN DETECTING PHISHING ATTACKS

Triangle number membership functions	Linguistic variable
(0/3 0/15 0)	Low
(0/7 0/5 0/3)	Medium(normal)
(1 0/85 0/7)	High
ANFIS system training data	
0,0,0,0,0,0	
0-0.025,0-0.025,0-0.025,0-0.025,0-0.025,0.05	
0.025-0.05,0.025-0.05,0.025-0.05,0.025-0.05,0.025-0.05,0.1	
0.05-0.075,0.05-0.075,0.05-0.075,0.05-0.075,0.05-0.075,0.15	
0.075-0.10,0.075-0.10,0.075-0.10,0.075-0.10,0.075-0.10,0.2	
0.10-0.15,0.10-0.15,0.10-0.15,0.10-0.15,0.10-0.15,0.25	
0.15-0.25,0.15-0.25,0.15-0.25,0.15-0.25,0.15-0.25,0.3	

0.25-0.30,0.25-0.30,0.25-0.30,0.25-0.30,0.25-0.30,0.35
0.30-0.35,0.30-0.35,0.30-0.35,0.30-0.35,0.30-0.35,0.4
0.35-0.4,0.35-0.4,0.35-0.4,0.35-0.4,0.35-0.4,0.45
0.40-0.45,0.40-0.45,0.40-0.45,0.40-0.45,0.40-0.45,0.5
0.45-0.5,0.45-0.5,0.45-0.5,0.45-0.5,0.45-0.5,0.55
0.50-0.55,0.50-0.55,0.50-0.55,0.50-0.55,0.50-0.55,0.6
0.55-0.6,0.55-0.6,0.55-0.6,0.55-0.6,0.55-0.6,0.65
0.60-0.65,0.60-0.65,0.60-0.65,0.60-0.65,0.60-0.65,0.7
0.65-0.7,0.65-0.7,0.65-0.7,0.65-0.7,0.65-0.7,0.75
0.70-0.75,0.70-0.75,0.70-0.75,0.70-0.75,0.70-0.75,0.8
0.75-0.80,0.75-0.80,0.75-0.80,0.75-0.80,0.75-0.80,0.85
0.8-0.85,0.8-0.85,0.8-0.85,0.8-0.85,0.8-0.85,0.9
0.85-0.9,0.85-0.9,0.85-0.9,0.85-0.9,0.85-0.9,0.925
0.90-0.95,0.90-0.95,0.90-0.95,0.90-0.95,0.90-0.95,0.95
0.95-1,0.95-1,0.95-1,0.95-1,0.95-1,0.975
1,1,1,1,1,1

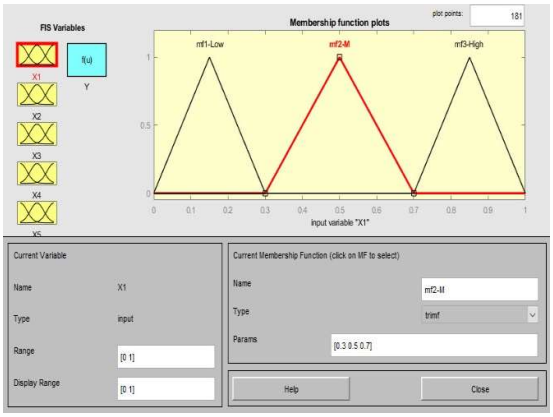

Figure 3. Segmentation of the output variable of the neural-fuzzy inference system - fuzzy values associated with linguistic variables (membership functions of triangular and trapezoidal numbers).

