ISSN 2278-3091

Volume 8, No.1.5, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse6481.53019.pdf

https://doi.org/10.30534/ijatcse/2019/6481.52019

Analysis Against DDOS Flooding Attacks in Healthcare System using Artificial Neural Network

Ravi Tomar [1], Yogesh Awasthi [2]*

[1] School of Engineering & Technology ,Department of CS, Shobhit Institute of Engineering & Technology, Meerut, India

[2] School of Engineering & Technology, Department of CS, Shobhit Institute of Engineering & Technology, Meerut, India

*Present Address: Assistant Professor, Department of Information Technology, Lebanese French University, Erbil, KR-Iraq

ABSTRACT

The research on cyber security has gained more attention and interest outside the availability of computer security experts. Cyber security is not a single issue, but a series of highly different issues involving multiple threats. The data accommodation in health care system is growing continuously, which demanded a highly efficient and intelligent system to deal with the health records. The increase in the data increases the probability of affecting data by the cyber attacker. Therefore, it becomes essential to deal with cyber-attacks. This research focused on the utilization of cyber security for healthcare organization using machine learning approach. Our aim is to detect Distributed Denial of Service (DDoS) attack, which is one of the most commonly present cyber-attacks. This type of attack is designed to prevent genuine user from the required network resources. By using the concept of Artificial Neural Network (ANN), the system is trained based on the database related to the clinical record, financial record, individual record etc. During the data communication process, cross-validation is performed using ANN approach, which matched the data with the database and at last check the performance parameters. The experiment results indicate that there is an increase in the True Positive Rate (TPR) and False Positive Rate (FPR) of 0.27 % and 8.79 % respectively has been observed.

Key words: Cyber security, healthcare system, Distributed Denial of Service, Artificial Neural Network.

1. INTRODUCTION

Cybercrime/ computer crimes are illegal actions, which involve computers and their networks. The attacker affects the performance of the computer. Such crimes can pose a threat to financial health and hence to the security of the nation [1]. There is number of methods through which the cybercrime takes place, the most common causes are hacking, steal personal data, pornography and copyright violation. In case of intercepting confidential information, confidential issues arise [2]. One of the aspects that must be considered when considering certain tools for enhancing cyber security is the connectivity of users with the threats nature with its necessary countermeasures. Also, people adjust their ways based on the risk factor, which can they can bear [3]. Thus, risk perception plays an essential role in improving cyber security. Government agencies are also susceptible to cyber-attacks. For the last couple of years, it was found that approximately 70 % of institutions claim their security against the successful cyber-attack [4]. People around the world use the internet and other distinct system models to communicate, transfer and store data. Most data and information are private and very sensitive; therefore, protecting this data is compulsory. However, in the present time hacking has become very common [5-7]. In computer networks, hacking is a technical means of getting hold of victim's computer and connection system with malicious purposes, with the aim of collecting information to extort and destroy people's lives. Therefore, our main motive is to protect healthcare systems from cybercrime [8]. Due to the inherent weaknesses in its security posture, healthcare faces greater cyber risks than other sectors. It is one of the most targeted industries in the world; 81% of the 223 healthcare organizations have surveyed, and in 2015 alone, more than 110 million patient's information in the United States was leaked [9]. The common threats found in healthcare systems are listed in Table 1.

Table 1: Common and Emerging Cyber Threats in Healthcare

Cyber Threats in healthcare	*Description*
Data steal for financial purpose	Breaching patient's personal information related to their name, address and financial information for the purpose of money.
Data steal for impact	The theft might steal information related to the high profile patient such as celebrities, politicians that affects their profile.
Ransomeware	The attacker, block the patient or completely delete from its database until the patient has paid the entire fee.
Data corruption	The attacker changes the testing values for a reputed person gain
Denial of Service Attack	Interrupt the performance of an organization by flooding a number of requests

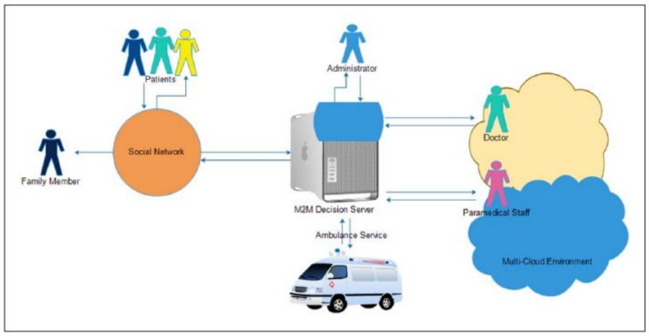


Figure 1: Healthcare System

To protect healthcare system as shown in Figure 1 from distributed denial-of-service (DDoS), we used an artificial intelligence technique. The detail description of those is provided in section III. As shown in above figure 1, a patient registers into the healthcare system through the social network. Using wireless technology, the patient is capable to interact with doctor, other patient, ambulance services etc [10-11].

