Intelligent Intrusion Detection System for Healthcare Using Fuzzy Neural Networks

Rehab Flaih Hasan shatha h. Jafer [*]
Computer Sciences Department - University of Technology
110019@uotechnology.edu.iq shatha.h.jafer@uotechnology.edu.iq

Abstract:
Healthcare facilities in the modern day are a significant problem, particularly in developing nations where distant locations are hampered by a scarcity of high-quality hospitals and medical professionals. As artificial intelligence has revolutionized several fields of life, it has also had a positive impact on health. The existing architecture is facing several issues for the conventional telemedicine store-and-forward method. These include the requirement for a local health centre with dedicated staff, the need for medical equipment to prepare patient reports, the time constraint of 24–48 hours in receiving diagnosis and medication details from a medical expert in the main hospital, the cost of local health centres, and the requirement for a Wi-Fi connection, among others. Medical gadgets equipped with wireless communication capabilities allow for remote monitoring and are becoming more linked to one another and the Internet. Internet of Intelligent Things-enabled Medical and connected medical devices, also known as IoMT, have allowed continuous real-time patient monitoring, improved diagnostic accuracy, and more effective therapy than ever before. Although these devices have various advantages, they also create new attack surfaces, resulting in an increased number of security and privacy risks, which must be addressed. Attacks against medical equipment that are linked to the Internet have the potential to inflict significant bodily injury and even death on the patients who are targeted. In this study, we examine the strategies that may be used to provide advice on how to safeguard a network of connected medical devices.

Keywords : Intrusion Detection, Healthcare systems**,** Machine Learning Techniques**.**

نظام ذكي لكشف التسلل للرعاية الصحية باستخدام الشبكات العصبية الغامضة

رحاب فليح حسن شذى حبيب جعفر
قسم علوم الحاسوب – الجامعة التكنولوجيا

الخلاصة :
تمثل الرعاية الصحية في العصر الحديث مشكلة كبيرة، لا سيما في الدول النامية حيث تعوق المواقع البعيدة ندرة المستشفيات عالية الجودة والمهنيين الطبيين. نظرًا لأن الذكاء الاصطناعي أحدث ثورة في العديد من مجالات الحياة، فقد كان له أيضًا تأثير إيجابي على الصحة. تواجه البنية الحالية العديد من المشكلات المتعلقة بطريقة التخزين وإعادة التوجيه التقليدية للتطبيب عن بعد. وتشمل هذه المتطلبات وجود مركز صحي محلي يضم موظفين متخصصين، والحاجة إلى معدات طبية لإعداد تقارير المرضى، والقيود الزمنية البالغة 24-48 ساعة لتلقي التشخيص وتفاصيل الدواء من خبير طبي في المستشفى الرئيسي، وتكلفة العلاج المحلي. المراكز الصحية، وشرط الاتصال بالواي فاي، من بين أمور أخرى. تسمح الأدوات الطبية المجهزة بقدرات الاتصال اللاسلكي بالمراقبة عن بعد وأصبحت أكثر ارتباطًا ببعضها البعض وبالإنترنت. أتاحت الأجهزة الطبية والأجهزة الطبية المتصلة بإنترنت الأشياء الذكية، والمعروفة أيضًا باسمIoMT ، مراقبة مستمرة للمريض في الوقت الفعلي، وتحسين دقة التشخيص، وعلاج أكثر فعالية من أي وقت مضى. وعلى الرغم من أن هذه الأجهزة تتمتع بمزايا مختلفة، إلا أنها تنشئ أيضًا أسطح هجوم جديدة، مما يؤدي إلى زيادة عدد المخاطر الأمنية والخصوصية، والتي يجب معالجتها. إن الهجمات ضد المعدات الطبية المرتبطة بالإنترنت لديها القدرة على إلحاق إصابات جسدية كبيرة وحتى الموت للمرضى المستهدفين. في هذه الدراسة، نقوم بدراسة الاستراتيجيات التي يمكن استخدامها لتقديم المشورة حول كيفية حماية شبكة من الأجهزة الطبية المتصلة.

