SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I7P122

Volume 11 Issue 7, 220-227, July 2024
© 2024 Seventh Sense Research Group®

Original Article

Automated Detection of Cyber security Intrusions in Healthcare Systems Using Several Approaches

Shamija Sherryl. R. M. R[1], Sudhan. M. B[2], Deeptha. R[3], Karpagam. T[4]

[1]*Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamilnadu, India.*
[2]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamilnadu, India.*
[3]*Department of Information Technology, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamilnadu, India.*
[4]*Assistant professor, R.M.K. College of Engineering and Technology, RSM Nagar, Thiruvallur, Tamil Nadu, India.*

[1]*Corresponding Author : rmrshamija@outlook.com*

Received: 14 May 2024 Revised: 12 June 2024 Accepted: 12 July 2024 Published: 27 July 2024

Abstract *- To ensure that patients are receiving the proper care, the healthcare data must be improved, real-time monitored, and accurate in illness detection. Thus, machine learning techniques are widely employed in Smart Healthcare Systems (SHS) to extract valuable features for tracking patient behaviors and forecasting various diseases from diverse and high-dimensional healthcare data. The kidneys gradually lose their functionality as a result of Chronic Kidney Disease (CKD). It talks about a medical condition that damages the kidneys and has an impact on a person's overall health. In this study, Recursive Feature Elimination (RFE) and multilayer perceptrons are used to develop a model for identifying anomalies and cyber-attacks (MLP). Experimental data are used to evaluate the suggested MLP model's performance. Recall, precision, accuracy, and F1-score are only a few of the performance metrics used to forecast patient activities. When compared to the RFE technique, the recommended strategy provides the highest levels of accuracy, precision, recall, and F1 score. Specifically, 98.56% recall, 98.13% F1-score, 98.76 accuracy, and 98.93% precision are obtained using the proposed MLP technique. When the outcomes were compared to recent state-of-the-art and machine learning algorithms from recent times, they performed better.*

Keywords *- Internet of things, Cyber security intrusions, Smart healthcare systems, Intrusion detection, Machine learning.*

1. Introduction

Among others numerous medical care associations utilize Electronic Health Record (EHR) frameworks, e-prescribing frameworks, practice the board emotionally supportive networks, clinical choice emotionally supportive networks and other specialised hospital information systems. Radiology information frameworks and mechanized physician request passage frameworks. The Internet of Things, which is comprised of endless special gadgets, should likewise be secured. They include items like infusion pumps, HVAC (heating, ventilation and air conditioning) systems that are intelligent, smart lifts, among others. [1]

Healthcare cyber security must be a top priority for all medically related organizations, comprising healthcare suppliers, insurers, pharmaceutical firms, biotechnology firms, and producers of medical equipment. In addition to ensuring the It involves taking a range of actions to safeguard organisations against both inner and outer cyberattacks. These incorporate keeping up with the accessibility of clinical benefits, the proper working of clinical frameworks and hardware, safeguarding the privacy and respectability of patient information, and complying with industry rules.

Healthcare cyber security includes safeguarding electronic data. All medical industry businesses, including those in biotechnology, insurance, healthcare, pharmaceutical, and medical device manufacturing, view healthcare cyber security as a strategic concern. In order to safeguard companies from both internal and external cyber-attacks, guarantee patient privacy, maintain the availability of medical services, guarantee the reliability of medical technology and systems, guarantee the integrity of patient data, and adhere to industry regulations, a number of steps must be taken.

All medical industry businesses, including those in biotechnology, insurance, healthcare, pharmaceuticals, and medical device manufacturing, view healthcare cyber security as a strategic concern. Several actions are expected to safeguard associations from internal and external digital assaults, ensure the openness of clinical benefits, protect patient privacy, guarantee the dependability of medical devices and systems, ensure patient data integrity, and abide by industry rules.

This part examines the theoretical underpinnings of the learning algorithm and the neural network architecture that are relevant to this study. [2] The Multilayer Perceptron (MLP), with its straightforward algorithm and transparent construction, is among the most often used neural network models. The utilisation of input, hidden, and output layers may enable the diagnosis of heart disease up the three layers of a multilayer perceptron network. —that is a system this complex. 40 variables that were obtained from an experimental study on numerous patient instances are sent to the system's input layer. Using a cascade learning technique, the buried layer's node count is determined. The output layer's five nodes correspond to the five relevant cardiac scenarios.