2. RELATED WORK

To secure information from threats is a major problem for most of the IT companies. Security of corporate data is extremely important to ensuring business continuity. The main reason is that information is an asset to the organization or any other institutes and therefore needs to be adequately protected. Therefore, it becomes essential to protects information from a wide range of threats to ensure business continuity, minimizing job losses, and achieving strategic advantages to maximize profit and business opportunities. Von et al. [12] have stated information security as well as ICT security. The document further argued that cybersecurity is different from information security, although it is often used as a similar term for information security. Information security is the protection of active information from possible damage as a result of various threats and vulnerabilities. Cybersecurity, on the other hand, is not only the protection of the cyberspace itself but also the protection of those working in cyberspace and any assets that can be acquired in cyberspace. Tsai et al. [13] have analyzed weblog posts for multiple types of cybersecurity threats that are similar to the attacks which have to be detected. Existing intelligence research has focused on examine news/ forums related to cybersecurity, but very few people have looked at websites. A probable latent semantic analysis tool has been used to identify keywords from cybersecurity websites for specific topics. After that, the researchers have presented the blogosphere with keywords that can be measured in terms of topics and thus follow popular conversations along its topics in the blog environment. The information retrieval from the weblogs can be increased by using a probabilistic approach. Javaid et al. [14] have discussed a variety of security attacks to an Un-named vehicle system. The designed system has been protected from various security attacks and a secure path has been provided to the communicating UAVs. The designed model has assisted the users of UAV systems to understand the system's threat profile so that the user can address a variety of system weaknesses, recognize high-priority threats, and use methods to reduce those threats. Goztepe, K. [15] have designed a fuzzy rule-based technical approach to provide security to cyber system, the designed expert system is known as Fuzzy Rule-Based Cyber Expert System (FRBCES). To compute complex processes, a rule-based fuzzy system has been used. Jing et al. [16] have presented a secure network against DDoS flooding attack using Chinese Remainder Theorem based Reversible Sketch (CRT-RS) to store past traffic information. For the detection of DDoS attack Modified Multi-chart Cumulative Sum (MM-CUSUM) technique has been used. From the experiment, the authors have analyzed that the presented wireless network can be used effectively to handle large amount of network traffic.

3. MATERIALS AND METHODS

This section demonstrated the detailed description of the techniques used with their working algorithms of the designed framework; mainly develop for a healthcare system with multiple patients, doctors and database management system. The patient share data with doctors and appropriate action has been performed when required.

