EasyChair Preprint

№ 15969

Machine Learning-Based Automated Threat Detection Network Security in Healthcare

Dharti Patel and Savitri Bevinakoppa

June 27, 2025

Machine Learning-Based Automated Threat Detection Network Security in Enterprises

Dharti Patel
School of IT and Engineering
Melbourne Institute of Technology
Victoria, Australia
MIT225099@stud.mit.edu.au

Savitri Bevinakoppa
School of IT and Engineering
Melbourne Institute of Technology
Victoria, Australia
sbevinakoppa@mit.edu.au

***Abstract*—This paper presents an automated threat detection for healthcare networks using machine learning models. It addresses the increased cybersecurity needs arising from integrating IoT devices and cloud services in healthcare. The approach involves data collection from IoT devices, pre-processing, and training models on historical attack data. It evaluates machine learning algorithms such as SVM, Naive Bayes, and Random Forest for their effectiveness in detecting threats, deploying them in real-time monitoring systems, and assessing their performance based on accuracy, precision, and recall.**

The results show that these models significantly improve threat detection and mitigation in healthcare networks, particularly in identifying anomalous behaviors that could lead to breaches. However, challenges such as limited real attack data and high false positive rates for some algorithms indicate the need for continuous model training and more advanced techniques. The proposed framework offers promise but requires ongoing innovation to keep pace with evolving cyber threats.

Keywords—machine learning, automated threat detection, network security, response system

I. INTRODUCTION

Organized under the larger field of health informatics, the healthcare industry has evolved to incorporate modern-day cultured technologies like artificial intelligence and machine learning, the Internet of Things, cloud services, and various web-based software systems. These technologies have improved treatment by increasing the rate at which patients are diagnosed in the early stages, improving access to healthcare facilities, and introducing new forms of treatment. The role of these technological advancements the point is that their utilization has led to the creation of a new age in healthcare. They created several opportunities for the enhancement of patient subjective condition and organizational-infrastructural development of healthcare [1].

This change has brought shocking disadvantages mainly due to misconceptions about various technologies especially in matters of security. The rising trend of cyberattacks on healthcare organizations is because of the high risk involved with accessing and storing such information. This is because records belonging to patients consist of personal details, their financial information, and most importantly their health status, making them relevant in black markets. Thus, there has been a prolific rise in the incidence of healthcare data breaches with hacking and insider misuse of privileged credentials constituting the most common vectors. The relationship of trust that patients have towards the healthcare providers since their privacy is violated [2].

This study aims to review the literature in search of primary solutions for protecting healthcare data and to develop a framework based on machine learning algorithms. Among AI's multiple subfields, machine learning presents wonderful tools for the identification and counteraction of attempts at unauthorized access. Applying machine learning in healthcare implies that the organizations carry out a better analysis of the system, observation of variances, and threats, as well as recognition of potential threats and formulation of quick reaction mechanisms.

The various risk factors that come with digital technology and the reasons behind the need for protective mechanisms are discussed [3-4]. The feasibility of using machine learning approaches to identify insider threats in healthcare contexts are identified. The specific approach and lay of the land for creating the suggested threat detection and reaction system based on machine learning will be discussed in the next section. Various steps for data gathering will be designed, with the help of IoT devices to get data from the healthcare centers in a real-time manner [5]. The model training phase will include a pre-testing of the various machine learning algorithms including Naive Bayes and Random forest using the labeled data sets.

Finally, the conclusion section will point out further study directions that could refine threat detection precision by using other advanced machine learning methods, including deep learning. It will also highlight the concepts that require models that more effectively manage the insider threat and given previously unidentified, new risks.