[*] Corresponding author : shatha h. Jafer

الكلمات المفتاحية: كشف التسلل، أنظمة الرعاية الصحية، تقنيات التعلم الآلي.

1. **Introduction**

omputer network security has been a hot topic of study for many years. Organizations realize that information and network security technologies are critical in securing their data. Information resources that are compromised in any way are classified as security breaches or intrusions, regardless of whether they are successful or unsuccessful. New threats are being confronted by businesses daily. An intrusion Detection System is one method of addressing this issue (IDS).

The IDS employs a method known as machine learning to identify threats. This branch of computer science is focused on developing algorithms and techniques that enable computers to learn on their own and continually improve themselves to do their duties more quickly and effectively. Machine Learning Intrusion Detection Systems have shown impressive results in .recent years, providing excellent accuracy IDS is a security method that seeks to identify different forms of intrusion. Techniques for detecting suspicious behaviour on both the host and network levels are included in this collection [2].

The influence of connected healthcare systems (CHS) on the sharing of patient health information (PHI) across various healthcare providers across medical technology platforms is also examined in another research.

In this research, the technology used to monitor the physical status is the primary focus of the investigation.

The study's findings on cybersecurity-related dangers focused on threats from inside the system and external threats, including malware and data transfers .

The authors' "Stacked autoencoder" strategy to secure PHI as described in the study's findings as a means of countering several sorts of possible security attacks .

A more efficient IDS may be achieved by cutting down on the burden of the IDS and using ways that best use their resources like they did when they implemented their stacking approach[1].

Researchers are also studying diverse techniques to IDS. Specific anomaly-based intrusion detection systems differed from those without anomaly-based methodologies in several respects .

They also wanted to see any additional problems with implementing IDS .

The limitations of machine learning and the technique used by many systems that contained principal component analysis were among the authors' noted issues .

It has been established that machine learning strategies for solving IDS problems are more flexible than neural network techniques compared to those that use machine learning techniques for solving IDS problems[1].

2. **Related work**

Researchers were interested in observing the influence of intrusion detection systems (ids) on mobile healthcare information systems, which serve as a defence mechanism against digital threats during data transmission .

Seven different intrusion detection systems (IDS) were inspected and compared against one another in terms of their capacity to secure patient health information (PHI) and healthcare data from outside attackers trying to access the system. In addition, the authors offer a new strategy for using a recurrent neural network, which they believe will be successful (RNN). Using a third-party dataset, the researchers concluded that their new approach enhanced detection rates while simultaneously decreasing false alarm rates via neural networking techniques.

Similar findings were shown in the conclusions of a study undertaken by researchers who investigated how healthcare data included inside commonly used apps may be exposed due to data breaches and a failure to maintain patient information security. An appliance known as a Wireless Body Area Network (WBAN), which patients use in combination with their electronic health records, makes it possible to monitor patients' health information (PHI) from a remote location (EHR) .To protect the confidentiality of PHI .To do this, the researchers used a study review procedure, which included examining and comparing many papers that took comparable approaches to the subject matter[10].

According to another article, there are ways to avoid intrusion detection in the event of a computer-based hack .It is possible to create an alerting system for users if two different intrusion detection techniques, such as anomaly-based and specifically-misuse approaches, are coupled .More articles are compared and contrasted in the next section to show the differences between the two. To decrease false alarms in intrusion detection systems (IDS), various techniques, including fuzzy logic and soft computing, may be used while still ensuring that legitimate detection requirements are met[11].

A study of the influence of IDS on various neural network systems that use fuzzy logic-based technologies was presented in an article. Researchers wanted to see whether the evolutionary fuzzy logic procedures used in IDS affected pairwise learning. Neural networking in IDS was beneficial in gaining a better understanding of such activities, allowing researchers to identify which components of information transfer should be given special attention given the nature of the data being sent[12].

Compare the effects of IDS on medical and network data in healthcare systems. Various medical environments, including hospitals and clinics, are discussed privacy and security problems related to patient health information (PHI) and other types of personally identifiable information. The authors constructed a bedside EHMS monitoring system that could track network flow data for patients during their stay. An automated network server then reviewed the data and alerted a third-party security reviewer if there was a risk of patient information being compromised. Overall, this research indicated a significant rise in the percentage of cyberattacks that were disrupted, ranging from 7% to 25%. As a result, this suggests that third-party EHMS security solutions have a positive influence[13].