Step 3: Designing a Neural-Fuzzy Inference System Knowledge Base - This step involves extracting the expertise rules and evaluating them by experts and creating a fuzzy rule database. The fuzzy rule database is a set of "if-then" rules that are at the heart of the PHISHING.IDS + ANFIS system, as other components of the fuzzy system are used to implement these rules effectively and efficiently. Here the probability of occurrence of different states between the main variables of the same neural-fuzzy inference system is considered. The starting point for building a rule-based knowledge base in a fuzzy system is to obtain a set of rules. If fuzzy is then the knowledge of experts or the knowledge of the field under research, the next step is to combine these rules into one system. Is a unit. Other rules of the knowledge base of this neural-fuzzy inference system were also generated in this way. Finally, the number of fuzzy rules of the module "Improving the security of the bank network in detecting phishing attacks" of PHISHING.IDS + ANFIS system is equal to 243 due to the existence of 5 main variables, each of which has 3 modes. The figure for the PHISHING.IDS + ANFIS system module fuzzy rule databases is as follows:

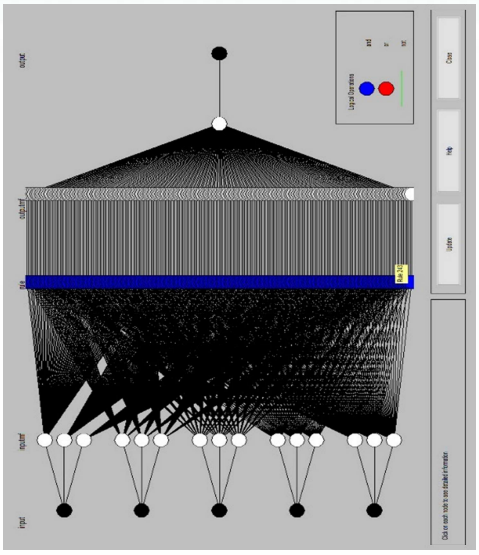

Figure 4. How to generate fuzzy rules within the knowledge base of the module "Improving Bank Network Security Management in Detecting Phishing Attacks".

Step 4: Designing the inference engine for the PHISHING.IDS + ANFIS system - In this step, the Centrid method has been selected for de-fuzzy to convert numbers and fuzzy sets to a definite value to actually check the performance of the system. The following figure shows the inference engine of the PHISHING.IDS + ANFIS system:

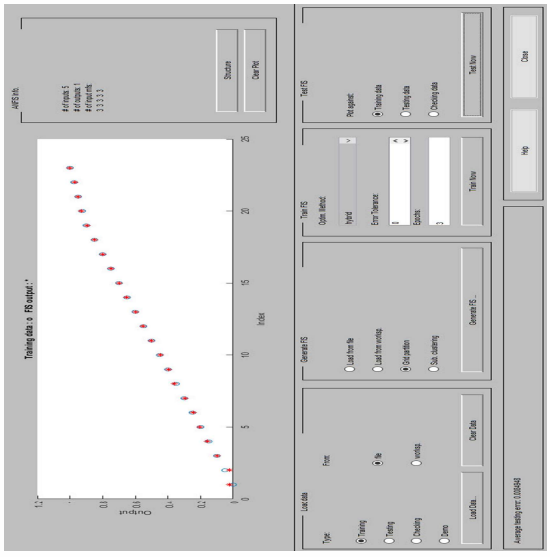

Figure 5. PHISHING.IDS + ANFIS system inference engine.

Using MATLAB R2017B software, inference can be made based on the rules in the PHISHING.IDS + ANFIS system knowledge database. The mean error of the test data in the inference engine of PHISHING.IDS + ANFIS system for "Implementation of IDS for phishing detection" is equal to 0.0085 (less than 1%) which shows the very high accuracy of synthetic neural network and logic logic calculations. . In fact, the most important reason to use the Sugeno inference engine (instead of Mamdani) is that in Mamdani inference engine, the choice of type of implication and fuzzy rule aggregation style (to collect fuzzy rules for inference

and inference) is not fixed. Min is used to select the type of request in MATLAB software because the Prod operator shortens and completes the output fuzzy set. The non-fuzzy instrument in the PHISHING.IDS + ANFIS¬ system converts the fuzzy output to a definite number. In the non-fuzzy part of MATLAB software, wtavar method is used because this non-fuzzy helps to reduce the complexity of the problem and also less time for calculations. Here, due to the connection of the fuzzy rules of the system using the "And" operator, in the MATLAB software, we select the "Max" fuzzy rule aggregation style. In this case, the more precise sum of each output set of rules is considered, not part of them.