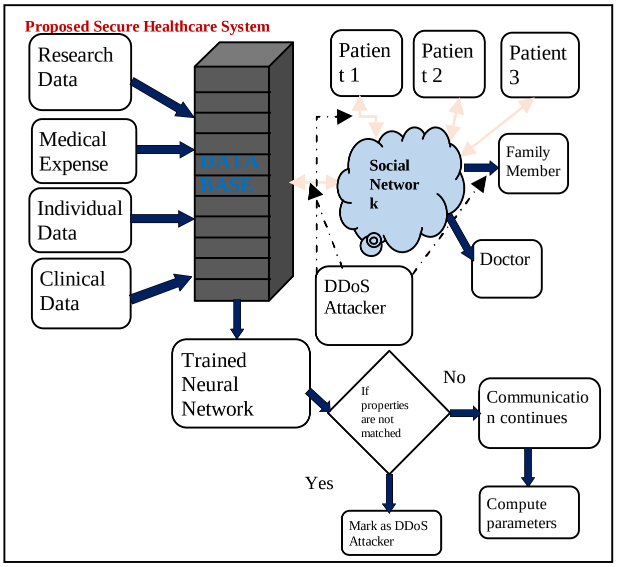


Figure 2: Proposed Healthcare System

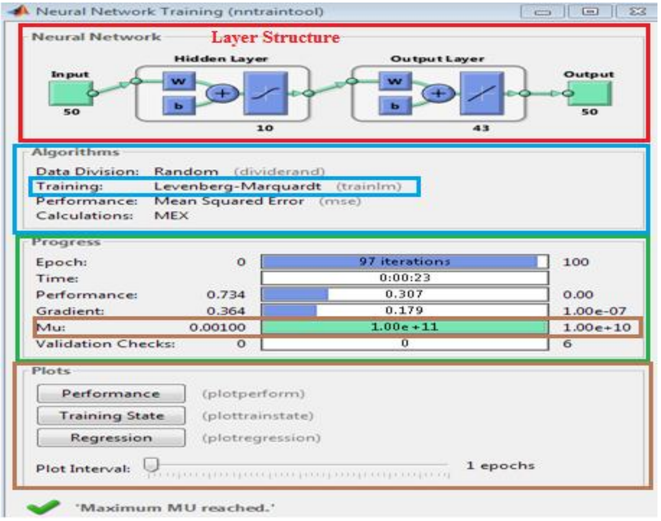
Figure 2 illustrated a detailed overview of the entire work. The health data such as research data, medical expenses that are financial record, individual data (name, address, email address, contact number) and clinical data (test readings) are saved in the organization database. The stored information is shared by the patient as well as their family members along with doctors. In case of any emergency, the signal to the organization has been sent through internet. The shared data between organization and patient can be affected or altered by the attacker (DDoS). Therefore, to protect, the data and for successful communication, artificial neural network approach is used. The system is trained using ANN. Therefore, if the system found unmatched properties of patient, which is not available in the database, then considered as DDoS attacker otherwise pass the data. At last, performance parameters are evaluated to determine the efficiency of the present work.

A.DDoS Attack

A DDoS attack is a malicious attempt in order to disturb normal communication between patient and healthcare system. The DDoS attacker behaves like a genuine user and starts dropping data or stealing confidential information related to the patient [17]. These threats affect network bandwidth by assigning the actual user's available bandwidth to unauthorized users. The impact of this attack will temporarily block the network from normal communication. A DDoS attack can affect a single patient or multiple patients at the same time. For example, an attacker can affect a system by exhausting limited wireless resources (such as bandwidth, data savings areas, battery consumption, etc) [18].

B. Artificial Neural Network (ANN)

It is an intellectual algorithm inspired by the human biological neural network, comprises of human brain. In this each neuron is interconnected to each other and passes information in a similar fashion as that of synapses in human brain [19-20]. The interconnection is known as edge and corresponds with weight. The weight is adjusted based on which the learning capability of ANN is analysed. In this research, the system is trained by applying input as the health data or the patient-related confidential information provided at the input layer of ANN. After training, the system is ready for detecting DDoS attack. The trained structure of ANN during research work is depicted in Figure 3.



Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

```
Epoch:                 0   97 iterations   100
Time:                      0:00:23
Performance:       0.734   0.307           0.00
Gradient:          0.364   0.179           1.00e-07
Mu:              0.00100   1.00e+11        1.00e+10
Validation Checks:     0   0               6
```

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)
Plot Interval: 1 epochs

✓ 'Maximum MU reached.'

Figure 3: Trained ANN Structure

Figure 3 comprises of four different panels named as neural network, Algorithms, progress and plots. Under the neural network, the information such as number of layers, input and output data is shown. From the algorithm section, it is clear that the data division is performed randomly and trained using Levenberg-Marquart principle with Mean Square Error (MSE) as a performance parameter. During training, the progress is shown under progress panel, which indicates that after completing mutation, the system is trained. Therefore, every time whenever there is a communication between patient and doctor, or the other members of organization, ANN cross-validate the data with its database, if any mismatching found, and then indicated that it is not a genuine user. Kindly don't share your data. In this way, the system is protected from unauthorized access.

Algorithm: ANN

Input: Patient information (medical expenses, financial record, and clinical data) as a Training Data (T), Target (G) and Neurons (N)
Output: Detected DDoS Threat

```
Initialize ANN with distinct constraints – Epochs (E)
                                         – Performance parameters: MSE, Gradient, Mutation and Validation Points
For each set of T
    $Group = Categories\ of\ Training\ data$ (Normal and affected data)
End
Initialized the ANN using T & G
Net = Newff ($T, G, N$)
Set the training constraints as per desire and train the network
Net = Train ($Net, T, G$)
Classify = malicious data within the communication process
If Classify = True
Transmit data to the destination user
Else
Do not pass data
End
Return; a secure network after detection of DDoS threat
End
```

At last, the computation parameters are measured to evaluate the efficiency of the proposed system, which is discussed in the following section.