Recursive Feature Elimination (RFE), a feature selection strategy, seeks to find the optimal feature subset in accordance with the learning model and characterization accuracy. Subsequent to the classification of an order model, traditional RFE efficiently disposes of the most exceedingly terrible component that adds to a reduction in classification accuracy. As of late, a clever RFE technique that utilizes a help vector machine (SVM) model to assess "highlights (variable) pertinence" instead of characterization exactness" and chooses the most un-critical elements for erasure was proposed. [3] Recursive Feature Elimination (RFE), a feature selection strategy, removes the model's weakest feature (or features) up until the point at which the required number of features is met. One popular technique for highlight choice is called recursive feature end, or RFE. Since RFE is easy to apply and proficient at distinguishing the highlights (sections) in a preparation dataset that are pretty much valuable for foreseeing the objective variable, it is widely used.

2. Literature Review

Naraei et al. (2016) have explained the research, which compares Using a dataset of cardiac diseases, support vector machines and multilayer perceptron neural networks built. Using a dataset of 303 patients, this analysis examined the support vector machine's classification efficacy. Alharam et al. (2017) have examined several security vulnerabilities in the healthcare sector. The study will focus on how cyber security is used in the healthcare sector and the various measures taken to protect the IoT-based healthcare sector. The primary subject of this presentation (EHR) will be the use of AES (Advanced Encryption Standard) to safeguard the healthcare industry from cyber-attacks and their use in electronic health records. Strielkina et al. (2018) have explained that for the purpose of evaluating cyber security, Considering these systems, a case-based methodology comprising an Advanced Security Assurance Case (ASAC) and an illustration of its application to a wireless insulin pump is offered.

Alromaihi et al. (2018) have examined the creation of defenses against cyberattacks on Internet of Things (IoT) devices in smart cities for use in healthcare applications by taking into account the different kinds of assaults, and the security needs that go along with them. To tackle these problems and ensure a seamless deployment, government authorities and healthcare organizations must work in harmony. Chacko et al. (2018) have investigated the importance of IoT in healthcare, as well as security problems and solutions. The FDA was constrained to give official proposals on how clinical gadget producers ought to answer claims in regard to digital weaknesses because of the development in hack capable clinical devices. This empowers early helpful activity by permitting clinical experts to gather information and utilize choice help models consequently.

Al-Muhtadi et al. (2019) have explained that this study compares the intricacy of cyber security architecture and how it applies to the Internet of Clinical Things. The motivation behind the review is to safeguard the medical services industry against online assaults that target IoT-based clinical hardware. The study looks at the resources utilized for different architectures to handle the complexity issue of IoT-based healthcare systems' cyber security architecture. McFarland et al. (2019) have examined the weaknesses, dangers, and hazards associated with the usage of Medical Technology based on the Internet. (IoMT). This work not only identified the problems but also guided mitigation measures that might be applied to thwart emerging security risks. The continuous discussion about quiet protection security with network framework, verification, and appropriately designed end gadgets is achieved by IoT gadgets.

Sparrell et al. (2019) have proposed the two-step validation process utilized to assess and the revised GA algorithm produced satisfactory results; in the first stage, a traditional DFJSP was used to demonstrate the algorithm's efficacy, and in the second stage, the algorithm was applied to solve a real-world problem. The outcomes were encouraging and showed that the suggested improved GA algorithm could successfully resolve the conflicts brought on by GA encoding techniques. Albesher et al. (2019) have overviewed the various IoT applications in healthcare given in this article. It covers some of the most important IoT healthcare services and their advantages for society as a whole, including global projects. Along with several cutting-edge IoT enabled health applications, also covered are current and cutting-edge wearable health technology. It is complemented with a thorough analysis of the challenges and security requirements for IoT in healthcare. The research methodology has been proposed by Agrawal et al (2020) and is tested using 10 distinct data sets related to medicine from the UCI AI assortment. The presentation of the proposed technique is assessed against four newly developed algorithms that draw inspiration from nature: The Grey Wolf Optimization algorithm, Notable in the literature are the Cuckoo Search, Bat, and Whale Optimization Algorithms, in addition to the traditional Back-propagation training method. The results show that the suggested method surpasses the already employed algorithms that are bioinspired in terms of accuracy and speed of convergence.