Step 5: Explain how to use the neural-fuzzy inference system designed and analyze its outputs - to analyze the variable output behavior of the system "Implement IDS to detect phishing" PHISHING.IDS + ANFIS can be analyzed by PHIDING. + ANFIS paid numerically (accurately) and linguistically. The table and figure below analyze the behavior of the input and output variables of the PHISHING.IDS + ANFIS system module:

TABLE VI. INFORMATION ABOUT THE WEIGHT OF EACH OF THE MAIN RESEARCH VARIABLES

Research Variables	Weighted Mean	Fuzzy weight
Signature Detection (X1)"	5.3325	0.7618
Network-based " "intrusion detection (X2)	5.388	0.7697
Distributed Infiltration " "Detection (X3)	5.306	0.7580
Host-based intrusion " "detection (X4)	5.5863	0.7980
Intrusion Analysis and " Detection Schedule "(X5)	5.5325	0.7904

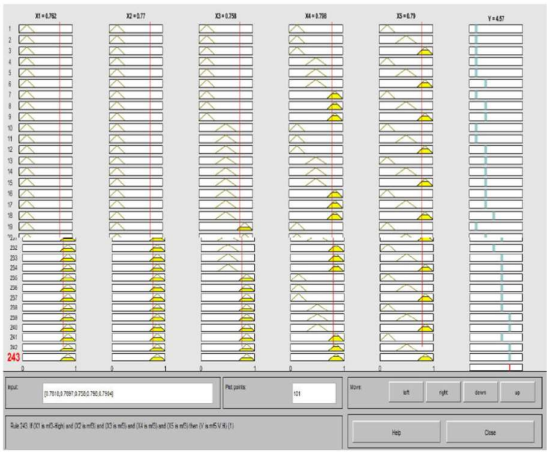

Figure 6. Analysis of the behavior of the output variable in the module "Improving the security management of the bank network in detecting phishing attacks" numerically and linguistically.

According to the rules of the knowledge base of the main module of PHISHING.IDS + ANFIS system based on calculating the weight of each of the main variables using the opinions of experts; If; "Signature-based (X1)" status is good, and "Network-based intrusion detection (X2)" is good, and "Distributed intrusion detection (X3)" is good, and "Host-based intrusion detection (X4)" is good. ; And "Intrusion Analysis and Detection Schedule (X5)" is in good condition; Then; The status of "Banking Network Security Management in Detecting Phishing Attacks (Y)" is at its fifth level, "excellent". According to the membership functions of language variables by the experts in the tables above, 4.57 within a 5-value range in the range defined for the "excellent" language variable, the IDS implementation state for phishing detection, is calculated to be exactly 0.914. Therefore, the status of "bank network security management in detecting phishing attacks (Y)" in the above state is at the fifth level of "excellent". After designing the neural-fuzzy inference system of the research, the outputs and responses of the neural-fuzzy inference system of this research were compared in a separate measurement tool with the opinions of 18 experts, the result of which can be based on the rules of neural-fuzzy inference and response systems. Experts examined:

Assumption Zero (H0): There is a significant difference between the average opinions of experts and the outputs of "PHISHING.IDS + ANFIS system".

Hypothesis (H1): There is no significant difference between the average of expert opinions and the output of "PHISHING.IDS + ANFIS system".