II. PROBLEM DOMAIN AND RESEARCH QUESTIONS

Digital technologies particularly the Internet of Things have recently become widely adopted by the healthcare sector, providing new and improved ways in which patients can be treated and diagnosed [6]. With the help of IoT devices like fitness tracking devices, smart health care equipment, remote diagnostics, etc. actual health monitoring and data recording have become easier and better therefore benefiting the patients. The application of these interconnected devices has resulted in the creation of multiple points of failure. Every connected thing can become a point of attack, and as a result, the threat reaches not only the specific connected thing but also the overall healthcare network. The amounts of data generated and shared by these devices, including clients' personal health information, and other operational highlights, make healthcare networks a prime target for hackers [7]. The utilisation of multiple web-

based software applications as well as cloud services introduces new vulnerabilities that can be used to compromise the data and assets of an organization.

Adding to these risks, insider threats, where an authorised user intentionally violates the organisational security policy to gain unauthorized access to network resources are also a cause for concern. It is for this reason that insider threats are some of the hardest to identify because they often act in secret and may even be trusted individuals. Such threats can be highly complex and usually do not pose a threat to organizations using traditional security mechanisms, thus requiring more sophisticated solutions. This research fills vulnerabilities by proposing automated threat detection and response systems based on ML systems. The use of artificial neural networks and other similar methods provides an opportunity to analyze huge amounts of information and search for suspicious activities and other unusual indicators pointing at the presence of threats, all this in real-time [8]. The integration of ML into healthcare organizations can increase security in an organized way to identify threats and quickly adapt to threats that may threaten the organization. The objective is to build an effective security model that can detect both the external threat as well as the internal threat thus providing adequate protection for the healthcare networks.

Research Questions:

- What are the distinct forms of security threats that confront healthcare networks?
- In what way will the application of machine learning techniques contain these vulnerabilities?
- What are the guidelines that will help in incorporating continuous authentication into the HC IoT framework?
- How can machine learning detect insider threats in healthcare environments?

III. BACKGROUND

Growing incidents of cyber threats to healthcare facilities put in light the importance of protection measures. Phases of patient records constitute healthcare networks that have become attractive targets for hackers. The implications that such breaches have included the loss of personal and financial data, to the loss of important medical services. The traditional security measures that are so necessary are even more insufficient to challenge the new forms of cyber threats [9]. As a result, existing and more advanced, preventive security measures are required.

The studies conducted in the last few years reveal that the application of Artificial Intelligence and Machine Learning can go a long way toward enhancing the detection and prevention of cyberattacks in the healthcare sector. These technologies are particularly effective in the context of processing big data and detecting patterns that potentially indicate a security threat. Unlike traditional methods, which depend on set rules and signatures, machine learning models are flexible and can learn new characteristics of threats as they unfold making it more beneficial when it comes to cybersecurity. For instance, organizations can use ML algorithms to identify links between specific process activities and criminal intent, including frequent login attempts or unusual access to data.

Research has shown that implementing ML can improve cybersecurity by using different techniques. More specifically, deep learning, a sub-discipline of the broader field of ML, has been found to offer great potential in insider threat detection, which is widely considered one of the most difficult areas of cybersecurity on account of its privileged status. Other methods like Hidden Markov Models and Support Vector Machines have been used before, but deep learning methods especially Recurrent Neural Networks seem to be far more effective in identifying intricate patterns of behavior that suggest an insider threat.

The goal of this research is to expand on these insights by creating a comprehensive Machine Learning model that can be used for the continuous identification and response to threats in healthcare networks. They believe that this framework may offer a structured and comprehensive solution for addressing external threats as well as internal ones in healthcare systems to improve their security and reliability.

Objectives of the Research

Creating a systematic approach to threat detection and response based on machine learning in medical infrastructure. This includes:

- Identify cyber threats and compare ML algorithms in terms of their efficiency in threat detection and prevention.
- Provide better security, the concern must be given to plan and adopt methods of continuous authentication.
- Design optimal approach to address insider threats affecting healthcare-related IoT systems.

IV. SYSTEM DESIGN

Internet of Things (IoT) are used to capture real-time information regarding healthcare facilities as shown in Fig.1. Many machine learning applications can be efficient for monitoring real-time information keeping security measures stored on the Internet. The data stored for the healthcare facilities such as health records of the patient, real-time monitoring records, and staff records. It keeps all new and old health reports for the individual patient, real-time monitoring of medical equipment, and the condition of the operation machines can be stored within large datasets.