Tanwar et al. (2020) have suggested that a chain code-based Hyper Ledger-based Access Control Policy Algorithm is used by an Electronic Health Record (EHR) Sharing System to enhance data accessibility between healthcare providers and simulation settings. Trip duration (RTT), throughput, and other execution measurements in blockchain networks have likewise been adapted to improve results. The proposed framework utilizes block chain instead of the client-server design utilized by customary EHR frameworks to build effectiveness and security. Djenna (2020) have explained the unique method for detecting and mitigating DDoS cyberattacks that aim at Internet of Things infrastructure. Identifying the essential components most likely to serve as the cyberattacks DDoS reactor to be more accurate. In the future work, plan to expand the suggested work and test it in real environments, on the one hand, and concentrate on forensic security investigation with a view to authorship attribution.

Echeverría et al. (2021) have suggested modelling a sequence of seven steps that would be utilized to carry out hardening procedures and reduce the attack surface. By using a checklist that takes into account were able to develop a suggested method for assessing the degree of security of an Internet of Things solution by considering the security elements in each of the three IoT architecture layers. The dangers to privacy and security associated with IdM systems based on HIoT BC have been suggested by Thomasian et al. (2021), who have also provided a security taxonomy, security framework, and framework for controlling cyber security risk. This created a research methodology with four primary steps in order to address the three research topics. SLR demonstrated that the suggested HIoT BC-IdM systems do not adhere to a strict and organized architecture for risk and security management.

3. Proposed Methodology

IoT cyber security is a field of technology devoted to safeguarding networks and connected devices. Encompasses tying mechanical and digital devices, items, living things, and/or people to the Internet. Chronic kidney Disease (CKD) has a fatal and rapidly expanding impact on society. The main forms of treatment are: You may maintain the best possible health by modifying your way of living. Medicine: utilized to treat associated conditions like high blood pressure and cholesterol. In advanced (stage 5) CKD, dialysis, a form of treatment, may be necessary to mimic some kidney functions. Adults with Chronic Kidney Disease (CKD) most commonly have diabetes and hypertension. A family background of persistent Kidney Disease (CKD), obesity, heart disease, old age, and other risk factors, genetic renal issues, and prior kidney damage. Maintaining good blood pressure and sugar levels can support kidney health.