According to the descriptive information in the table above, it is possible to compare the outputs of the neural-fuzzy inference system with the average opinions of experts. Since the opinions of experts are expressed based on the 5-value spectrum (MFs), to test the above hypothesis, we can use the percentage difference between the outputs of the neural-fuzzy inference system with the average of the experts' opinions as follows:

TABLE VII. INFORMATION ABOUT COMPARING THE OUTPUTS OF "PHISHING.IDS + ANFIS SYSTEM" WITH THE AVERAGE OPINIONS OF EXPERTS

Rules of neural-fuzzy inference system	Neuro-fuzzy inference system outputs	Average answers of experts	Ratio of difference	The final difference
Rule. 3	1	1/22	4 / 0/22 0/055 =	0/065
Rule. 45	3	2/72	4 / 0/28 0/0675 =	
Rule. 79	3	2/78	4 / 0/22 0/055 =	
Rule. 86	2	1/67	4 / 0/22 0/0825 =	
Rule. 103	2	1/67	4 / 0/22 0/0825 =	
Rule. 140	3	2/78	4 / 0/22 0/055 =	
Rule. 157	3	3	= 4 / 0 0	

Rule. 219	2	2/94	4 / 0/06 0/015 =
Rule. 224	2	2/39	4 / 0/61 0/1525 =
Rule. 235	2	2/67	4 / 0/33 0/0825 =

As can be seen, the final difference between the outputs of the neural-fuzzy inference system and the mean of the experts' opinions is not significant and is equal to 0.065. Since there is not enough reason to accept the null hypothesis, the opposite hypothesis is accepted, i.e. there is no significant difference between the average opinions of experts and the outputs of the "PHISHING.IDS + ANFIS system".

VI. Summary of Research Findings

In order to achieve the objectives of the research and according to the research background, the main findings of the research are presented here. As can be seen in the statistical tables in Chapter 4, based on the opinions and professional experience of managers and senior experts in the banking industry and the opinions of university professors, the most important criteria for signature-based detection processes (X1) is network-based intrusion detection (X2). Distributed intrusion detection (X3), Host based intrusion detection (X4) and intrusion analysis and intrusion detection (X5), respectively: Detection of forged signatures with an average of 5.57; Detection of intra-network attacks with a mean of 5.57; Detection of extranet attacks with a mean of 5.57; Intrusion hardware distribution with an average of 5.60; Recognize features based on JavaScript and HTML with an average of 5.80; And authentication methods with an average of 5.78; Were calculated. Ranking of research variables based on the weighted average of their indicators are: Host-based intrusion detection with a weighted average of 5.5863, Mohawk analysis analysis and intrusion detection with averaged 5.5325, Mohsen-centered intrusion 5.3325 and detected distributed intrusion with a weighted average of 5.306. In fact, the data of this research are in good condition in terms of symmetry and aggregation. In fact, the main reason for analyzing the reliability of the data collection tool of this research is to what extent the measurement tool gives the same results under the same conditions and that the correlation between one set of answers and another set of answers in an equivalent test that How much is an independent form obtained on a group of subjects? Here, Cronbach's alpha for the research variables is greater than 0.9, indicating that the reliability of the IDS implementation modeling tool for phishing detection is excellent. Since the sign of correlation coefficient is the slope of the regression line, there is a positive and relatively significant relationship between signature-based detection (X1) and host-based intrusion detection (X4), because the correlation coefficient between them is calculated to be 0.572. On the other hand, there is a positive and significant relationship between signature-based detection (X1) and distributed intrusion detection (X3), because the correlation coefficient between them is calculated to be 0.887. There is a positive and significant relationship between signature-based detection (X1) and network-based intrusion detection (X2), because the correlation coefficient between them is calculated to be 0.646. On the other hand, there is a positive and significant relationship between distributed intrusion detection (X3) and network-based intrusion detection (X2), because the correlation coefficient between them is calculated to be 0.589.