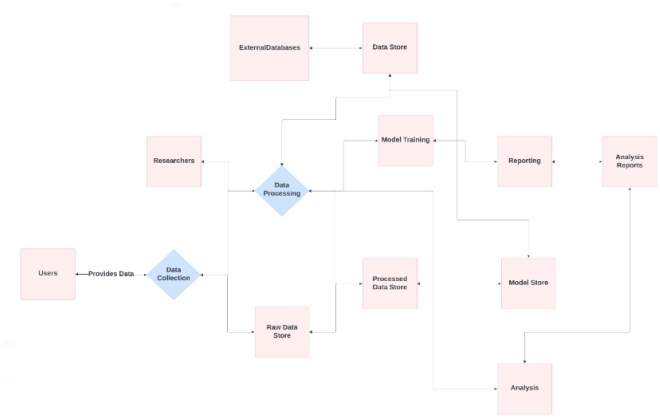

Fig. 1. System Design

The data collected for network security in the healthcare sector can be collected using IoT gadgets like sensors and devices which include smart tags, wearables, and various other IoT platforms [13]. IoT-based healthcare is focused on different aspects such as privacy and security technology, e-health, system design and architecture, and network and communication techniques. The data is collected from various IoT gadgets and stored at some platforms that will process this data under data cleaning and cleansing for easy data analysis. Further data analysis can be helpful in supporting or refusing the research hypothesis and then finally generating conclusions on the study subject matter [14].

Data Discretisation: It is the process that transforms the uninterrupted data into fixed intervals with the majority of data mining practices in the real world.

Data Normalisation: It is a process that includes the scaling of data in the form of attributes. It is also used for generating the data into smaller ranges for classification algorithms. It includes decimal scaling, minimum-maximum normalisation and Z-score normalisation.

Data reduction: It is a technique that reduces the data in the form that the meaning of data stays as it was. It includes data cube aggregation, dimension reduction and step-by-step selection methods [15].

Model Training: Using labelled datasets, perform experiments with different types of Machine Learning algorithms: Text classifiers Naive Bayes, KNN, Random Forest, Decision tree, SVM, Gradient boosting and LDA. Among the machine learning algorithms, the support vector machine (SVM) classifier algorithms have been getting better with time in most applications that are used for disease identification and face recognition. In the healthcare sector, the real-time monitoring and detection of chronic kidney-related diseases can be done by using the three main algorithms of machine learning [16].

Decision tree is shown in Fig. 2.

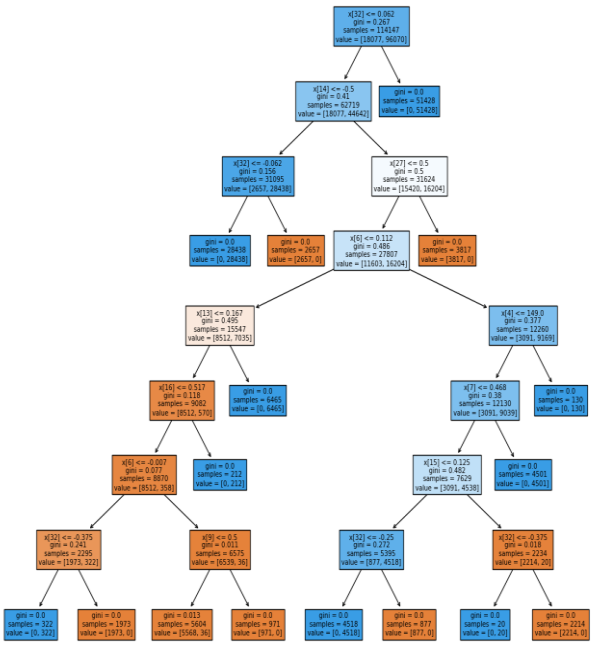

Fig. 2. Decision tree

KNN: It is one of the simplest but highly effective classification algorithms that stands for the K-nearest neighbour algorithm. It comes from competitive learning and lazy learning algorithms. It has advantages that include some features such as robustness for noisy data, ease of implementation, and effective results for large datasets of training data while it also includes some limitations [17]. Implementing as shown in Fig. 3, this algorithm in the network security of healthcare facilities can be costly and finding the k value is crucial and difficult at the same time. The mathematical formula as shown in equation 1, used for calculating the Euclidean distance is