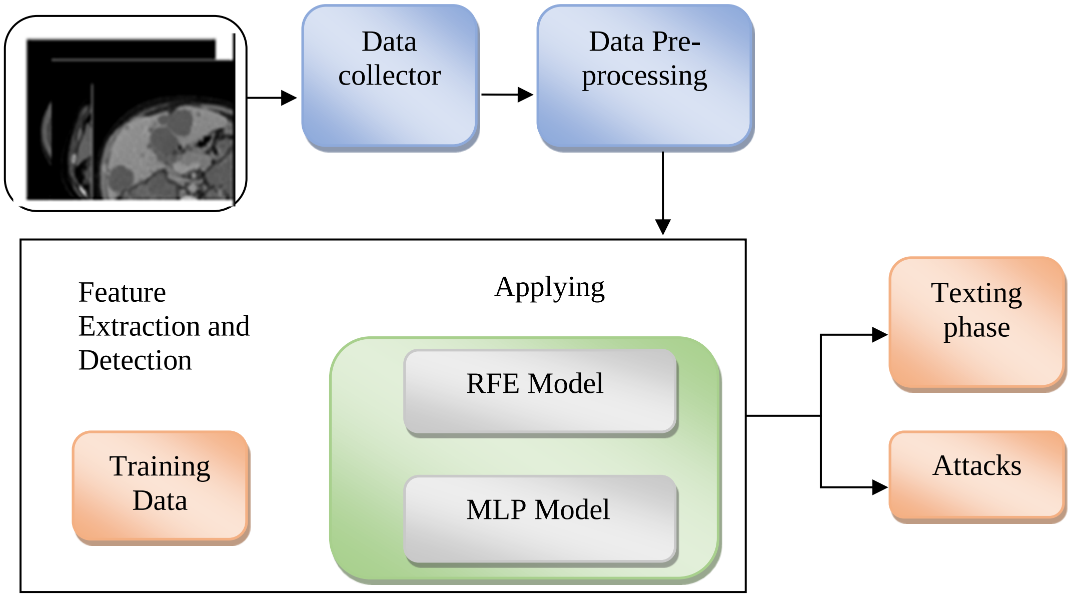

Fig. 1 Block diagram of the proposed framework

The proposed approach and the framework are shown in Figure 1, referred to as the multilayer perceptron optimisation and recursive feature elimination takes input data, processes it, and then produces a subset of ideal features that enable better categorization. The standard classifiers are then executed on the selected features in order to gauge performance. Many tests are run to evaluate the healthcare performance. The techniques used to assess data and feed it to the model are one factor that affects the performance of the models. As a result, converting data into categorical variables that RF models can understand is a crucial step in the encoding process. This part will be focused on class balancing and determining the relevance of features in balanced data. Data preparation must come first for every learning system. Every incoming data is tracked by the recommended system, which then stores it in its data storage. The data must be cleaned of noise and anomalies during the data pre-processing stage before being submitted to the learning module.

3.1. Data Preparation

The dataset was submitted to a variety of feature selection and sampling procedures, as mentioned in the sections above, in order to emphasize the key characteristics for classification and improve accuracy. The attack columns were combined into three feature columns: target, which served as the attack labels, which served as the attack's name, and binary targets, which revealed if the packet was malicious or not. The phases in CKD are shown below in Table 1.

$$y = \frac{(x-\overline{x})}{\alpha} \tag{1}$$

The dataset must be altered and cleaned up before the model can be applied to it; this is referred to as pre-processing the data. The performance and accuracy of the prediction model are impacted by the quality of the dataset and pre-processing, in addition to the techniques used. In this investigation, the pre-processing stages listed below were used:

Table 1. The phases in which CKD develops

Stage	Description	The rate of globular filtration (GFR)	Treatment stage
1	Normal kidney function	≥ 90	monitoring and blood pressure management
2	Mild kidney damage	60-87	Risk factors, blood pressure management, and observation
3	Moderate Kidney damage	30-59	Risk factors, blood pressure management, and observation
4	Severe Kidney damage	15-28	Making plans for acute kidney failure
5	kidney failure that is established	< 16	Options for treatment

3.2. Pre-processing

The pre-processing of the data includes scaling, normalization, and input-output coding. In actuality, certain data could not be in a format that the learning module can use because the current solution only takes numerical input and can only provide results within a range determined by the fitness function can work with. Different data points' input values may not all have the same scale. Pre-processing is a crucial step in the dataset's refinement. The redundant features and missing values reduce the method's accuracy. Hence, first, search the dataset for repetitive features and missing values. At first deal with missing values in a variety of ways, such as by ignoring all values, substituting specific numeric type values, often occurring values for that feature, mean values, etc. The two stages that make up the pre-processing stage are substituting the missing data and deleting the unnecessary features. Here, the mean value of the column was computed to fill in the missing values for three observed variables, including the patient's blood pressure, cholesterol, and age group.

$$x'_i = \frac{(x_i - X_{min})}{(X_{max} - X_{min})} \tag{2}$$

Where x_i, X_min and X_max stand for the original values, scaled values, and maximum and minimum values.

Normalization is carried out to maintain all of the input values within a range that the learning module can process. The normalizing formula is presented in

$$x'_i = X_{max} - X_{min} * \left\lceil \frac{(x_i - X_{min})}{(X_{max} - X_{min}} \right\rceil + X_{min} \tag{3}$$

Raising the values of the achieved accuracy and average correlation throughout the process is crucial after determining the average correlation's resultant value and repeated perception in order to optimize those values. The features must be different and little correlated in order to discover a solution. Average correlation must be altered to average non-correlation in order to do this. Subtract the average correlation value for each generation from 1 to arrive at this result (the best possible value). As a result, both ascending and descending order can be used to display the average correlation values and accuracy. The converted fitness values can then be determined using the chromosome's accuracy and average correlation value.

$$corr_{avg} = \frac{sumsofvaluesabovethediagonal}{Numberofvalues} \quad (4)$$

$$corr^{t}{}_{avg} = (1 - corr_{avg}) \quad (5)$$

$$F_i = \frac{(A_i + (1 - M_i))}{2} \quad (6)$$

4. Results and Discussion

Table 2. Statistical analysis of the dataset of numerical features

Features	Mean	Standard deviation	Max	Min
Age	51.87	17.65	85	2
blood glucose arbitrary	148.908	74.566	476	23
Blood pressure	75.56	13.89	140	50
Blood urea	57.98	49.89	378	1.5
Potassium	4.98	2.89	47	3.5
Volume of packed cells	38.78	8.78	65	9
Sodium	135.67	9.87	163	4.7
Hemoglobin	12.65	2.876	17.8	3.1
White blood cell count	8406.67	2835.78	26400	2100
Red blood cell mass	4.707	0.89	8	2.1