VII. Conclusion

In this research, a neural-fuzzy inference system for implementing IDS to detect phishing using Matlab programming environment, called PHISHING.IDS + ANFIS was presented. Neural-fuzzy inference system knowledge database design - includes the extraction of expert rules and their evaluation by experts and the creation of a fuzzy rule database. The fuzzy rule database is a set of "if-then" rules that are at the heart of the PHISHING.IDS + ANFIS system, as other components of the fuzzy system are used to implement these rules effectively and efficiently. In the design phase of the inference engine, the PHISHING.IDS + ANFIS system - Centered method for de-fuzzy to convert numbers and fuzzy sets to a definite value has been selected to evaluate the actual performance of the system. PHISHING.IDS + ANFIS system was addressed. Describes how to use a neural-fuzzy inference system designed and analyzing its outputs - to analyze the variable output behavior of the system "Implement IDS to detect phishing" PHISHING.IDS + ANFIS to analyze the output of the system We have dealt with the numerical (exact) and linguistic form. Finally, by using the PHISHING.IDS + ANFIS system, the status of "bank network security management in detecting phishing attacks (Y)" can be examined numerically and more precisely: if; the status of "signature-based detection (X1)" is good. , That is, it is exactly 0.758, and "Intrusion Analysis and Detection Schedule (X5)" in good condition means exactly 0.762, and "Network-based intrusion detection (X2)" is good, that is, exactly 0.798, and X has been deleted. "OK means exactly 0.770" and "Host-based intrusion detection (X4)" OK means exactly 0.790; then "Banking network security management detection of phishing attacks (Y)" at "excellent (fifth level)" That is, it is exactly 0.914.In fact, the most important and key research proposal for the implementation of IDS for phishing detection is that the neural-fuzzy inference system for the implementation of IDS " "Detect phishing and pay more attention to its effectiveness."

References

[1] Nankeli, Majid, 2015, Customization and Evaluation of Snort Infiltration Detection System in Banking Network, First International Conference on Information Technology, Tehran, Iran Development Conference Center

[2] Amrei, Majid and Akram Beigi, 1397, A multi-layer intrusion detection system with a combined approach, 15th International Conference of the Iranian Password Association, Tehran, Iran Password Association - Tarbiat Dabir Shahid Rajaei University

[3] Sahingoz, Ozgur Koray, et al. 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, Volume 117, 1 March 2019, Pages 345-357

[4] Rao, Routhu Srinivasa & Alwyn Roshan Pais. 2019. Jail-Phish: An improved search engine based phishing detection system. Computers & Security, Volume 83, June 2019, Pages 246-267

[5] Daneshjoo, Parisa and Seyed Ahmad Taherzadeh, 1397, Detection of Infiltration in Banking Transactions Using Individual Value Analysis and RBF Neural Networks, Annual

National Congress of New Research Ideas in Engineering and Technology, Electrical and Computer Science, Science and Computer

[6] Heshmatian, Zahra; Mohammad Hossein Shafiabadi and Fatemeh Safara, 1397, Increasing the accuracy of intrusion detection systems using PSO & SVM algorithms, 2nd International Conference on Electrical Engineering, Computer Science and Information Technology, Hamedan, Permanent Secretariat

[7] 7. Samadiani, Najmeh and Zeinab Hassani, 1397, Identification of Phishing Websites Using Cuckoo Comparative Algorithms, Fourth International Conference on Industrial and Systems Engineering, Mashhad, Ferdowsi University of Mashhad

[8] Akhlaghpour, Mohammad and Maryam Shahriari, 1397, A solution using a support vector machine to improve false alarms in intrusion detection system, 4th National Conference on Modern Science and Technology of Iran, Tehran, Association for the Development and Promotion of Basic Sciences and Technologies

[9] Dami, Sina and Akram Ghasemnejad, 1397, Presenting a New Method Based on Tutorial Learning for Network Intrusion Detection System, Annual National Congress of New Research Ideas in Engineering and Technology, Electrical and Computer Science, Sari, Target Institute of Higher Education

[10] Bahmani, Ali and Sidamir Hassan Monjemi, 1397, Presenting a two-stage solution based on deep learning in order to increase the accuracy of network intrusion detection systems, 7th Conference on Electrical Engineering, Isfahan, 7th Conference on Electrical Engineering

[11] Behravan, Tayebeh;Hossein Ebrahim Pourkoumleh and Ali Mohammad Nikfarjam, 2017, Phishing detection using URL-based features and anomalies, 3rd International Conference on Pattern Recognition and Image Analysis, Shahrekord, Shahrekord University - Iranian Machine and Image Processing Association.

