Information Sciences and Computer Engineering, Vol.1 No.1, (2023) 20-26

PHARUS

International Journal of
Information Sciences and Computer Engineering

journal homepage: http://www.ijisce.org

Distributed Intrusion Prevention System based on Cloud Computing in the Internet of Things

Mohadeseh Mir[1], and Hamid Reza Naji[1, *]

[1]*Department of Computer Engineering and Information Technology, Graduate University of Advanced Technology, Kerman, Iran*

Abstract— Cyber security is a serious issue in cyberspace. Thousands of zero-day attacks are constantly evolving due to the addition of various protocols on the Internet of Things. On the other hand, using deep learning in various information security fields has been successful. Also using deep learning to detect an attack in cyberspace is a flexible mechanism for detecting new attacks. In this research, we introduced a distributed penetration system for the Internet of Things, which used Apache Spark and also an expert system for optimal performance. The proposed model is compared with the suggested architecture of a distributed attack detection scheme using the deep learning approach for the Internet of Things. Also, the effectiveness of the proposed deep learning against the shallow learning algorithms for detecting attacks on the Internet of Things is evaluated. The results indicated that the proposed approach is more optimal in accuracy, learning speed and memory consumption in compare to another discussed method.

Keyword: Security; internet of things; intrusion prevention system; deep learning; apache spark; expert system**.**

1. Introduction

Network security is an actual necessity with the widespread use of the Internet [1]. The Internet of Things has created a lot of expectations because of the ability to turn physical objects of different application domains into Internet hosts. However, attackers may also use the great potential of the Internet of Things like a new way of violating the privacy and security of users [2]. Therefore, security solutions for the Internet of Things must be developed. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are one of the most important security tools for the Internet of Things [3]. The Intrusion detection system means identifying inappropriate, false, and abnormal activities. The purpose of the intrusion detection system is to determine if an unauthorized computer system or network is being used [4]. Intrusion prevention systems are considered to be an enhanced status of intrusion detection systems. The main difference between these systems and intrusion detection systems is that these systems can prevent or stop malicious activities [5]. Managing intrusion detection systems is also a challenge for network administrators and users. Therefore, IDS management in The Internet of Things cannot be depended on continuous human intervention. Therefore, researchers should propose automatic methods for IDS alerts in The Internet of Things.

One of the mechanisms for creating security on the Internet is the use of a secure and intelligent architecture to deal with threats automatically. Therefore, the purpose of this study is to introduce an efficient, scalable and intelligent security architecture to deal with attacks on The Internet of Things. Our architecture is based on cloud computing. In a cloud-based structure, resources are available to the cloud service provider and users access it remotely. Remote processing is done in this way that the data and other elements are transmitted to the cloud by the user and the processing result is sent to the user [6].

Cloud computing not only minimizes the cost and limitations of automation and computing by a single computer but also reduces the cost of maintaining infrastructure, optimizing its management and providing users with access to them. The advent of cloud computing technology is a useful, scalable, and cost-effective solution to the challenges of using big data in a variety of applications [7]. One of the main issues

[*] Corresponding author:

Email address: naji@kgut.ac.ir, Ph: +98 913 198 2781

that we have to consider when we are using cloud is its security and protection. A survey on intrusion detection systems for cloud computing is presented in [8].

The solution proposed by scientists to better utilize cloud computing and the Internet of Things is the integration of both new technologies. Cloud computing can offer an effective solution for managing and interconnecting the Internet of Things. It can also be used to run applications and services where things or data are extracted from them [9]. On the other hand, Cloud can use the Internet of Things to develop realms to deal with real-world things in most distributed and dynamic situations and to deliver new, real-life scenarios on a large scale.

n fact, the cloud facilitates the flow of data between data collection and processing of things on the Internet, and it has the ability to set up and integrate new things quickly while maintaining low costs for deployment and processing of complex data. As a result, the decision-making and prediction of the data-driven algorithms can be at a low cost by providing a method for increasing revenue and risk reduction [10].