The importance of technology in the healthcare industry has grown as a result of the development of e-Health and m-Health. There are millions of sensors connected to the patients, and a multitude of physiological, environmental, and behavioral aspects constantly monitor the patient's health. For monitoring patients, Wireless Body Sensor Networks (WBSN), sometimes referred to as e-Health and m-Health, are a common IoT technology in the healthcare industry. All across the human body are sensors for the WBSN. The sensor layer, the levels of the WBSN's layered design are the processing, storage, mining, and learning layers, as well as the communication layer. For people with chronic kidney disease, these devices collect crucial data on blood glucose, pulse, breath rate, circulatory strain, internal heat level, and ECG shown in Table 2.

Table 3. Analysis of feature evaluation

Features	Mean	Evaluation
Age	51.87	0.763
Blood glucose random	148.908	0.79
Blood pressure	75.56	0.65
Blood urea	57.98	0.76
Potassium	4.98	0.54
Packed cell volume	38.78	0.87
Sodium	135.67	0.56
Hemoglobin	12.65	0.63
White blood cell count	8406.67	0.74
Red blood cell count	4.707	0.85

Blood Glucose, Hypertension, and Red Blood Cell Count are all noted to have moderate relationships with ranks 0.699, 0.645, and 0.621, respectively. Additionally, the remaining parameters, such as salt levels, white blood cell counts, and red blood cell counts, show a humble affiliation in Table 3. Lastly, the target class discovers no proof that 0.092 and potassium are related.

Random Forest also ranks the hemoglobin feature first, while Gain Ratio places this danger factor third. In addition, different approaches capture different aspects of relevance in different ways. All attributes will be used in the models' training and evaluation because they are crucial indicators for kidney surgery and, consequently, CKD management by doctors.

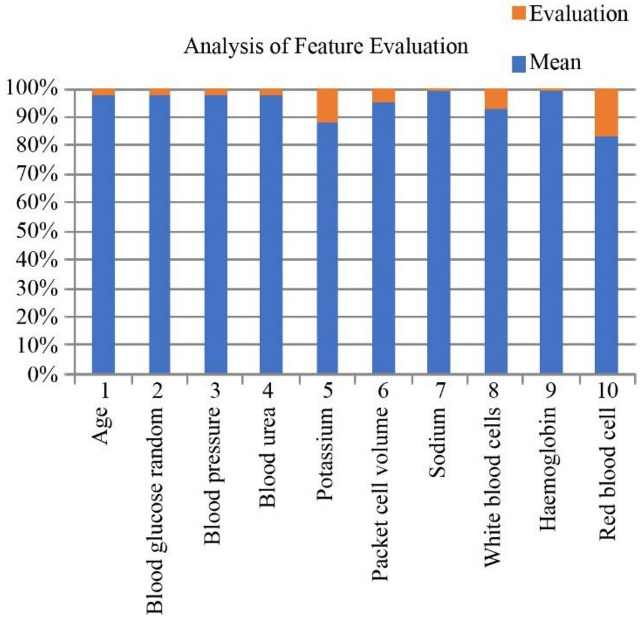

Fig. 2 Radiation pattern of single element micro strip patch antenna for X band

Accuracy and recall, two common evaluation criteria, are used to assess the outcomes. The feature evaluation is shown in Figure 2, and These elements are taken into consideration when evaluating the final categorization module. Accuracy: Accuracy serves as a performance indicator for classifiers. The outcomes are better the higher the precision.

The metrics mentioned above are used to assess the generated algorithm's performance. The impact of device reduction on the potency of untargeted attacks is illustrated in Figure 3; reducing the number of devices lowers the proposed attack's success rate. In comparison to the RFE approach, the proposed MLP achieves a higher success rate of 15.70% for the removal of 2 devices (blood oxygen and glucose) and 1 device.