[12] Mohammadi Jalkani, Meysam and Mohammad Reza Hassani Ahangar, 2017, Evaluation of intrusion detection systems based on unattended neural networks, Third National Conference on New Approaches in Computer and Electrical Engineering, Rudsar, Islamic Azad University, Rudsar and Javangaran Branch Rudsar and Amlash units.

[13] Abdolrazaghnejad, Majid, 2016, Classification and Identification of Phishing Websites Using Fuzzy Rules and Modified Slope Optimization Algorithm, Iranian Journal of Electrical Engineering and Computer Engineering - B Computer Engineering, Winter 2016, Volume 4, Number 14; From page 311 to page 321.

[14] Dadkhah, Mehdi, Davarpanah Jazi, Mohammad and Saeedi Mobarakeh, Majid, 2016, Presenting an Approach for Identifying and Predicting Phishing Websites by Classification Algorithms Based on Web Page Characteristics, Modeling, Vol. From page 213 to page 227.

[15] Saeedi, Parisa, 1394, Identification of Phishing Website in Electronic Banking with Fuzzy Logic, Ministry of Science, Research, and Technology - Urmia University of Technology, 1394.

[16] Zangiabadi, Laia and Ali Nasser Asadi, 2016, Application of Data Mining and Text Mining in Detection of Phishing Emails, 2nd National Conference on Computer Engineering Research, Hamedan, Ekbatan Research Group

[17] Rehabilitation, Jafar; Hossein Amouzad Khalili and Mostafa Haji Aghaei Keshtali, 2015, Challenges and Strategies for Combating Fishing in Online Banking, The First International Conference on Industrial Engineering, Management and Accounting, Electronically, Online

[18] Saeedi, Parisa, 2015, Investigation of Intelligent Detection Systems and Phishing Website in Electronic Banking by Fuzzy Logic Method, First International Conference on Information Technology, Tehran, Iran Development Conference Center

[19] Teymouri, Saeed, 2015, Designing a New Framework for Dealing with Random Network-Based Phishing Websites, International Conference on New Research Findings in Electrical Engineering and Computer Science, Tehran, Nikan Institute of Higher Education

[20] Moghimi, Mahmoud; Hossein Akbaripour and Mohammad Reza Amin Naseri, 2012, Development of an expert system based on the characteristics of web pages in order to detect phishing attacks in electronic banking, 9th International Conference on Industrial Engineering, Tehran, Iranian University of Industrial Engineering, Tehran University of Technology

[21] Elahi, Sha'ban; Ali Shayan and Behnam Abdi, 2007, Designing a Convergent Network Security Management Framework among Stakeholder Banks, Fourth International Conference on Information and Communication Technology Management, Tehran, Nedaye Eghtesad Bamdad (Lean)

[22] Vincent, Adam. 2019. Don't feed the phish: how to avoid phishing attacks. Network Security, Volume 2019, Issue 2, February 2019, Pages 11-14

[23] Parsons, Kathryn, et al. 2019. Predicting susceptibility to social influence in phishing emails. International Journal of Human-Computer Studies, Volume 128, August 2019, Pages 17-26

[24] Li, Yukun, et al. 2019. A stacking model using URL and HTML features for phishing webpage detection. Future Generation Computer Systems, Volume 94, May 2019, Pages 27-39

