International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.065

Neural Network-Based Intrusion Detection System in Hospital Management Systems

Pawankumar Sharma,
Sr. Product Manager, Walmart,
University of the Cumberlands, PhD
Candidate, Department of IT,
Williamsburg, KY 40769, United States,
psharma8877@ucumberlands.edu

Shaik Salma Begum
Assistant Professor, school of computing
Mohan Babu University ,
Tirupati, Andhra Pradesh, India,
salmabegum.s@mbu.asia

Deepthi B
Assistant Professor,
Department of Computer Science and
Engineering, ChaitanyaBharathi
Institute of Technology,
Gandipet, Hyderabad, India,
deepthiraya@gmail.com

N.Pandeeswari,
Associate Professor,
Department of IT, PSNA College of
Engineering and Technology,
Dindigul, Tamilnadu, India,
pandeeswari@psnacet.edu.in

N.Krishnamurthy,
Department of Mathematics,
Vel Tech MultitechDr RR and
Dr SR Engineering college,
Avadi-veltech Road, Avadi, Chennai-600062,Tamilnadu
krishnamurthy@veltechmultitech.org

R.Vinay Raj
Faculty, B.Goidhoo,
Ministry of Maldives, 06080.
vinsrvin@gmail.com

***Abstract*—The technological transformation has helped to simplify formerly time-consuming tasks. In this study, we will look at neural network-based intrusion detection systems in hospital management systems. This paper presents an intrusion-identifying system based on NN modeling. A hospital managing system (HMS) is a computer-based system that assists in controlling the healthcare data in the way of the effective ending of healthcare providers' jobs. An intrusion detection system (IDS) is software that identifies malicious activity on a network. A neural network (NN) is a set of algorithms that aims to determine interactions in a data set using a process that resembles how the human brain works, and the HMS is functioned in this proposed system using these NNs. In this research, K-Means algorithm is implemented to identify the intrusion in the hospital management System.**

Keywords—***Hospital Management System (HMS), Intrusion Detection System (IDS), Neural Network (NN), K-Means Algorithm***

I. Introduction

A neural network (NN) is a type of algorithmic learning system that employs a network of functions to comprehend and translate a data input in one form into an expected outcome, typically in another form. The neural network concept was inspired by human neuroscience and the way neurons in the human brain work with each other to understand input from human senses. In ML algorithms, NNs are one of many techniques and methodologies. The NN can be used as a component in a variety of machine learning algorithms to convert complex information inputs into a space that the computer understands. An intrusion detection system (IDS) is software that detects malicious network activity [1-2].An HMS is a computerized model which assists in the managing of healthcare data and effective ending of healthcare providers' jobs. They manage data for all departments of healthcare, including clinical, finance, research lab, outpatient care, primary care, operating room, equipment, nursing, pharmacy, radiation oncology, pathology, and so on. HMS entered the hospital management scene in the 60s and has since evolved and synchronized with technology while modernizing healthcare facilities [3]. In today's world, healthcare management begins in the hands of patients via their cell devices and facilitates the patient's needs.

The incorporation of IoT systems into healthcare applications has made it feasible to remotely monitor the information pertaining to patients and to deliver appropriate diagnoses whenever it is required. The provision of high-security features that can ensure the accuracy and confidentiality of patients' data, on the other hand, is a considerable difficulty. Any change to the data might have an effect on the care that the patients get, which could result in human fatalities in an emergency situation [4-5]. When it comes to providing an efficient solution for intrusion detection, machine learning has the potential to live up to its potential as a viable option due to the high dimensionality and conspicuous dynamicity of the data involved in such systems. On the other hand, the majority of the currently available healthcare intrusion detection systems construct their datasets by using either network flow measurements or the biometric data of patients [6-7]. The purpose of this research is to demonstrate that using a combination of network metrics and biometric measurements as features yields superior results than use either one of the two kinds of features alone [8]. A real-time Enhanced Healthcare Monitoring System (EHMS) testbed has been developed by our team. This testbed monitors the biometrics of patients and gathers network traffic measurements. The data that is being watched is then transferred to a remote server so that further diagnostic and treatment choices may be made [9-10].