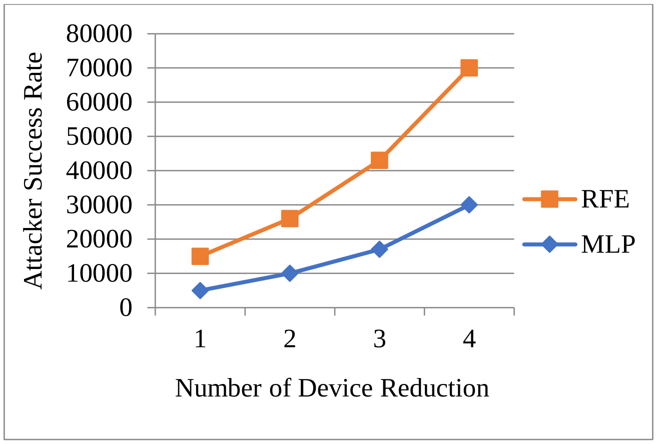

Fig. 3 Analysis based on the success rate of attackers

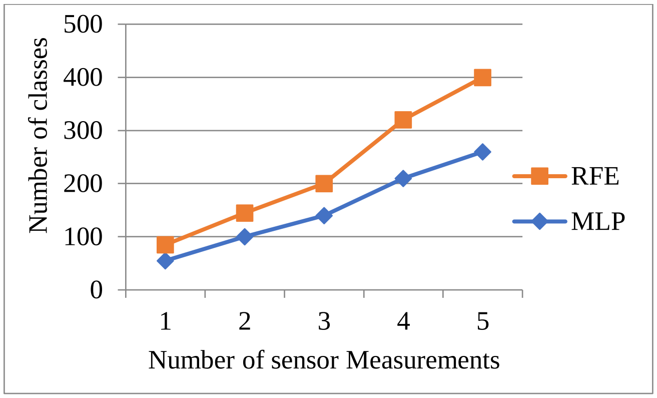

Fig. 4 Synthetic data complexity analysis

The suggested MLP approach and the RFE are compared in order to assess the performance. The accuracy analysis of the suggested strategy is displayed in Figure 4. There is a comparison between the detecting activities of the MLP and RFE. 98.7% accuracy is achieved by the suggested approach MLP, which is greater than the other methods.

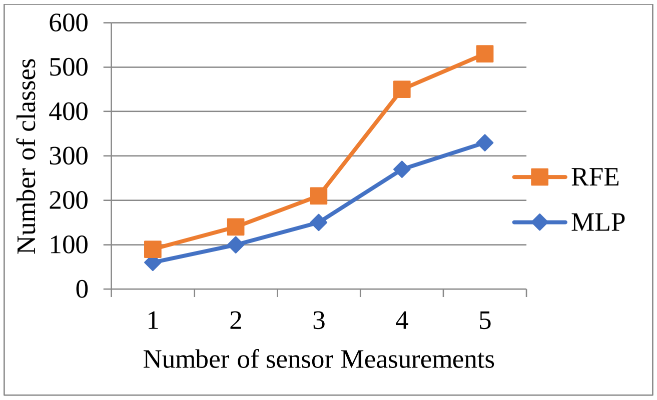

Fig. 5 Data complexity analysis

Figure 5 shows a graphical representation of the precision analysis. The suggested method achieves a precision that is 98% higher than the RFE methods, as can be seen in Figure 5.

4.1. Measures of Evaluation

Performance indicators were employed to assess the capabilities of each of the four classifiers. Performance testing of the proposed approach using the used intrusion detection dataset is shown in Table 4. One of these actions is the disarray grid, which is figured utilizing the conditions beneath to distinguish the examples that were erroneously arranged (FP and FN) and accurately recognized (TP and TN). Accuracy, precision, recall, and F1-score are then taken from this confusion matrix. The value varies between 0 (worst) and 1 (best). Equation illustrates the accuracy computation (7). False positives are addressed by the letters FP, false negatives by the letters FN, true negatives by the letters TN, and misleading up-sides by the letters FN. The expressions "false positives," "false negatives," and "true positives" (TP, FP, FN) are interchangeable and TN for "true negatives."

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \tag{7}$$

$$Sensitivity = \frac{TP}{TP+FN} \tag{8}$$

$$recall = \frac{TP}{TP+FN} \tag{9}$$

$$F_1 - score = 2 * \frac{sensitivity*recall}{sensitivity} \tag{10}$$

Table 4. Performance testing of the proposed approach using the used intrusion detection dataset.