Society's increasing reliance may improve information security on mobile devices and devices that are easy to carry about. As a result, the authors studied wearable medical data exchanges employing cloud-based medical data exchanges. There are two kinds of approaches to evaluate cloud-based data: First, cloud-based data was communicated through trusted devices, while the second model enabled similar-prognosis and-diagnosis patients to discuss and talk about their experiences via a distinct cloud-based platform. The authors used information from these two models to categorize them into three different aspects depending on the various forms of communication they may be deemed to be. Thus, they may take a fresh look at the problem by using an IDS strategy that combines many cloudlet devices and exchanges information among them to give a proactive defence against breaches[10].

3. Intrusion detection system

Intrusion Detection Systems (IDS) are algorithms that scan a network system for malicious assaults or other abnormal activities. Anomaly-based and signature-based systems are the two basic kinds of intrusion detection and prevention systems.

Anomaly-based systems make a model of the system's normal behaviour and compare it to the behaviour that is being monitored. This model is used to create a baseline model. If a specific action is different from usual, the IDS looks into it and puts it in a particular category. The primary benefits of these systems are their ability to identify harmful assaults that the system was unaware of before and their ability to operate in a real-time environment. They may, however, generate a large number of false positives as a result of noise or other factors in the data .It appears as follows: Figure 1 demonstrates the overall framework of an anomaly-based Intrusion Detection System.

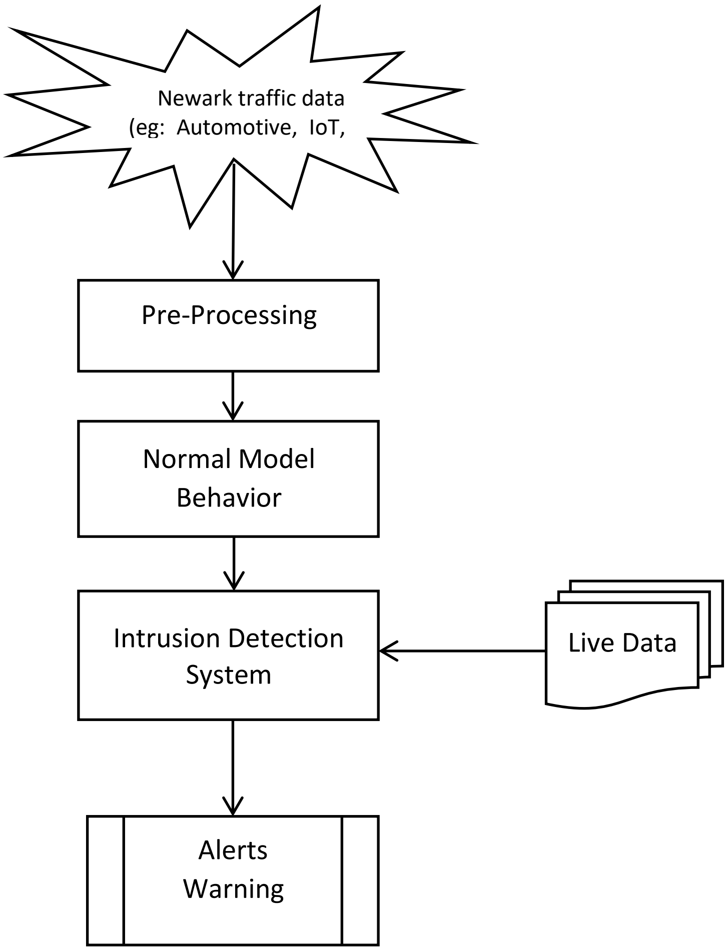

Figure (1) : IDS Architecture[3]

Signature-based systems look for predefined and preset attack patterns referred to as probes and sweeps in the data. These factors serve as the foundation for issuing an alert in the event of attack behaviour. While signature-based IDS are effective when attack signatures are known in advance, they fail miserably when no previous information of the assaults is available. As a result, the disadvantage of such systems is the constant need to update the database of attack signatures. Additionally, signature-based IDS are inefficient against self-modifying assaults[3].