Due to the high amount of data and rules, we used deep learning. Increasing the diversity of attacks raises the limits of modeling of signatures. Machine learning provides a way of developing the Internet of Things [11]. Its a kind of artificial intelligence that enables machines to learn, without explicit programming [12]. Deep learning is a subcategory of machine learning based on a set of algorithms that attempt to model high-level abstract concepts in the data. It helps to model the processes using a deep graph that has multiple processing layers consisting of several layers of linear and nonlinear transformations. In other words, its foundation is based on learning to display knowledge and features in the model layers [13]. Using deep learning to detect attacks on computer networks, due to feature extraction, can be a flexible mechanism for small jumps or new attacks. The ability to self-learning and compression in deep learning is the key to discover the hidden patterns in training data and discriminating attacks from optimistic traffic. The main advantage of deep learning is the lack of use of manual techniques and also, unsupervised compression can allow it to be used in resource constraint networks. This means that deep learning has the ability for self-learning of results in higher accuracy and faster processing [14].

The overall structure of the paper is as follows: Section two covers related works. Section three describes the proposed method. Section four involves simulating, evaluating and comparing the proposed method with the related works and section five contains conclusions and suggestions.

2. Related works

In this section, we review the literature for detecting attacks on the Internet of Things.

Raza et al. (2013) design, implement and evaluate a new intrusion detection system for The Internet of Things called SVELTE. SVELTE is a hybrid IDS whose goal is to provide a satisfactory balance between the cost of signing-based storage and the cost of calculation based on an abnormal behavior approach. In their work, the host router is responsible for detecting Intrusion by analyzing network RPL data. The SVELTE detects malicious nodes [15].

Thanigaivelan et al. (2016), presents a distributed internal anomaly detection system for The Internet of Things: An IDS that assign various responsibilities to the border router and network nodes. The IDS module running in a node checks the nodes neighbors and when an event is detected, the node sends a report to the IDS module on the border router. Next, the border router module performs the final decision by communicating notifications from different nodes. This system uses fingerprinting on the network to be aware of changes in network topology and node positions without any help from a positioning system [16].

Diro et al. (2018) proposed a distributed deep learning-based system for network attack detection in The Internet of Things. This research is aimed at adopting a new approach, deep learning, to provide cyber security and enable the detection of attacks in the Internet of Things. The fog nodes are responsible for training models and hosting attack detection systems. The coordinating master node should be in place for collaborative parameter sharing and optimization. The benefits of this approach are the acceleration of data training near to the source and the gain of updated parameters from neighbors. The master node updates the parameters and propagates them back to the worker nodes. This sharing scheme results in better learning as it enables to share best parameters and avoids local overfitting [17].

Cervantes et al. (2015), suggested a solution called INTI (Intrusion detection of Sinkhole attacks on 6LoWPAN for The Internet of Things), to identify sinkhole attacks on the routing services in The Internet of Things. At first, nodes are classified as a leader, dependent nodes or members, and constitute a hierarchical structure. Each node's role over time can be changed due to a network reset or an attack event. The system detects the attackers by analyzing the behavior of devices. The INTI showed a low false positive and false negative rate in compare to SVELTE. The authors do not discuss the effect of this solution on low-power nodes [18].

Haddadi et al. (2018) presented a novel, cooperative system between the home gateway and the Internet Service Provider (ISP) to provide data-driven security solutions for detecting and isolating The Internet of Things security attacks. This approach is based on a combination of powerful machine learning techniques on traffic traces and the edge processing techniques to provide efficient, yet privacy-aware The Internet of Things security services. Their systems, SIOTOME, is an architecture to monitor an The Internet of Things network, providing user security and privacy, despite potentially vulnerable or compromised devices [19].

Pandyswari and Kumar (2016) presented the use of machine learning in intrusion detection. Their methodology is based on the analysis of virtual network traffic, which is gathered in normal and abnormal conditions. This work proposes an anomaly detection system that uses a hybrid algorithm which is a mixture of the Fuzzy C-Means clustering algorithm and Artificial Neural Network (FCM-ANN) to improve the accuracy of the detection system. The proposed system is able to detect the anomalies with high detection accuracy and low false alert rate [20].

Some other articles that used machine learning to detect attacks are as follow:

Lee et al. (2006) determine the characteristics of the normal network behavior using math rules, such as unions and associations rules. The conflict with these rules indicates attacks on the network [21]. Zhang et al. (2008) used a random forest algorithm for automatic attack patterning [22]. Mabou et al. (2011) used the Fuzzy class-association rules extraction to detect attacks using genetic network programming [23]. Khor and colleagues (2012) proposed a dualization algorithm in which rare classes of educational data are separated and cascaded classes are trained to control rare attacks and other cases [24].