II. Literature Review

Ashraf, Eman, et al. (2022) and Sivakumar P (2015) proposed FIDChain IDS using lightweight Artificial Neural Network in learning means to guarantee to care of health information secured in managing preservation with the advancements of blockchain platform that enable the ledge that is shared for gathering the weights in local and transmitting the developed weights in global after taking an average, that restricts poisoning attacks and delivers complete transparency at the same time immutability in a distributed system according to the negligibility.Laxminarayana, Nikhil, et al. (2022), Karnan B et al (2022), and Latchoumi TP et al (2022) investigated the IDS is trained using NNs and the concepts of quantum physics. It is suggested to use a hybrid classical-quantum neural architecture with a quantum-aided activation function, It uses less architectural memory than traditional systems while yet successfully capturing patterns in the dataset [11]. On the well-known KDD99 dataset, the experimental results are shown, and our approach is contrasted with various traditional models. Begli et al. (2022) and Monica.M et. al. (2022) proposed a secure remote medical system architecture. We aim to provide a secure framework for remote healthcare systems that keeps the system's data as safe as possible from common network affection such as the Denial of supplying and User Root attacks [12]. To accomplish this, they have created an IDS based on the ML algorithms, SVM. Following the implementation of the proposed method, the evaluation parameters of IDS' layered architecture demonstrate the efficacy of our proposed framework.Awotunde, et al. (2021), Vemuri et al (2021), and Buvana M et al (2021) presented a study that offers a Deep Learning based detection of intrusion in the form of a framework for the Internet of Things with hybrid regulations based on the feature selection to prepare and analyze the data captured from TCP data packets [13]. The training procedure has been carried out using a deep feedforward NN model and a hybrid rule-based feature selection approach. Two network datasets, NSL-KDD and UNSW-NB15, were used to test the proposed scheme. He, Daojing, et al. (2019) and Sridaran K et. al. (2018) investigated system security flaws and introduced a new intrusion detection system based on a piled autoencoder. They performed the results, and the status demonstrates that the model and its method are effective [14].

He, Daojing, et al. (2019) proposed a stacked autoencoder and a DNN-based intrusion detection system. To reduce feature width, the layered AE learns the features from the input network record unsupervised. The DNN is then trained and supervised to extract DL features according to the classifier [15]. The proposed system has two latent layers in the stacked AE and two or three layers in the DNN, with every layer having an entirely in-touch layer, a batch with normalization, and dropout. Biswas et al. (2019) proposed a cloud service delivery model based on a single window, whereby a smart card acts as a single entry point to several electronic services, including banking, healthcare, employment, and so on.The authors of this paper focused on the IDS of the cloud service model throughout cloud banking transactions to identify and mitigate unauthorized access [16]. Alzahrani et al. (2021) performed research that illustrates the deployment of ML models for traffic analysis to identify the malicious protocol behavior as part of the Software Defined Network controller's NIDS. To demonstrate attack detection, three classical tools that are ML-based tree techniques like Decision Tree classifier, Random Forest Classifier, and Boosting algorithm, are used. The NSL-KDD data info is being used for both the analysis of the dataset; it is a dataset for several options that are laid in the cutting-edge NIDS approaches. Various advanced techniques that are used for preprocessing are applied to the data for obtaining a stable form of data, yielding exceptional results when compared to pre-defined systems. Nandy, Sudarshan, et al. (2021) suggested an Empirical Intelligent Agent based on a cutting-edge Swarm-Neural Network (Swarm-NN) technique to detect attackers in the edge-centric IoMT framework. The major objectives of the suggested technique are to identify assaults during data transmission across a network and to perform a more accurate and efficient analysis of health data at the network edge [17-18].