4. Intrusion Detection System using Machine Learning Techniques

Application machine learning methods for intrusion detection is based on automatically building the model from scratch using a training data set. It is possible to define each data instance using a set of characteristics (features) and the associated labels in this data set, which comprises a collection of data instances. Different factors, such as categorical and continuous, may describe the data. The nature of the characteristics being investigated determines the usefulness of anomaly detection methods. For example, distance-based approaches were initially designed to function with continuous features and, consequently, do not consistently provide satisfactory results when applied to categorical characteristics .

Most of the time, the labels associated with data instances take the form of binary values, such as normal or abnormal .

On the other hand, some researchers have deployed various sorts of assaults, such as denial-of-service (DoS), U2R, R2L, and Probe, rather than the anomalous label .

Learning approaches can give more information on the different sorts of anomalies in this manner. However, experimental findings reveal that existing learning approaches are not accurate enough in identifying the types of abnormalities seen in the field. Furthermore, human specialists generally do labelling manually means that getting an exact labelled data set that is representative across all sorts of behaviours is a time-consuming and costly endeavour. Because of this, three operating modes for anomaly detection algorithms are established depending on the availability of labels: Supervised Learning, Unsupervised Learning, and Semi-supervised Learning. Supervised Learning is the most often used mode[4].

5. Application of Machine Learning Approaches in Intrusion Detection System

The foundation of machine learning approaches is establishing an explicit or implicit model. A distinguishing feature of these approaches is the need for labelled data to train the behavioural model, a process that puts a high demand on available resources. However, in many circumstances, the application of machine learning principles is identical to that of statistical approaches, despite the former focusing on developing a model that improves its performance based on prior findings. As a result, machine learning for IDS can adapt its execution approach in response to new inputs. This property may make it beneficial to use such methods in all circumstances.

1.1 Supervised Learning

Classification is another name for guided learning. It is important to label each instance in the training phase of supervised learning data. Sustained learning algorithms may be found . Nearest Neighbour, Support Vector Machines (SVMs), Hidden Markov Models (HMMs), Bayesian Networks (Bayesian Trees), and K-nearest neighbours are just a few of the terms associated with artificial neural networks. In addition, boosting, Supervised learning methods include ensemble classifiers (Bagging, Boosting), linear classifiers (Logistic regression, Fisher linear discriminant, Naive Bayes classifier, Perceptron, SVM), and quadratic classifiers are widely used in many fields.

1.2 Unsupervised Learning

Data instances in unsupervised learning are not labelled. Clustering is a standard method of implementing this strategy.

Cluster analysis (K-means clustering, fuzzy clustering), hierarchical clustering, self-organizing maps, the Apriori algorithm, the Eclat algorithm, and outlier detection are some of the more prevalent unsupervised learning methods used (Local outlier factor).

1.3 Reinforcement Learning

Reinforcement learning is the process through which a computer interacts with its surroundings in order to accomplish a goal. A reinforcement strategy may request that a user (e.g., a domain expert) name an instance, which may be drawn from a collection of unlabelled cases[5].

6. Healthcare

Healthcare is one of the most pressing issues that can be addressed more effectively with the Internet of Things and associated technologies .

Systems and associated technologies based on the Internet of Things (IoT) offer a great deal of promise to enhance healthcare delivery systems .

There are many other kinds of healthcare applications offered by academics, including e-health, community health, home health monitoring, telemedicine, and clinical assistance for clinicians, to name a few examples .

The critical contribution of this study is the development of gadgets that assist in monitoring, management, and communication amongst various players in the healthcare sector[2].

Signature-based systems look for predefined and preset attack patterns referred to as probes and sweeps in the data. These factors serve as the foundation for issuing an alert in the event of attack behaviour. While signature-based IDS are effective when attack signatures are known in advance, they fail miserably when no previous information of the assaults is available. As a result, the disadvantage of such systems is the constant need to update the database of attack signatures. Additionally, signature-based IDS are inefficient against self-modifying assaults[3].