3. The Proposed approach

Deep learning can dramatically improve performance in the training of large models. On the other hand, training large models can be very time-consuming. Hence, we proposed an architecture to accelerate deep network training. On the other hand, the final classification accuracy improves significantly when the number of training examples increases. In recent years, using expert systems has made significant progress. This architecture has led to an improved application optimization using learning and inference algorithms. One of the main capabilities of the proposed method is using an expert system and its application in the prevention system. In fact, our expert system used the proposed optimal deep learning algorithms to provide its rules. The deep learning parameters are set to have the highest accuracy and minimum error as well.

In this paper, we describe a distributed approach: using massive clusters in machines that distribute training and inference in deep networks. This leads to a desirable response to attacks. In this approach, the workers' nodes are responsible for training models. They are also a host for intrusion prevention systems in the Internet of Things. The master node is used to share and optimize parameters. The benefits of this research are the autonomy of detecting local attacks. They also accelerate training models using optimizing local parameters at the workers. Fig. 1 demonstrates a general architecture of our parallel and distributed intrusion prevention system.

This architecture provides a model in the form of a master-worker for synchronizing and communicating under master management. Here, we combine an optimal deep learning algorithm with expert system techniques to design and implement distributed training on a large scale. Our experiments show the results in a confrontation with attacks on a large scale for The Internet of Things. We present two main findings: The proposed deep learning algorithm that can increase the accuracy and reduce the error. Using an expert system also leads to automation of confronting the attack operation. On the other hand, an expert user monitors the system and model to correct it if it performs inappropriately.

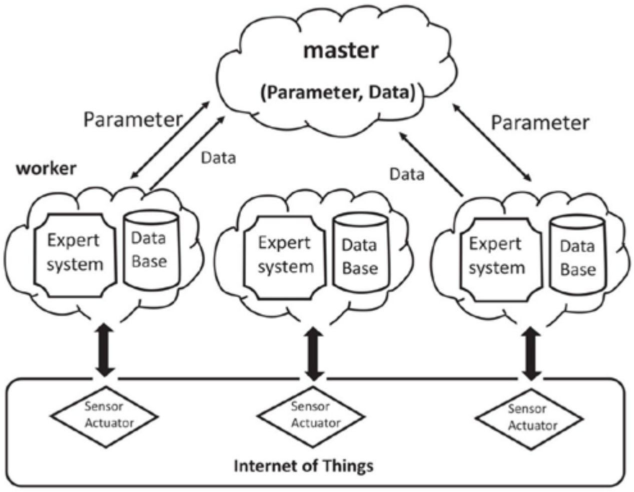

Fig. 1. The proposed Intrusion Prevention System on the Internet of Things.

Our Focus is to optimize the fully connected deep learning technique to train very large models. We believe that multilayer architecture is effective to overcome computing attack detection.

4. Distributed model

To facilitate the training of large learning networks, an architecture is used to support distributed computing. In each layer calculations, data, and transferable parameters are defined. For large models, there are several distributed workers, each of which is responsible for supporting a number of things on the Internet of things. Each worker can use all the cores in parallel to conduct deep learning calculations. The workers also manage communication, synchronization and data transfer during training and inference. This parallelism is defined in the deep learning algorithms.

The used architecture is a small version of parallel execution. This approach enables us to process training samples in different models at workers simultaneously. They also combine the results to optimize the target performance sequentially. Adam is a method of training deep learning networks. It updates weights and bias. The basic approach is as follows:

Each worker receives data from things in the Internet of Things. The worker nodes include a database and an expert system. The data from the sensors of the Internet of Things are aggregated into the workers' database. Fig. 2 shows the structure of the expert system in each worker.

In the knowledge base, the rules are obtained from applying deep learning algorithms to the database. In this operation, first, the parameters are selected randomly. Due to feature extraction, deep learning can use a flexible mechanism in Cyberspace to detect new attacks. In this approach, this algorithm is fully connected. Relu is an activity function that is used in each layer. Here, Adam optimizer has been used to reduce the cost function. The deep learning algorithm includes 150 neurons in the first layer, 100 in the second, 50 in the third, and in the last layer, the neurons are equal to the class number. This class number is applied for classification by softmax regression. This model has 16 epochs. To avoid the overload problem, Dropout is placed in each layer. In order to detect the type of attacks, we classified the algorithm output in two modes: At first, we classified two classes: (Attack, Normal) and in the latter case into four classes (DOS.R2L, U2R, Probe, Normal).