III. PROPOSED WORK

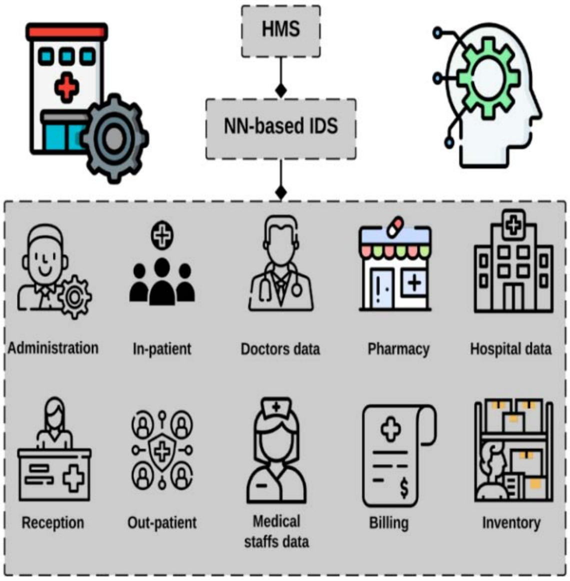

Fig.1. Illustration of NN-based IDS in HMS

Fig.1 Illustrates the Neural Network-based Intrusion Detection System in Hospital Management System. Malicious activity includes the distribution of viruses and other operations that disrupt the ability of others to effectively use networks, systems, services, software, or equipment [19]. A software intrusion detection system (IDS) detects malicious network activity. Because of the services it provides, an IPS is also known as an intrusion detection and prevention system. An IDS monitors network traffic. It works by detecting malicious network activity by analyzing intrusion signatures, generic behavior, and heuristic methods, and then drops the packet and blocks the specific traffic [20]. When such an event happens, the administrator is also notified. The proposed intrusion detection system, which is based on a neural network model, manages healthcare information and ensures that healthcare providers' jobs are completed effectively. The proposed system effectively manages data for all clinical, financial, research lab, outpatient care, primary care, operating room, equipment, nursing, pharmacy, radiation oncology, pathology, and other departments of healthcare [21].

Let ρ_j signify the required to charge up the required stations and can charge those pre-fixed equipment utilization ratio $\rho_j = (\lambda_j / y_j \mu_j)$ According to the conventional slight Equation the waiting period for such $h^{th}\, TC$ and trying to charge point j is represented by Equation (1).

$$g_{ih}^{H} = \sum_{j=1}^{y} \frac{(x_j \rho_j)^{t_j} \rho_j}{\lambda_j y_j!\,(1-\rho_j)^2 \varphi_{E_j}} \left(\sum_{m=0}^{x_i - 1} \frac{(y_j \rho_j)^m}{m!} + \frac{(y_j \rho_j)^{y_j}}{t_j!\,(1-\rho_j)} \right)^{-1} H_{jh} \times h^{th} TC \tag{1}$$

The charging k-means method which is always used to detect the intrusion for the h^{th} TC at endpoint j is as shown in Equation (2).

$$g_{jh}^{H} = \sum_{j=1}^{h} \frac{T_{min} - T_{jh}^{h}}{m_g} \tag{2}$$

K-Means Algorithms to enhance **e**nergy consumption is influenced not just by the maintenance of hospitality and various standard servers. Whenever a TC with a charge travels at B_C transportation distance ŋkm/gc on a flat, the ability to run power $E(B_c, c)$ is represented by Equation (3).

$$E(B_c, c) = \frac{\left((x+B_c).h.\int c + \left(S_m .Z_j .c^3/22.56\right)\right)}{3700\,\text{ŋkm}/gc} \tag{3}$$