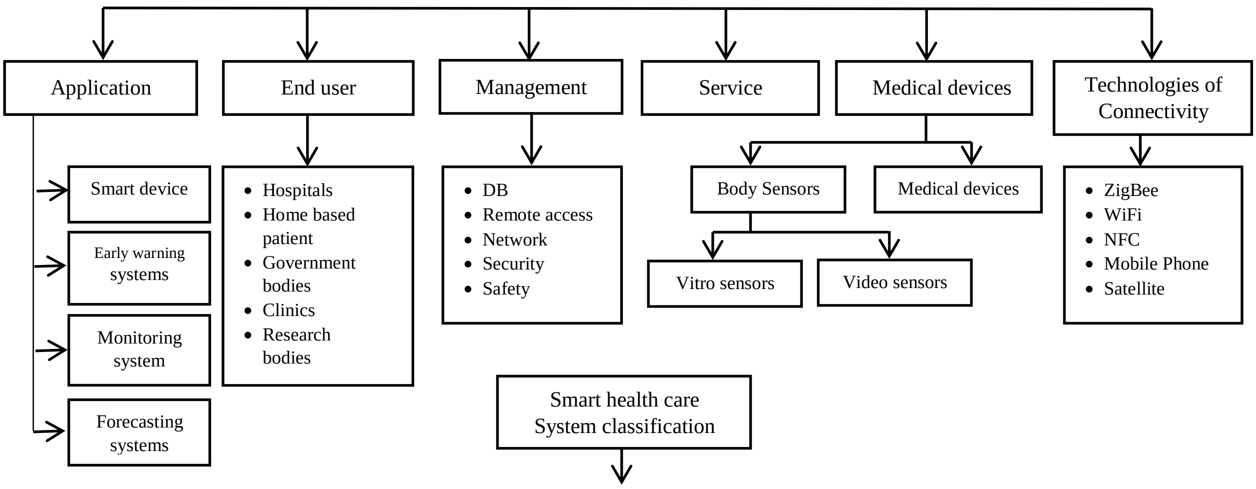

Figure (2) : Smart Health Care System Classification

7. Fuzzy neural networks

In general, neural networks and neuro computations imply an implicit nature of information being learned from a family of training patterns and dispersed along with the structure's connections throughout their learning. Adopting this perspective may consider neural networks structure-free and entirely distributed models.

The overall trend toward combining fuzzy sets with neural networks dates back to the early stages of fuzzy set research. Nowadays, the breadth of available techniques is rather remarkable. This section will examine the synergy between fuzzy sets and neural networks from a system modelling and fuzzy simulation viewpoint. By establishing a suitable degree of abstraction, this sort of environment enables us to investigate specific well-known structures (such as fuzzy controllers or pattern classification schemes, to mention a few) more systematic and universally.

The fundamental premise behind fuzzy models is that they are produced and examined at the level of conceptual aggregates such as linguistic labels. Fuzzy modelling is concerned with this level of modelling. The fuzzy sets employed in their implementation form a so-called cognitive flame (fuzzy partition). Using a suitable selection of this flame, one may quickly amplify or suppress (hide) a large number of subtleties communicated by the data, as well as erase associations that would otherwise be viewed as meaningless at a preselected degree of generality. Fuzzy models may be thought of succinctly as modelling systems composed of three obviously distinct conceptual elements.

- Input Interface
- Processing Block.
- Output Interface.

Synergistic links exist between fuzzy sets and neural networks .On the one hand, we can see how neural networks augment the numerical processing of fuzzy data. These applications include global characteristics such as elicitation of membership functions and realization of mappings between fuzzy sets used to construct inference processes. On the other hand, there are instances when domain knowledge is defined in fuzzy sets and then used to improve the learning algorithms of neural networks or their interpretation skills, for example. The most apparent application areas include pattern recognition and control[6].