4. RESULT AND DISCUSSIONS

This section deals with the simulation results performed in the presence of DDoS attack and after preventing health care network from DDoS attack. The entire simulation has been performed in MATLAB simulator. The following parameters are evaluated during the testing process.

A. True Prostive Rate (TPR)

It represents the rate of correctly identified malicious data and evaluated using the formula;

TPR=TP/(TP+FN)

Here; TP • True positive

FN • False Negative

B.False Prostive Rate (FPR)

It represents the rate of incorrectly identified as attacker data by the trained neural network. It is examined using the formula;

FPR=FP/(FP+TN)

TN • True Negative

FP • False positive

Table 2: Computed Parameters

Number of Iterations	TPR	FPR	Throughput × 10^4	Computation Time (ms)
1	98.65	0.65	9	430
2	98.79	0.67	8.5	455
3	99.02	0.64	8.88	487
4	99.57	0.63	7.9	358
5	97.86	0.62	8.2	397
6	98.77	0.58	8.5	502
7	98.99	0.57	8.9	497
8	99.01	0.59	9.0	512
9	99.08	0.55	7.5	567
10	98.74	0.52	7.2	497

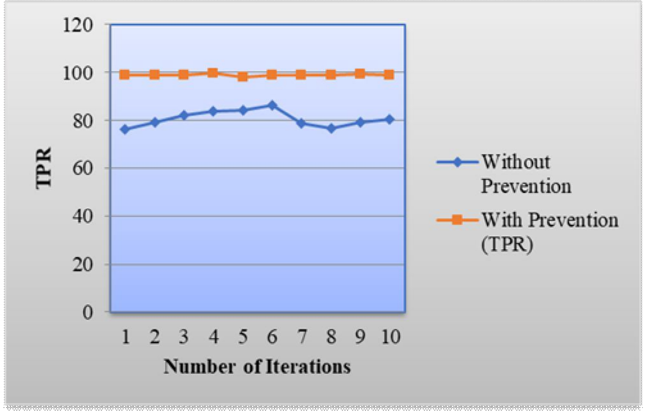


Figure 4: TPR

Figure 4, represents the truly identified malicious/ affected health care data during the communicating process. From the figure, it is clearly seen that initially, the identification rate of truly identified DDoS attacker data increases up to 4th iteration and then there is sudden fall in the TPR has seen. This is due to the fact that the trained ANN structure cannot identify the affected data and hence steal the information. From the graph it has been analysed that when no prevention mechanism is used the TPR is less compared to the TPR obtained with prevention technique.

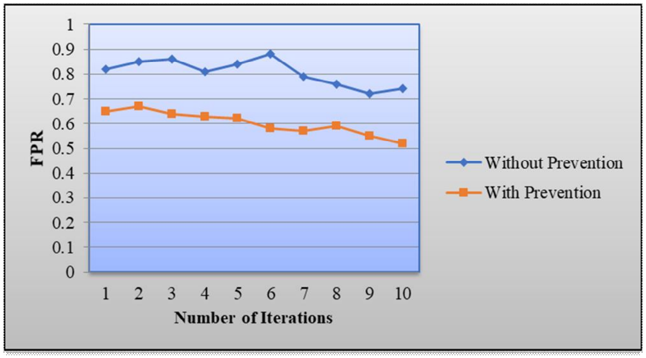


Figure 5: FPR

The comparison of FPR with and without FPR is shown in figure 5. It represents the incorrectly identified the data as an affected data by the DDoS attacker. From the graph, it has been examined that the false detection rate of affected data is less using ANN approach compared to without prevention algorithm. The average of FPR examined with and without prevention approach is 0.807 and 0.602 respectively. Thus there is an enhancement of about 25.4 % while utilizing ANN approach in the proposed healthcare system.

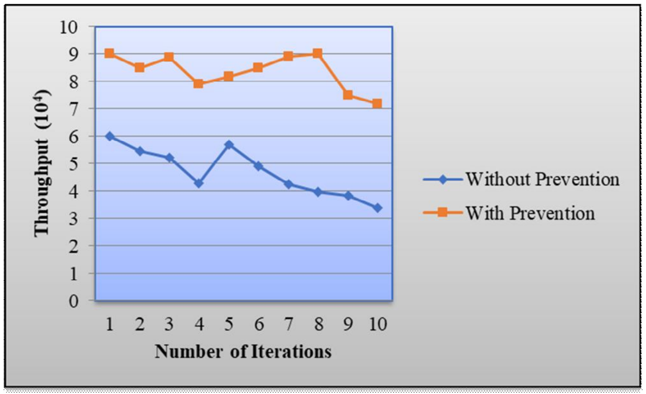


Figure 6: Throughput

Figure 6 represents the relationship between throughput and the number of iteration. The graph indicates that that maximum throughput is attained at 8th iteration, which is about 9 × 104. This is due to the successful transmission of data after identifying the attacker from the network. Also, the comparison between the throughput obtained with and without prevention approach is depicted by the red colour and the blue colour respectively. The average of throughput for 10 number of iteration without and with prevention is 4.697 × 104 and 8.358× 104 respectively. Thus, there is an improvement of 77.94 %.