The *K-Means Algorithms assess and detection of diabetes in healthcare* and h_{ij} the receiver needs to be one of a kind from the alternative whereas at the same time the operator can certainly be connected in the form of neural networks and to the desired tool without dispute. Transition pace is $m_j - \overline{m}$is classed into-the-spot transition and time change. Space-time transformation, inclusive of the preceding NG, takes a while to comply with the series represented within Equation (4).

$$NG = c_{ij}(s) \sum_{i=1}^{y} \frac{y \sum_{i=1}^{y} \sum_{j=1}^{y} + \sum h_{ij} (m_i - \overline{m})(m_j - \overline{m})}{\sum_{i=1}^{y} \sum_{j=1}^{y} + h_{ij} (m - \overline{m})^2} \tag{4}$$

The following Equation (5) represents the detections of intrusion based extrude within the transition time.

$$NG = c_{ij}(s) \sum \frac{y \sum_{i=1}^{y} \sum_{j\neq1}^{y} + h_{ij} (m_i - \overline{m})(m_j - \overline{m})}{C^2 \sum_{i=1}^{y} \times \sum_{j=1}^{y} h_{ij}} \tag{5}$$

IV. Experimental Results

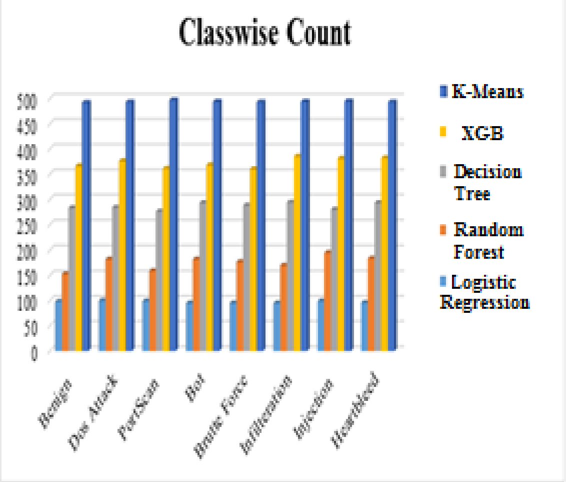

Fig.2. Performance AnalysisK-Means Algorithms to enhance the performance under the Neural Network for Intrusion Detection

The model Swarm-Neural Network strategy is tested using a real-time privacy dataset, the ToN-IoT information, which collects OS, and Telemetry for Internet of Things applications and analyses the performance of normal models that are deployed in classification rule using various parameters. The results show that the model Swarm-Neural Network strategy outperforms the ToN-IoT dataset in terms of accuracy. SGM is a novel class imbalance of technology managing for high-scale datasets proposed by Zhang, Hongpo, et al. (2020), which integrates Based on the Gaussian Mixture Model, the Synthetic Minority Over-Sampling Technique with under is used for clustering. They concluded that SGM-CNN outperforms intrusion detection methods and is a good option for unbalanced intrusion detection. The numerical results are presented in Table 1 as below.

TABLE 1.COMPARISON RESULT ANALYSIS FOR THE EXISTING SYSTEM

Algorithm	Detection of intrusion in healthcare Training (%)	Detection of intrusion in healthcare Testing (%)	Overall Accuracy (%)
K-means Algorithm	95.63	91.78	97.67
Existing Method: Optimization Algorithm	90.98	89.87	92.98

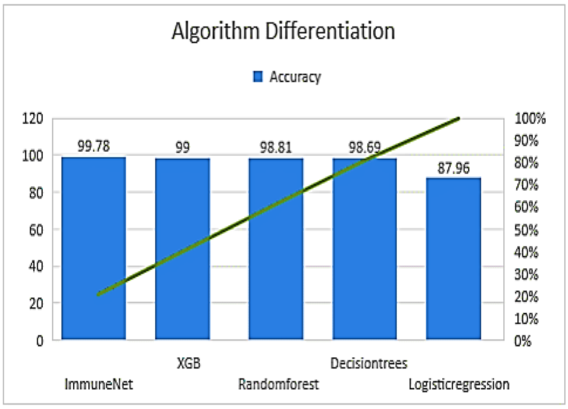

Fig.3. Accuracy Analysis based on different algorithms

Fig.3 represents the accuracy evaluation in detecting the intrusion in hospital environment and the results show that the proposed K-Means algorithm has obtained the highest accuracy in intrusion detection in the hospital data management system.