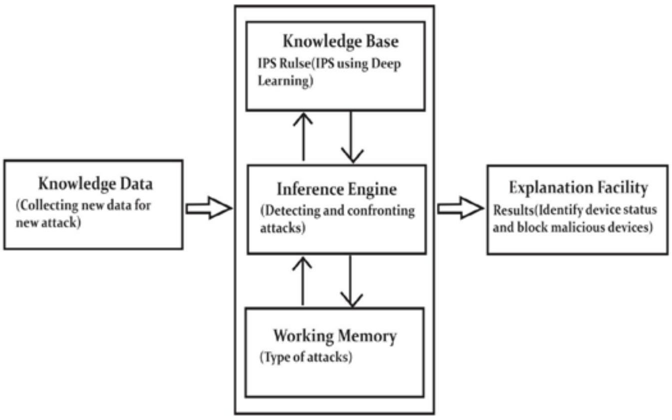

Fig. 1. Implementing prevention mechanism using Expert System.

The inference engine does the attack detection and confronting operations using the rules obtained from the database and the facts in the working memory. If an attack is detected, it sends a signal to block the device. The expert system provides the user with the status of all the devices on the Internet of Things. In each worker, the parameters of this algorithm are sent to the master. These parameters include weights, bias and training data. The master node uses the Deep learning algorithm and Adam method to calculate the gradient descent. It checks the local parameters and weights received from the workers. Next, it obtains the optimal parameters that have lower cost functions. This sharing scheme improves learning and enables it to share the best parameters to avoid overfitting. The master broadcasts the updated weights and biases the entire workers. The workers update their weights and biases and apply the learning algorithm based on them. Each worker uses the Adam method. It also obtains the optimal parameters with a lower cost function of new data. Therefore, the new parameters and data return to the master and this process continues repeatedly. Therefore, the higher accuracy and the lower error rate are achieved with the pass of time and more data.

Dividing the data into several machines accelerate the operation. As a result, the network overhead decreases and less work needs to be done on every worker. This method is suitable for the efficient use of the storage and computing resources of the Internet of Things. It provides quick response time as well.

5. Evaluation

5.1 Simulation environment

For this research, we use the Python programming language, Apache Spark for parallel and distributed processing. The keras library has been used to implement the deep learning algorithm and the pyknow for the expert system. Also, we used the NSL-KDD dataset [25].

The NSL-KDD collection is an optimal and reduced version of the KDDCUP99 dataset. The NSL-KDD dataset consists of 125973 records of training and 22544 records of the test. Each includes 41 features, such as duration, protocol, source bytes, destination bytes, traffic type, etc [26]. The Attacks are categorized into four main groups as shown in Table 1.

Table 1. Category of attacks in the NSL-KDD database.

Attack	Description
DOS	The attacker sends a large number of requests to a host.
U2R	The attacker tries to find an unauthorized hypothetical external machine to access the root of the system.
R2L	The attacker tries to use control system of a foreign machine through the network as a local user.
Probe	The attacker is trying to find information about the machines and network services for the purpose of searching.

5.2 Results

Accuracy (Acc) in Eq. (1), Discovery Rate (DR) in Eq. (2) and False Alert Rate (FAR) in Eq. (3) are selected for the test data set. These are important metrics to determine the precision of attack detection.

$$ACC = \frac{TP+TN}{TP+FP+FN+TN} \quad (1)$$

$$DR = \frac{TP}{TP+FN} \quad (2)$$

$$FAR = \frac{FP}{FP+TN} \quad (3)$$

Where TP is true positive, TN is true negative, FP is false positive, FN is false negative.

The experiment we have done are for two purposes: (1) Comparison of the results of the distributed attack detection in the proposed approach with a similar one in the paper by Diro et al [17]. (2) Evaluating the effect of deep model versus the shallow model for detecting attacks on the Internet of Things. The shallow model is the same as the deep model while it does not have the middle layers.

In the first attempt to evaluate the model performance, the dataset is categorized into 2 classes (Attack, Normal) and then into 4 classes (Normal, Dos, Probe, R2L.U2R). The minority U2R and R2L have been merged to form a R2L.U2R. Before training the network, the categorical features have been encoded into discrete features using 1-to-n encoding technique. As a result, we obtained 123 input features and one label. The system uses preprocessing technique for both training and test. Finally, 122 non-labeled normal input features have been given to deep learning algorithms.