Measures	Mean	Evaluation
Precision	98.94	98.93
Sensitivity	86.99	98.81
Accuracy	98.76	98.76
Recall	98.97	98.56
F_1-Score	97.62	98.13

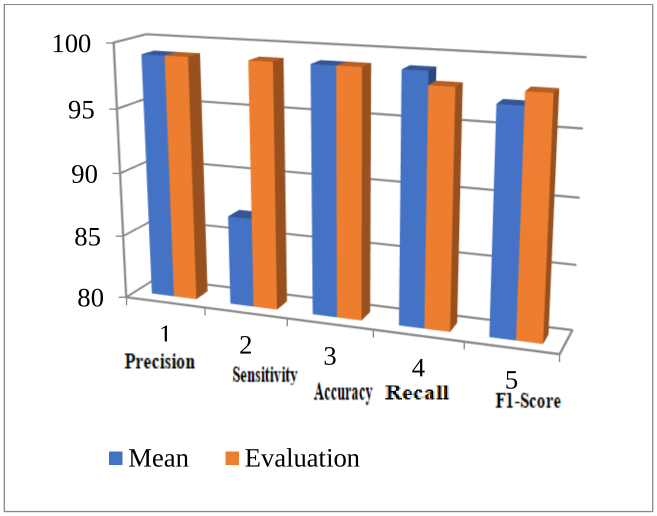

Fig. 6 Graphical diagram of intrusion detection dataset

The obtained recall, accuracy, precision, and F1-score have important applications in the fields of illness detection and healthcare data security. The Intrusion detection dataset is shown in Figure 6. A low pace is indicated by the great precision of false alarms, guaranteeing that medical personnel will not be deluged with false warnings and can act on model alerts with confidence. The model's capacity to efficiently identify possible problems and reduce the possibility of missing important events is indicated by the similarly high recall.

The astounding F1 score strikes a mix between recall and precision, highlighting the model's ability to retain accuracy while offering thorough coverage. By selectively combining features from several layers and giving priority to trustworthy data while attenuating adversarial or noisy signals, the MLP model counters adversarial attacks. It differs from previous methods in that it can adapt to a variety of healthcare data types and maintain robustness without compromising computing efficiency.

5. Conclusion

IoMT devices lack hardware and software security designs, making them vulnerable to a range of assaults. This paper investigates potential privacy and security concerns with the IoT that cyber security has enabled. The research mainly works on enhancing ML models to increase the accuracy of forecasting outcomes for chronic kidney disease. The findings indicate that methods for outlier detection and recursive feature elimination, in conjunction with different classifications, may offer helpful tools for inference in this field. In order for classification systems to be able to predict more variables, their effectiveness on various feature selection methodologies needs to be increased. The experiment's findings demonstrated that the suggested model is a reliable tool for healthcare industry cyber security.

Acknowledgments

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

References

[1] Sara Alromaihi, Wael Elmedany, and Chitra Balakrishna, "Cyber Security Challenges of Deploying IoT in Smart Cities for Healthcare Applications," *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, Barcelona, Spain, pp. 140-145, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Aysha K. Alharam, and Wael Elmedany, "The Effects of Cyber-Security on Healthcare Industry," *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, Manama, Bahrain, pp. 1-9, 2017.[CrossRef] [Google Scholar] [Publisher Link]

[3] Jalal Al-Muhtadi et al., "Cybersecurity and Privacy Issues for Socially Integrated Mobile Healthcare Applications Operating in a Multi-Cloud Environment," *Health Informatics Journal*, vol. 25, no. 2, pp. 315-329, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sudeep Tanwar, Karan Parekh, and Richard Evans, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications*, vol. 50, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Anastasiia Strielkina et al., "Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment," *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, pp. 67-73, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] M. Sornalakshmi et al., "RETRACTED ARTICLE: Hybrid Method for Mining Rules Based on Enhanced Apriori Algorithm with Sequential Minimal Optimization in Healthcare Industry," *Neural Computing and Applications*, vol. 34, pp. 10597-10610, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Parisa Naraei, Abdolreza Abhari, and Alireza Sadeghian, "Application of Multilayer Perceptron Neural Networks and Support Vector Machines in Classification of Healthcare Data," *2016 Future Technologies Conference*, San Francisco, CA, USA, pp. 848-852, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[8] Utkarsh Agrawal et al., "Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 16, no. 1s, pp. 1-20, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Xu-Dong Li et al., "Multi-Layer Perceptron Classification Method of Medical Data Based on Biogeography-Based Optimization Algorithm with Probability Distributions," *Applied Soft Computing*, vol. 121, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Anil Chacko, and Thaier Hayajneh, "Security and Privacy Issues with IoT in Healthcare," *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, no. 14, pp. 1-7, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] Rashad J. McFarland, and Samuel BO Olatunbosun, "An Exploratory Study on the use of Internet_of_Medical_Things (IoMT) in the Healthcare Industry and their Associated Cybersecurity Risks," *Proceedings on the International Conference on Internet Computing (ICOMP)*, pp. 115-121, 2019. [Google Scholar]