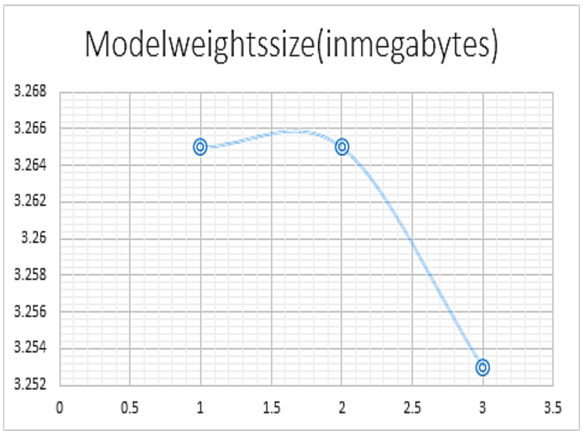

Fig.4. Analysis based on Model Weight

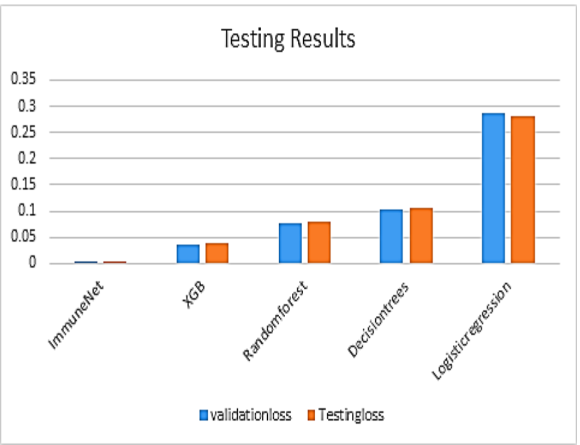

Fig.5. Analysis based on the Testing Results of the model

Fig.4 and Fig. 5 indicates the analysis of the proposed system based on the model weight and testing results evaluation with the existing system respectively. In the research, the existing system considered for analysis are XGB, Random Forest, Decision Tree, and Logistic Regression respectively. In the considered parameters for evaluation, the proposed K-Means have achieved highest performance than the existing models.

V. Conclusion

HMS was developed to address the difficulties associated with managing all of the paperwork associated with each patient associated with various departments of hospitalization while maintaining confidentiality. HMS allows you to manage all of your paperwork in one place, which saves you time organizing and analyzing the patient framework. Hospital Management System performs a differential tasks, which include maintaining patient's medical records, collecting contact info, managing appointment details, tracking bill payments, details of insurance, and so on.

References

[1] Ashraf, Eman, et al., "FIDChain: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications," Healthcare. vol. 10. no. 6. Multidisciplinary Digital Publishing Institute, 2022.

[2] Laxminarayana, Nikhil, et al., "Quantum-Assisted Activation for Supervised Learning in Healthcare-based Intrusion Detection Systems," IEEE Transactions on Artificial Intelligence, 2022.

[3] Begli, MohammadReza, FarnazDerakhshan, and HadisKarimipour, "A layered intrusion detection system for critical infrastructure using machine learning," IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), IEEE, 2019.

[4] Awotunde, Joseph Bamidele, ChinmayChakraborty, and Abidemi Emmanuel Adeniyi, "Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection," Wireless communications and mobile computing, 2021.

[5] He, Daojing, et al., "Intrusion detection based on stacked autoencoder for connected healthcare systems," IEEE Network, vol. 33.6, pp. 64-69, 2019.