$$E_d = \sqrt{\sum_{i=1}^{n}(a_i - b_i)^2} \quad (1)$$

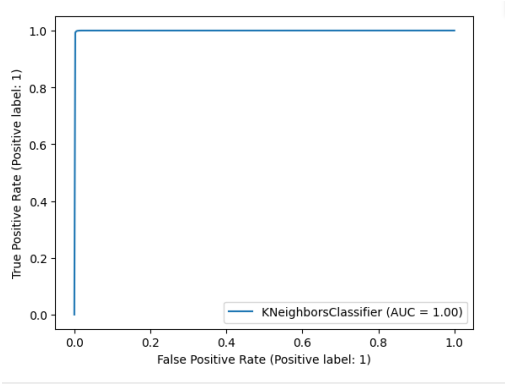

Fig. 3. KNN Results

Naïve Bayes: The multinomial naïve Bayes has been beneficial when used in classifying discrete features. This algorithm uses the probabilities of each attribute that comes from individual classes in the training set to predict the class of new data instances. This algorithm uses the Bayes theorem that states that the prediction of the datasets can be done with the assumption that attributes of the datasets that belong to a class are independent of each other [18]. The naive Bayes algorithm has been working well (as shown in Fig. 4) with both continuous and discrete datasets with individual class attributes. It can be mathematically (as shown in equation 2) defined by following the mathematical formula:

$$P(X|Y) = \frac{P(Y|X)P(X)}{P(Y)} \quad (2)$$

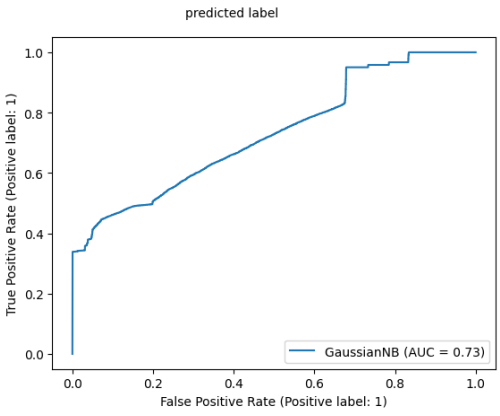

Fig. 4. Naïve Bayes Results

Random Forest Algorithm: This machine-learning algorithm is supervised for both classification and regression purposes. This research is used for classification purposes as it is beneficial in the betterment of the large datasets and experimental methods for detecting variable interaction. Still, it is complex for multiple values and uncertain attributes, and it also requires more computation power. It can easily be used in the Healthcare sector, customer intelligence and banking sector also for classification purposes [19]. Within the data pre-processing, it can be used for the filling of the missing values in large datasets to make them easily accessible for analysis purposes.

Threat Detection: Advanced algorithms in network security must be created in healthcare enterprises to detect threats to their data stored over internet-based platforms. This has radically changed with the integration of machine learning models that allow for real-time anomaly detection, instrumental in profiling and improving reactions to security threats. These models can analyse large amounts of data produced or captured by IoT devices, spotting patterns and deviations that may indicate possible breaches. Algorithms for supervised machine learning, such as Support Vector Machines and Random Forests, have already realised very high potential in identifying anomalous behaviours, hence very useful to improve cybersecurity within healthcare. For example, in an IoT-based health environment, ML models will be continuously monitoring network traffic flow and user activities to promptly raise red flags during any suspicious behaviour beyond their normality scores. Insider threat detection has become very important in security, as most insider threats are people with authorised access misusing those privileges. Training of ML models on historic data aids in recognising the slight indicators of insider threats and provides a robust defence to healthcare enterprises.