[12] Duncan Sparrell, "Cyber-Safety in Healthcare IOT," *2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K)*, Atlanta, GA, USA, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Abdulaziz A. Albesher, "IoT in Health-Care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments," *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 2, pp. 181-186, 2019. [Google Scholar] [Publisher Link]

[14] Aarón Echeverría et al., “Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation,” *Applied Sciences*, vol. 11, no. 7, pp. 1-28, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Nicole M. Thomasian, and Eli Y. Adashi, “Cybersecurity in the Internet of Medical Things,” *Health Policy and Technology*, vol. 10, no. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Amir Djenna, Djamel Eddine Saidouni, and Wafia Abada, “A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks,” *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Pramila Arulanthu, and Eswaran Perumal, “An Intelligent IoT with Cloud Centric Medical Decision Support System for Chronic Kidney Disease Prediction,” *International Journal of Imaging Systems and Technology*, vol. 30, no. 3, pp. 815-827, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Suliman A. Alsuhibany et al., “Ensemble of Deep Learning based Clinical Decision Support System for Chronic Kidney Disease Diagnosis in Medical Internet of Things Environment,” *Computational Intelligence and Neuroscience*, vol. 2021, no. 1, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mehdi Hosseinzadeh et al., “A Diagnostic Prediction Model for Chronic Kidney Disease in Internet of Things Platform,” *Multimedia Tools and Applications*, vol. 80, pp. 16933-16950, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Alaa Noor et al., “An IoT based mHealth Platform for Chronic Kidney Disease Patients,” *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, Dhaka, Bangladesh, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Phanindra Reddy Kannari, Noorullah Shariff Chowdary, and Rajkumar Laxmikanth Biradar, “An Anomaly-Based Intrusion Detection System Using Recursive Feature Elimination Technique for Improved Attack Detection,” *Theoretical Computer Science*, vol. 931, pp. 56-64, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] M. Akshay Kumaar et al., “A Hybrid Framework for Intrusion Detection in Healthcare Systems Using Deep Learning,” *Frontiers in Public Health*, vol. 9, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Mustufa Haider Abidi, Hisham Alkhalefah, and Mohamed K. Aboudaif, “Enhancing Healthcare Data Security and Disease Detection Using Crossover-Based Multilayer Perceptron in Smart Healthcare Systems,” *CMES-Computer Modeling in Engineering & Sciences*, vol. 139, no, 1, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Wenjuan Lian et al., “An Intrusion Detection Method based on Decision Tree-Recursive Feature Elimination in Ensemble Learning,” *Mathematical Problems in Engineering*, vol. 2020, no. 1, pp. 1-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Darshana Upadhyay et al., “Intrusion Detection in SCADA based Power Grids: Recursive Feature Elimination Model with Majority Vote Ensemble Algorithm,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2559-2574, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Ya Li, Seyed-mohsen Ghoreishi, and Alibek Issakhov, “Improving the Accuracy of Network Intrusion Detection System in Medical IoT Systems Through Butterfly Optimization Algorithm,” *Wireless Personal Communications*, vol. 126, no. 3, pp. 1999-2017, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Oliver Kornyo et al., “Botnet Attacks Classification in AMI Networks with Recursive Feature Elimination (RFE) and Machine Learning Algorithms,” *Computers & Security*, vol. 135, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yan Zhang et al., “A Comparative Study of Cyber Security Intrusion Detection in Healthcare Systems,” *International Journal of Critical Infrastructure Protection*, vol. 44, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Mavra Mehmood et al., “A Hybrid Approach for Network Intrusion Detection,” *CMC-Computers Material Continua*, vol. 70, no. 1, pp. 91-107, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] Priya Das, and Sohail Saif, *Intrusion Detection in IoT-Based Healthcare using ML and DL Approaches: A Case Study*, Artificial Intelligence and Cyber Security in Industry 4.0, pp. 271-294, 2023. [CrossRef] [Google Scholar] [Publisher Link]