8. Fuzzy logic techniques

Fuzzy logic is developed from fuzzy set theory, which allows for approximate reasoning rather than an exact deduction from classical predicate logic. Thus, fuzzy approaches are applied in anomaly detection primarily because the characteristics under consideration may be thought of as fuzzy variables[7]. The use of fuzzy logic to computer security was suggested for the first time in[8]. The Fuzzy Intrusion Recognition Engine (FIRE) is presented in [9] for identifying intrusion activities, and the anomaly-based IDS is implemented utilizing data mining methods and fuzzy logic. The fuzzy logic component of the system is in charge of managing both the massive number of input parameters and the inaccuracy of the input data. COUNT, UNIQUENESS, and VARIANCE are three fuzzy qualities employed in this study. The built fuzzy inference engine detects intrusions using five fuzzy sets for each data piece (HIGH, MEDIUM-HIGH, MEDIUM LOW, and MEDIUM-LOW) and appropriate fuzzy rules. The authors do not specify how they obtained their fuzzy set in their study. However, the fuzzy set is critical for the fuzzy inference engine, and in certain circumstances, a genetic algorithm may be used to find the optimal combination. The suggested system is evaluated using data obtained from the local area network at Iowa State University's College of Engineering, and the findings are presented in this study. Because the conclusions given are descriptive rather than numerical, it is difficult to assess their performance.

9. System Design For Intrusion Detection System

Figure 3 illustrates the intrusion detection system's architecture. It is divided into the following major modules.

8.1. Preprocessing Phase

IDS in real-time (online): - During this phase, packet sniffing tools (for example, Wireshark, Capsa) are used to collect packet information such as IP/TCP/ICMP headers from individual packets. Following that, segment the packet header with source addresses, destination addresses, etc. This step necessitates the use of specific strategies for determining the fundamental characteristic. Additionally, determining if the packet is legitimate or malicious.

IDS for offline use: - During this phase, packets are captured from datasets (for example, the KDD dataset/NLS KDD) to serve as the IDS's data source.

8.2. Classification

In the classification step, use the data collected in the preceding phase to determine if the packet is standard or attacked. Then, the associated algorithms categorize the packet into comparable groups based on the feature values .

It is composed of two stages: (a) Training data (b) Testing data

During the training phase, a response class is supplied together with packet characteristics that aid in the formulation of rules determining mapping domains. These guidelines may be modified or updated as a result of further training. Each algorithm has its own categorization approach.

During the Testing Phase, untrained data is fed into the system to determine whether or not genuine responses are produced. The system procedure is carried out by supplying input in the form of packets without defining a response class.