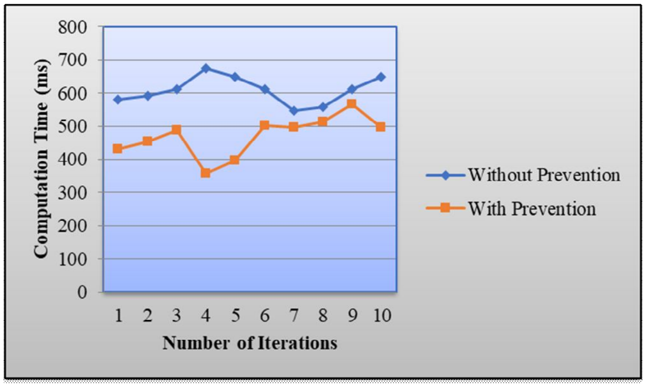


Figure 7: Computation Time

We also examined the computation time of the proposed healthcare detection and protection model for each iteration and the result part is illustrated in Figure 7. The results indicate that using ANN approach the detection method of analysing DDoS attack takes less time compared to the normal system. Therefore, based on the above values, the designed system is suitable for handling large amount of data traffic.

The show the effectiveness and the accuracy of the designed protection system, comparison of computed parameters is performed with the existing work performed by (Jing et al. 2019). The comparative parameters are listed in Table III.

Table 3: Comparison of Computed Results with Existing Work

Parameters	**TPR**		**FPR**	
	Proposed Work	**Jing et al. [16]**	**Proposed Work**	**Jing et al.**
Average Value	98.84	98.57	0.602	0.66

The comparison of computed TPR and FPR values in contrast to the existing work performed by Jing et al. [16] is shown in Figure 8 and Figure 9 respectively. The graph shows that the proposed system performs well while utilizing ANN as a machine learning approach and provides a secure healthcare system against DDoS attack. The percentage increase in the detection rate of TPR and FPR against the proposed technique of about 0.27 % and 8.79 % has been attained.

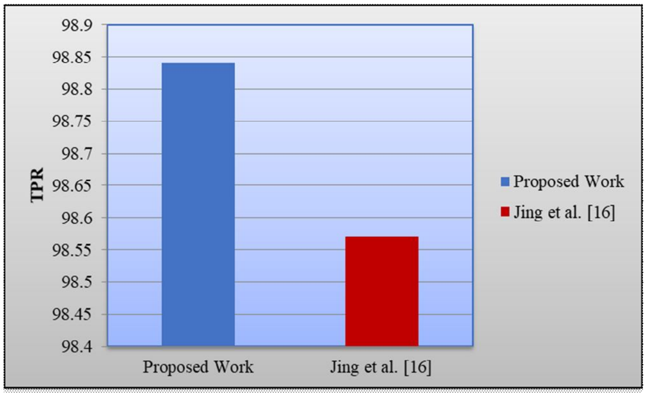


Figure 8: Comparison of TPR

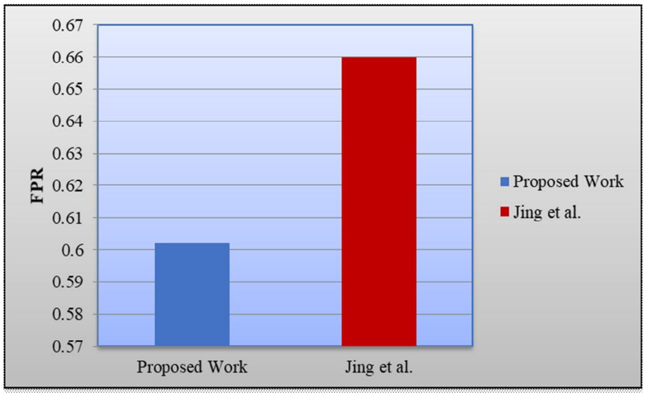


Figure 9: Comparison of FPR

5. CONCLUSION

The present transition to health care organization is based on the flow of information in real-time, the integration of information and communication technologies with physical equipment to provide a coherent system that can better track the patient's health in real-time and improve overall health services. As data communication is performed through wireless means therefore, the tendency to affect or steal data by an unauthorized person increases. This problem has been resolved by designed a secure healthcare system based on ANN approach. ANN has feature like it can handle large amount of data in less computation time and also works with nonlinear data. This feature has been used and a highly efficient system with TPR of 98.84% has been designed.