In the evaluation, the classification accuracy and other metrics demonstrate the effectiveness of our design versus the shallow models in the Internet of Things and also our IPS system based on the expert system versus the IDS proposed in Diro et al's [17]. The two approaches are compared in two modes, the shallow and deep model. Table 2 shows the comparison for Normal and Attack classes results demonstrates a better performance for our proposed model in compare to Diro et al, both in shallow and deep models. In this comparison, both accuracy and discovery rates have increased and the false alert rate has decreased by almost half.

Table 3 evaluates these two architectures. It categorized data into four classes of DOS, R2L.U2R, Normal, and Probe in two models of a shallow and deep. Also, the accuracy and discovery rate of the proposed architecture improved considerably in the deep model. The false alert rate has decreased in both the shallow and deep models in compare to the Diro et al's [17] approach.

In order to achieve e optimal performance, Diro et al. model train their system in 50 epochs, while we did the same training in 16 epochs which indicates an increase in the speed of the system learning. Also, the results show that our algorithm has less memory usage. As it is shown in Tables 2, 3, 4 and 5, the deep model performance is better than shallow model for training and prediction accuracy. It also has better performance in discovery and false alert rate as well. Also, the cost function (Loss) is downgraded considerably.

Table 2. The Results of our proposed model and Diro et al's approach (2-Class).

Method	Model	Accuracy Classes (%)	Discovery Rate (%)	False Alert Rate (%)
The proposed model	Deep model	99.47	99.36	0.39
	Shallow model	96.58	96.69	3.53
Diro et al	Deep model	99.20	99.27	0.85
	Shallow model	95.22	97.50	6.57

Table 3. The results of the proposed and Diro et al's approach (4-Class).

Method	Model	Accuracy Classes (%)	Discovery Rate (%)	False Alert Rate (%)
The proposed model	Deep model	99.72	99.44	0.35
	Shallow model	98.34	96.70	2.45
Diro et al	Deep model	98.27	96.50	2.57
	Shallow model	96.75	93.66	4.97

Table 4. Comparison of the deep and shallow model in the proposed approach (2-class).

Model	Training Accuracy (%)	Loss (%)	Training Time (s)	Estimated Time (s)
Deep model	98.83	3.16	223.73	1.74
Shallow model	95.48	13.01	43.54	0.59

Table 5. Comparison of the deep and shallow model in the proposed approach (4-class).

Model	Training Accuracy (%)	Loss (%)	Training Time (s)	Estimated Time (s)
Deep model	99.38	1.68	208.09	1.76
Shallow model	97.73	6.41	81.06	0.92

5. Conclusion and future work

In this study, we proposed a distributed intrusion prevention system using deep learning and expert systems. The results show the success of deep learning, machine learning and artificial intelligence in cyber security. This system designed to detect and confront the attacks in a distributed architecture of The Internet of Things such as smart cities. In the process of evaluation we calculated the accuracy, discovery rate, false alert rate and other metrics to demonstrate the effectiveness of the proposed approach. This approach can detect cyberattacks better than the compared system. The suggested deep learning algorithm uses less memory, makes learning faster, and the false alert rate is reduced greatly. In addition, it is more accurate than shallow model. Due to the sharing of parameters, the local minimum in the training of the algorithm is resolved considerably. Also, we have used the expert system for our model so if improper function is performed, or a malicious device- is operating, mainly in zero-day attacks, so the expert system will detect and gives automatically appropriate response quickly and more effectively.

In the future, this system can be used for other databases and implemented with other deep learning and machine learning methods.

References

[1] Da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., & de Albuquerque, V. H. C., Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks, 2019, 151, 147-157. https://doi.org/10.1016/j.comnet.2019.01.023.

[2] Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y., Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems, 2018, 19, 174-184. https://doi.org/10.1016/j.suscom.2018.06.003.

[3] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P., The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 2018, 6(2), 1606-1616. https://doi.org/ 10.1109/JIOT.2018.2847733.

[4] Holland, T., Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth. SANS Institute, 2004.

[5] Patel, A., Taghavi, M., Bakhtiyari, K., & JúNior, J. C., An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 2013, 36(1), 25-41. https://doi.org/ 10.1016/j.jnca.2012.08.007.

[6] Shahapure, N. H., & Jayarekha, P., Load balancing in cloud computing: a survey. International Journal of Advances in Engineering & Technology, 2014, 6(6), 26-57.

[7] Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U., The rise of "big data" on cloud computing: Review and open research issues. Information systems, 2015, 47, 98-115. https://doi.org/10.1016/j.is.2014.07.006.