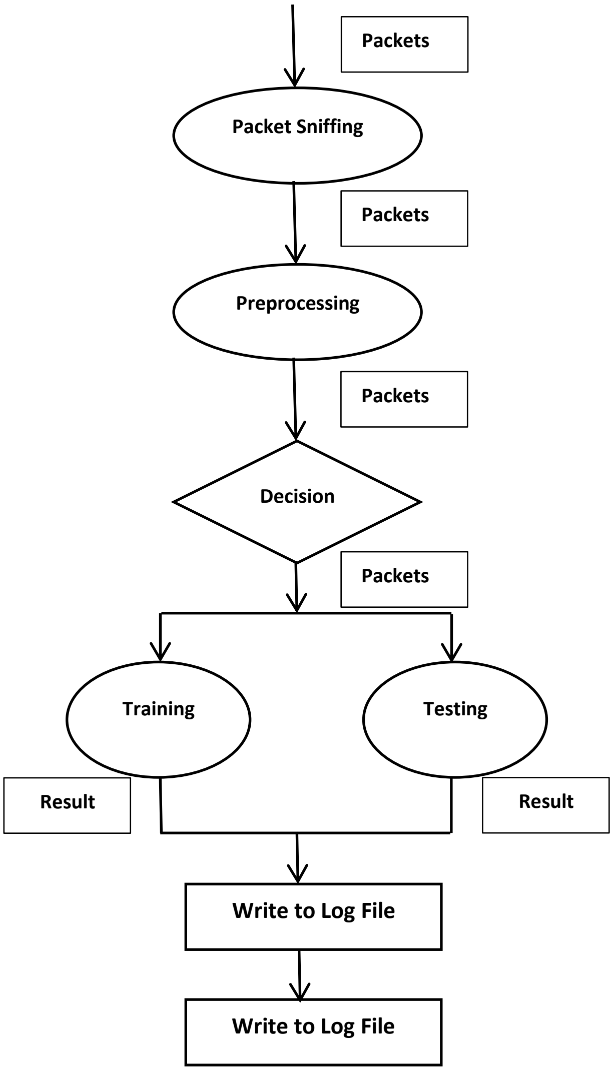

Figure (3) : System Design for IDS

8.3. Post Processing

The outcome of the pre-processing step is compared to the answer class, and the system's performance is quantified in terms of accuracy and false alarms. True Positive, True Negative, False Positive, and False Negative are the four types.

8.4. Reducing False Alarms

If the system continues to generate false alerts for any of the algorithms, more training is required. This is the machine learning process; the system will continue to learn without human intervention. As a result, no update is necessary[3].

[1] B. Ramasamy and A. Z. Hameed, "Classification of healthcare data using hybridised fuzzy and convolutional neural network," Healthc. Technol. Lett., vol. 6, no. 3, pp. 59–63, 2019, doi: 10.1049/htl.2018.5046.

[2] K. Hameed, I. S. Bajwa, S. Ramzan, W. Anwar, and A. Khan, "An Intelligent IoT Based Healthcare System Using Fuzzy Neural Networks," Sci. Program., vol. 2020, 2020, doi:

10.1155/2020/8836927.

[3] N. Kaja, A. Shaout, and D. Ma, “An intelligent intrusion detection system,” Appl. Intell., vol. 49, no. 9, pp. 3235–3247, 2019, doi: 10.1007/s10489-019-01436-1.

[4] S. KishorWagh, V. K. Pachghare, and S. R. Kolhe, “Survey on Intrusion Detection System using Machine Learning Techniques,” Int. J. Comput. Appl., vol. 78, no. 16, pp. 30–37, 2013, doi: 10.5120/13608-1412.

[5] N. Farah, M. Avishek, F. Muhammad, A. Rahman, M. Rafni, and D. Md., “Application of Machine Learning Approaches in Intrusion Detection System: A Survey,” Int. J. Adv. Res. Artif. Intell., vol. 4, no. 3, pp. 9–18, 2015, doi: 10.14569/ijarai.2015.040302.

[6] W. Pedrycz, “Fuzzy neural networks and neurocomputations,” Fuzzy Sets Syst., vol. 56, no. 1, pp. 1–28, 1993, doi: 10.1016/0165-0114(93)90181-G.

[7] S. M. Bridges, R. B. Vaughn, and M. State, “Fuzzy Data Mining and Genetic Algorithms Applied To Intrusion,” Proc. 12th Annu. Can. Inf. Technol. Secur. Symp., pp. 109–122, 2000.

[8] H. H. Homer, “Applying the Fw Logic Paradigm to the Multipolicy Paradigm,” Security, no. October, 1991.

[9] J. E. Dickerson and J. A. Dickerson, “Fuzzy network profiling for intrusion detection,” Annu. Conf. North Am. Fuzzy Inf. Process. Soc. - NAFIPS, no. FEBRUARY 2000, pp. 301–306, 2000, doi: 10.1109/nafips.2000.877441.

[10] T. Bari, “Environments : A Research Review,” pp. 2363–2369, 2021.

[11] H. T. Elshoush and I. M. Osman, “Reducing false positives through fuzzy alert correlation in collaborative intelligent intrusion detection systems - A review,” 2010 IEEE World Congr. Comput. Intell. WCCI 2010, 2010, doi: 10.1109/FUZZY.2010.5584418.

[12] I. Graetz, M. Reed, S. M. Shortell, T. G. Rundall, J. Bellows, and J. Hsu, “The Next Step Towards Making Use Meaningful,” Med. Care, vol. 52, no. 12, pp. 1037–1041, 2014, doi: 10.1097/mlr.0000000000000245.

[13] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, “Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study,” IEEE Access, vol. 8, pp. 106576–106584, 2020,doi: 10.1109/ACCESS.2020.3000421.