REFERENCES

1. Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., & Luo, H. H. (2015). Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications, 22(4), 104-112. https://doi.org/10.1109/MWC.2015.7224734
2. Kernan, W. N., Ovbiagele, B., Black, H. R., Bravata, D. M., Chimowitz, M. I., Ezekowitz, M. D., ... & Johnston, S. C. (2014). Guidelines for the prevention of stroke in patients with stroke and transient ischemic attack: a guideline for healthcare professionals from the American Heart Association/American Stroke Association. Stroke, 45(7), 2160-2236.
3. Loganovsky, K., & Bomko, M. (2009). National mental health care system following radiation accident and radiological terrorist attacks.
4. Chen, L., & Hoang, D. B. (2011, September). Novel data protection model in healthcare cloud. In 2011 IEEE International Conference on High Performance Computing and Communications (pp. 550-555). IEEE. https://doi.org/10.1109/HPCC.2011.148
5. Manogaran, G., Thota, C., Lopez, D., Vijayakumar, V., Abbas, K. M., & Sundarsekar, R. (2017). Big data knowledge system in healthcare. In Internet of things and

big data technologies for next generation healthcare (pp. 133-157). Springer, Cham.

6. Zhang, L., Zhang, Y., Tang, S., & Luo, H. (2017). Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. IEEE Transactions on Industrial Electronics, 65(3), 2795-2805.
7. Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. Journal of medical systems, 40(12), 263. https://doi.org/10.1007/s10916-016-0597-z
8. Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), 1656-1665. https://doi.org/10.1109/TII.2018.2794996
9. Huang, H., Gong, T., Ye, N., Wang, R., & Dou, Y. (2017). Private and secured medical data transmission and analysis for wireless sensing healthcare system. IEEE Transactions on Industrial Informatics, 13(3), 1227-1237.
10. Shakeel, P. M., Baskar, S., Dhulipala, V. S., Mishra, S., & Jaber, M. M. (2018). Maintaining security and privacy in health care system using learning based deep-Q-networks. Journal of medical systems, 42(10), 186. https://doi.org/10.1007/s10916-018-1045-z
11. Tomar, Ravi, and Yogesh Awasthi. "Prevention Techniques Employed in Wireless Ad-Hoc Networks." 2019 International Conference on Advanced Science and Engineering (ICOASE). IEEE, 2019.
12. Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0 (pp. 103-126). Springer, Cham. https://doi.org/10.1007/978-3-319-50660-9_5
13. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004
14. Tsai, F. S., & Chan, K. L. (2007, April). Detecting cyber security threats in weblogs using probabilistic models. In Pacific-Asia Workshop on Intelligence and Security Informatics (pp. 46-57). Springer, Berlin, Heidelberg.
15. Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In 2012 IEEE Conference on Technologies for Homeland Security (HST) (pp. 585-590). IEEE. https://doi.org/10.1109/THS.2012.6459914
16. Goztepe, K. (2012). Designing fuzzy rule based expert system for cyber security. International Journal of Information Security Science, 1(1), 13-19.
17. Jing, X., Yan, Z., Jiang, X., & Pedrycz, W. (2019). Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch. Information Fusion, 51, 100-113. https://doi.org/10.1016/j.inffus.2018.10.013
18. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2), 113-122.
19. Nor Shazwina Mohamed Mizan, Muhamad Yusnorizam Ma'arif, Nurhizam Safie Mohd Satar and Siti Mariam Shahar, "CNDS-Cybersecurity: Issues and Challenges in ASEAN Countries" in IJATCSE, Volume 8 No. 1.4 (2019) S I, pp. 113 - 119 https://doi.org/10.30534/ijatcse/2019/1781.42019
20. Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in Wireless Sensor Networks. Procedia Computer Science, 79, 715-721
21. Van Gerven, M., & Bohte, S. (2017). Artificial neural networks as models of neural information processing. Frontiers in Computational Neuroscience, 11, 114. https://doi.org/10.3389/fncom.2017.00114