Response Mechanism: Effective response strategies for dealing with the detected threats should be formulated to protect the integrity and safety of healthcare data. The speed and efficiency of threat mitigation can be increased by machine learning automated response mechanisms. On detecting any threat, such models will trigger predefined response protocols such as isolation of affected systems, notification of security persons, and initiation of data encryption processes. AI and ML come into play in developing these response mechanisms to guarantee timely responses based on the analysis of real-time data that shall help minimise the potential damage. For instance, AI-driven systems automatically change the security settings to counteract the identified threat, reducing manual intervention and continuing the protection provided. Moreover, continuous learning algorithms underline the system's onward movement, adjusting new threats to ensure that healthcare networks are kept secure from already known and emerging cyber threats. Such an automated approach improves safety and opens an opportunity for each healthcare organisation to better use its resources for proactive measures rather than just response.

V. IMPLEMENTATION RESULTS AND ANALYSIS

Data Collection: For healthcare patients, it is necessary to have real-time monitored records for analysing their health conditions. This healthcare operation can be done by using the IoT gadgets that are offering various help to the hospital sector. These implementations of the usage of IoT gadgets such as wearables, ingestible sensors, smart beds, defibrillators, sensors monitor the environment, and inventory management to improve efficiency and patient care. The area of application of RFID technology has been providing wireless sensor applications in conventional hospitals to track moments of the patients who require ongoing supervision. IoT has been introducing technologies that are network-enabled which include wearable and portable devices for real-time monitoring, triggering, detecting, synergising, and connecting with comparable media across the Internet.

In the healthcare centre, IoT devices can be used for several purposes that use the Internet sources on the cell phones of the patients to monitor their ECG, vital signs, and blood oxygen saturation. These health records were processed and stored by using the Arduino, a micro-controller, that needs wi-fi to share data on Blynk for security and privacy reasons that also need to be improved in the future. Therefore, all the collected data from the real-time monitoring of the healthcare facilities can be stored on the gateways and cloud storage that manages the vast amount of data.

Model Training: It is expected that the performance of the selected machine learning models will be based on previous attack data while being trained. This comprises using historical datasets containing labelled examples of normal and malicious activities for such models to learn patterns of various cyber threats. For instance, datasets in the healthcare sector may contain varieties of network traffic data, system logs, and records of user behaviours. The usual way of training involves inputting these labelled datasets into models like Support Vector Machines, Naive Bayes, and Random Forests using supervised learning techniques so that they can learn from and generalise the input data. This step is crucial in making sure that such models can clearly distinguish between benign and malicious activities, hence increasing their predictive capabilities. In most cases, the training phase includes procedures of hyperparameter tuning and cross-validation to make models perform optimally without being overfitted, so the results are robust and reliable for threat detection in real-world scenarios.

Deployment: Next will be the deployment of a real-time monitoring system, typically an environment with a data ingestion pipeline, streaming analytics platform, and automated response system. At this practical deployment stage, models must be made scalable for handling high volumes of data originating from different IoT devices and health systems. Such data streams can be handled efficiently using technologies like Apache Kafka and Apache Flink. Later, the deployed models continuously monitor the network traffic and user activities 24/7 to detect threats in real-time, alerting security personnel in case of suspicious activity. Such a proactive approach will very quickly trigger the healthcare institution's response to potential threats and hence give it great control over its impact on both the patient data and general network security.

VI. CONCLUSION, LIMITATIONS, AND FUTURE WORK

According to the practical results, it can be ascertained that both Random Forest Classifier and Gradient Boosting Classifier have been the most efficient models in actualizing

the objectives of the dissertation. According to the results (as shown in Table I) of the evaluation metrics, the performance of the two models was alike: accuracy, sensitivity, specificity, F1 Score, and recall for both models were 100%. Thus, these results demonstrate the effectiveness of these models in creating an automated system of threat identification and subsequent response to internal and external threats.