[6] Muhammad, Ghulam, M.ShamimHossain, and SahilGarg, "Stacked autoencoder-based intrusion detection system to combat financial fraudulent," IEEE Internet of Things Journal, 2020.

[7] Biswas, Sonam, and Abhishek Roy, "An intrusion detection system based secured electronic service delivery model," 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2019.

[8] Alzahrani, O. Abdulsalam, and J.F. Mohammed Alenazi, "Designing a network intrusion detection system based on machine learning for software-defined networks,"Future Internet, vol. 13.5,p. 111, 2021.

[9] Nandy, Sudarshan, et al., "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," IEEE Journal of Biomedical and Health Informatics, vol. 26.5, pp. 1969-1976, 2021.

[10] Zhang, Hongpo, et al., "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," Computer Networks, vol. 177, p. 107315, 2020.

[11] T. P. Latchoumi, K. Raja, Y.Jyothi, K.Balamurugan, andR. Arul, "Mine safety and risk prediction mechanism through nanocomposite and heuristic optimization algorithm," Measurement: Sensors, p. 100390, 2022.

[12] Pazhani. A, A. J., Gunasekaran, P., Shanmuganathan, V., Lim, S., Madasamy, K., Manoharan, R., &Verma, A. (2022). Peer–Peer Communication Using Novel Slice Handover Algorithm for 5G Wireless Networks. Journal of Sensor and Actuator Networks, 11(4), 82.

[13] M. Monica, P.Sivakumar, S. J.Isac, andK. Ranjitha, "PMSG based WECS: Control techniques, MPPT methods and control strategies for standalone battery integrated system,"In AIP Conference Proceedings, AIP Publishing LLC, vol. 2405, no. 1, p. 040013, April, 202,.

[14] P. Sivakumar, "Effectual web content mining using noise removal from web pages," Wireless Personal Communications, vol. 84, no. 1, pp. 99-121, 2015.

[15] Vemuri, RatnaKumari, Pundru Chandra Shaker Reddy, Puneeth Kumar, Jayavadivel Ravi, Sudhir Sharma, and SivakumarPonnusamy, "Deep learning based remote sensing technique for environmental parameter retrieval and data fusion from physical models," Arabian Journal of Geosciences vol. 14, no. 13, pp.1-10, 2021.

[16] Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaninathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications. Computers and Electrical Engineering, 102, 108130.

[17] M. Buvana, K. Loheswaran, K. Madhavi, S. Ponnusamy, , A. Behura, andR. Jayavadivel, "Improved resource management and utilization based on a fog-cloud computing system with IOT incorporated with classifier systems," Microprocessors and Microsystems, p. 103815, 2021.

[18] C.Bhuvaneshwari, and A.Manjunathan, "Reimbursement of sensor nodes and path optimization", Materials Today: Proceedings, vol. 45, pp.1547-1551, 2021.

[19] A.Manjunathan, E.D.Kanmani Ruby, W. Edwin Santhkumar, A.Vanathi, P.Jenopaul, and S.Kannadhasan, "Wireless HART stack using multiprocessor technique with laxity algorithm", Bulletin of Electrical Engineering and Informatics, vol. 10, no. 6, pp. 3297-3302, 2021.

[20] C.Jeyalakshmi, A.Manjunathan, A.Karthikram, T.Dineshkumar, W. Edwin Santhkumar, and S.Kannadhasan, "Automatic Wireless Health Instructor for Schools and Colleges", Bulletin of Electrical Engineering and Informatics, vol. 11, no. 1, 2022.

[21] ManjunathanAlagarsamy, KarthikramAnbalagan, YuvarajaThangavel, JeevithaSakkarai, JenopaulPauliah, and KannadhasanSuriyan,"Classification of covid patient image dataset using modified deep convolutional neural network system", Bulletin of Electrical Engineering and Informatics, vol. 11, no. 4, pp. 2273-2279, August 2022.