[25] Varshney, Gaurav, et al. 2018. Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks. Journal of Information Security and Applications, Volume 42, October 2018, Pages 1-17

[26] Goel, Diksha & Jain, Ankit Kumar, 2018, Mobile phishing attacks and defence mechanisms: State of art and open research challenges, Computers & Security, Volume 73, March 2018, Pages 519-544

[27] Smadi, Sami, et al. 2018. Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. Decision Support Systems, Volume 107, March 2018, Pages 88-102

[28] Merhi, Mohammad I. & Punit Ahluwalia. 2019. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. Computers in Human Behavior, Volume 92, March 2019, Pages 37-46

[29] Anciaux, Nicolas, et al. 2019. Personal Data Management Systems: The security and functionality standpoint. Information Systems, Volume 80, February 2019, Pages 13-35

[30] Huang, Chun-Hsian, et al. 2019. Adaptive and service-oriented embedded system for information security applications. Computers & Electrical Engineering, Volume 73, January 2019, Pages 145-154

[31] Steinbart, Paul John, et al. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, Volume 71, November 2018, Pages 15-29

[32] Kuo, Ren-Zong. 2018. EMRS Adoption: Exploring the effects of information security management awareness and perceived service quality. Health Policy and Technology, Volume 7, Issue 4, December 2018, Pages 365-373

[33] Tchakoucht, Ait, Taha, Ezziyyani, Mostafa, Building A Fast Intrusion Detection System For High-Speed-Networks: Probe and DoS Attacks Detection, Procedia Computer Science, Volume 127, 2018, Pages 521-530.

[34] Haider, W., J. Hu, J. Slay, B. P. Turnbull, Y. Xie, 2017, Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling, Journal of Network and Computer Applications, Volume 87, 1 June 2017, Pages 185-192.

[35] Aleroud, Ahmed, Zhou, Lina, 2017, Phishing environments, techniques, and countermeasures: A survey, Computers & Security, Volume 68, July 2017, Pages 160-196.

[36] Nguyen, Luong Anh Tuan; Ba Lam To; Huu Khuong Nguyen, 2016, An Efficient Approach Based on Neuro-Fuzzy for Phishing Detection, Journal of Automation and Control Engineering Vol. 4, No. 2, April 2016.

[37] Ram, B., A. H. Sung, Q. Liu, 2014, "Learning to detect phishing URLs", International Journal of Research in Engineering and Technology, 2014.

[38] Ajlouni, M., H. Wa'el, J. Alwedyan,2013, "Detecting phishing websites using associative classification", European Journal of Business and Management,2013.

[39] Aburrous, M., A. Hossain, K. Dahal, F. Thabatah, 2010, "Intelligent phishing detection system for e-banking using fuzzy data mining", Expert systems with applications, 2010.

[40] Hoshyar, Momeneh and Abbas Karimi, 2017, A New Method of Detection and Prevention of Infiltration Based on IPS and IDS, Elite Journal of Science and Engineering 2 (2).

[41] Moein Taghavi, Maryam and Khademi, Maryam, 2016, Detection of intrusion in computer networks based on fuzzy systems and forbidden search algorithm, Journal of New Ideas in Science and Technology, 2016, Volume 1, Number 2.

Mohsen Gerami received his Ph.D. degree in Engineering of Information and communication Technology from Seoul National University. He is an Assistant Professor at Faculty of Post and Communications (ICT Faculty) in Tehran. His research interests include Security, Block chain and Cryptocurrency, Cyber Security, Digital transformation, Information and Communication Technology and ICT Policy.

Abdollah Sahifeh - Master of Science and Communication Technology Management, Information Systems Development Orientation, Planning and Systems Manager of Pazargad Non-Industrial Operations Company (a subset of Persian Gulf Petrochemical Holding Companies), Project Manager of Information and Communication Technology in the Pasargad Oil company, ICT consultant in government agencies and organizations, instructor of specialized courses in the field of ICT.