TABLE I. COMPARATIVE RESULTS

Model	Accuracy	Sensitivity	Precision	F1 Score	Recall
Decision Tree	0.999553	0.999500	0.999969	0.999735	0.999500
Random Forest	1.000000	1.000000	1.000000	1.000000	1.000000
SVM	0.859497	0.964215	0.880270	0.920333	0.964215
Gradient Boosting	1.000000	1.000000	1.000000	1.000000	1.000000
Naive Bayes	0.442876	0.338673	0.998251	0.505759	0.338673
KNN	0.997477	0.998126	0.998875	0.998501	0.998126
LDA	0.887934	0.999813	0.882625	0.937571	0.999813

Limitations

Scarcity of Real Attack Data: Real attack data are pretty tricky to get since most attackers will apply sophisticated techniques to avoid leaving fingerprints. This scarcity severely restricts the possibility of proper machine learning model training and validation.

High False Positive Rates: Some algorithms in machine learning are pretty prone to yielding high rates of false positives, which raises undue alerts, wastes resources that are misdirected, and inundates security teams.

Problems of Scalability: Those models that work in a small setting are not easily translated to working across more extensive healthcare networks. Ensuring these models can still operate with the same efficiency in large-scale situations is itself a huge problem.

Complexity in Implementation: Integration of machine learning models into existing healthcare infrastructure is very human-resource-intensive, expertise-intensive, and time-consuming, which may complicate its wide adoption.

Dynamic Nature of the Threats: Cyber threats themselves are very dynamic, and this requires that, given changing circumstances, frequent updates and retraining are necessary for machine learning models to remain effective. The continuous upkeep needed for these can be resource intensive.

Data privacy concerns: Assurance of the privacy and security of sensitive patient data during training and deployment of machine learning models. Breaches are grave in nature.

Regulatory and Compliance Issues: Healthcare organisations are regulated by rigid laws that are the source of a host of problems in the implementation of novel technologies, including machine learning-based security solutions.

Future Recommendations

Advanced Machine Learning Techniques: Ten additional sophisticated machine learning techniques, including deep learning and ensemble methods to increase precision and adaptability in threat detection.

Insider threat detection: Develop models that can identify and mitigate insider threats. Usually, these are much harder to detect with traditional security measures.

Address New Forms of Cyber Attacks: Develop models for the identification and responses to, once new or completely unknown, cyber-attack forms to be always one step ahead of the attackers.

Large-Scale Experiments: Extensive experiments in simulation and real-world deployments to prove the efficacy and practicability of the proposed frameworks in real healthcare scenarios.

Continuous model training: Develop processes for regularly updating and retraining models to keep up with evolving cyber threats.

Collaboration with Experts: Engage critical experts from the cybersecurity community and very key practising health professionals in ensuring that developed solutions are workable, effective, and relevant to healthcare organizations.

Improved measures of data security: Integrate optimised encryption and anonymization technical capabilities to ensure patient data privacy and security in the processes of model training and deployment.

Regulatory Compliance: Ensure all machine learning solutions conform to healthcare regulations and standards for easier adoption and integration in existing systems.

REFERENCES

[1] T.O. Okoth, “Supply Chain Quality Management Practices and Performance of Private Hospitals in Kenya (Doctoral dissertation, University of Nairobi),” 2021.

[2] F. Sousa-Duarte, P. Brown, and Ana Magnólia Mendes, “Healthcare professionals’ trust in patients: A review of the empirical and theoretical literatures,” Sociology compass, vol. 14, no. 10, pp. 1–15, Sep. 2020, doi: https://doi.org/10.1111/soc4.12828.

[3] T. Dragos, A. I. Buzatu, C.-A. Baba, and B. Georgescu, “Business Model Innovation Through the Use of Digital Technologies: Managing Risks and Creating Sustainability,” vol. 22, no. 55, p. 758, Aug. 2020, doi: https://doi.org/10.24818/ea/2020/55/758.