[8] Chang, V., Golightly, L., Modesti, P., Xu, Q.A., Doan, L.M.T., Hall, K., Boddu, S. and Kobusińska, A., A Survey on Intrusion Detection Systems for Fog and Cloud Computing. Future Internet, 2022, 14(3), p.89. https://doi.org/10.3390/fi14030089.

[9] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B., Secure integration of IoT and cloud computing. Future Generation Computer Systems, 2018, 78, 964-975. https://doi.org/10.1016/j.future.2016.11.031.

[10] Botta, A., De Donato, W., Persico, V., & Pescapé, A., Integration of cloud computing and internet of things: a survey. Future generation computer systems, 2016, 56, 684-700. https://doi.org/10.1016/j.future.2015.09.021.

[11] Din, I. U., Guizani, M., Rodrigues, J. J., Hassan, S., & Korotaev, V. V., Machine learning in the Internet of Things: Designed techniques for smart cities. Future Generation Computer Systems, 2019, 100, 826-843. https://doi.org/10.1016/j.future.2019.04.017.

[12] Saravanan, R., & Sujatha, P., A State of Art Techniques on Machine Learning Algorithms: A Perspective of Supervised Learning Approaches in Data Classification. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) . IEEE. 2018, 945-949. https://doi.org/ 10.1109/ICCONS.2018.8663155.

[13] Bengio, Y., Learning deep architectures for AI. Foundations and trends® in Machine Learning, 2009, 2(1), 1-127. https://doi.org/ 10.1561/2200000006.

[14] Sarkar, S., Chatterjee, S., & Misra, S., Assessment of the Suitability of Fog Computing in the Context of Internet of Things. IEEE Transactions on Cloud Computing, 2018, 6(1), 46-59. https://doi.org/10.1109/TCC.2015.2485206.

[15] Raza, S., Wallgren, L., & Voigt, T., SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 2013, 11(8), 2661-2674.

[16] Thanigaivelan, N. K., Nigussie, E., Kanth, R. K., Virtanen, S., & Isoaho, J., Distributed internal anomaly detection system for Internet-of-Things. In 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE. 2016, 319-320. http://dx.doi.org/10.1109/CCNC.2016.7444797.

[17] Diro, A. A., & Chilamkurti, N., Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 2018, 82, 761-768. https://doi.org/10.1016/j.future.2017.08.043.

[18] Cervantes, C., Poplade, D., Nogueira, M., & Santos, A., Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE. 2015, 606-611. https://doi.org/10.1109/INM.2015.7140344.

[19] Haddadi, H., Christophides, V., Teixeira, R., Cho, K., Suzuki, S., & Perrig, A., SIOTOME: An edge-ISP collaborative architecture for IoT security. In Proc. IoTSec, 2018.

[20] Pandeeswari, N., & Kumar, G., Anomaly detection system in cloud environment using fuzzy clustering based ANN. Mobile Networks and Applications, 2016, 21(3), 494-505. https://doi.org/10.1007/s11036-015-0644-x.

[21] Lee, H., Chung, Y., & Park, D., An adaptive intrusion detection algorithm based on clustering and kernel-method. In Pacific-Asia Conference on Knowledge Discovery and Data Mining, Springer, Berlin, Heidelberg, 2006, 603-610. https://doi.org/10.1007/11731139_70.

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

[23] Mabu, S., Chen, C., Lu, N., Shimada, K., & Hirasawa, K., An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2010, 41(1), 130-139. https://doi.org/10.1109/TSMCC.2010.2050685.

[24] Khor, K. C., Ting, C. Y., & Phon-Amnuaisuk, S., A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection. Applied Intelligence, 2012, 36(2), 320-329. https://doi.org/10.1007/s10489-010-0263-y.

[25] https://www.unb.ca/cic/datasets/nsl.html, 2018.

[26] Kayacik, H. G., Zincir-Heywood, A. N., & Heywood, M. I., Selecting features for intrusion detection: A feature relevance analysis on KDD 99 intrusion detection datasets.

In Proceedings of the third annual conference on privacy, security and trust, 2005.

Mohadeseh Mir has MSc degree in Information Technology from the Graduate University of Advanced Technology, Iran. Her research interests include distributed systems, information security, cloud computing and IoT.

Hamid Reza Naji is associate professor of computer engineering at Graduate University of Advanced Technology, Iran. His research interests include embedded systems, distributed, parallel and multi-agent systems, networks, and security. Dr. Naji has a PhD in computer engineering from university of Alabama in Huntsville, USA. He is a professional member of the IEEE.