[4] Y. Meng, “Analysis of Performance Improvement of Real-time Internet of Things Application Data Processing in the Movie Industry Platform,” Computational intelligence and neuroscience, vol. 2022, pp. 1–9, Oct. 2022, doi: https://doi.org/10.1155/2022/5237252.

[5] N. Mani, A. Singh and Nimmagadda, S.L. “An IoT guided healthcare monitoring system for managing real-time notifications by fog computing services,” Procedia Computer Science, 167, pp.850-859, 2020.

[6] M. Senbekov, T. Saliev, Z. Bukeyeva et al., “The Recent Progress and Applications of Digital Technologies in Healthcare: A Review,” International journal of telemedicine and applications, vol. 2020, pp. 1–18, Dec. 2020, doi: https://doi.org/10.1155/2020/8830200.

[7] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “A Survey on Security and Privacy Issues in Modern Healthcare Systems,” ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 1–44, Jul. 2021, doi: https://doi.org/10.1145/3453176.

[8] D. Gaifulina and I. Kotenko, “A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities,” Research Square (Research Square), Aug. 2022, doi: https://doi.org/10.21203/rs.3.rs-1975426/v1.

[9] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and Opportunities in Securing the Industrial Internet of Things,” IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 1–1, 2020, doi: https://doi.org/10.1109/tii.2020.3023507.

[10] A. I. Alsalibi, M. Khaled, M. A. Abu-Hashem, and Q. Shambour, “Internet of Things in Health Care: A Survey,” ResearchGate, Jul. 2021. https://www.researchgate.net/publication/353417003_Internet_of_Things_in_Health_Care_A_Survey (accessed Jun. 22, 2024).

[11] H. Taherdoost, “Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique...,” ResearchGate, Aug. 12, 2021. https://www.researchgate.net/publication/359596426_Data_Collection_Methods_and_Tools_for_Research_A_Step-by-

Step_Guide_to_Choose_Data_Collection_Technique_for_Academic_and_Business_Research_Projects (accessed Jun. 22, 2024).

[12] K. Maharana, S. Mondal, and B. Nemade, "A review: Data pre-processing and data augmentation techniques," Global transitions proceedings, vol. 3, no. 1, pp. 91–99, Jun. 2022, doi: https://doi.org/10.1016/j.gltp.2022.04.020.

[13] B. Wohlwend, "Classification Algorithms: KNN, Naive Bayes, and Logistic Regression," Medium, Jul. 14, 2023. https://medium.com/@brandon93.w/classification-algorithms-knn-naive-bayes-and-logistic-regression-515bdb085047 (accessed Jun. 22, 2024).

[14] S. U. Hassan, J. Ahamed, and K. Ahmad, "Analytics of Machine Learning-based Algorithms for Text Classification," ResearchGate, Apr. 2022. https://www.researchgate.net/publication/359668791_Analytics_of_Machine_Learning-based_Algorithms_for_Text_Classification (accessed Jun. 22, 2024).

[15] Md. J. Nayeem, S. Rana, F. Alam, and Md. A. Rahman, "Prediction of Hepatitis Disease Using K-Nearest Neighbors, Naive Bayes, Support Vector Machine, Multi-Layer Perceptron and Random Forest," 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), Feb. 2021, doi: https://doi.org/10.1109/icict4sd50815.2021.9397013.

[16] S. Uddin, A. Khan, M. E. Hossain, and M. A. Moni, "Comparing different supervised machine learning algorithms for disease prediction," BMC medical informatics and decision making, vol. 19, no. 1, Dec. 2019, doi: https://doi.org/10.1186/s12911-019-1004-8.

[17] M. M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," Scientific reports, vol. 14, no. 1, Mar. 2024, doi: https://doi.org/10.1038/s41598-024-56126-x.

[18] R. A. Rayan, C. Tsagkaris, and I. Romash, "The Internet of Things for Healthcare: Applications, Selected Cases and Challenges," ResearchGate, Jan. 05, 2021. https://www.researchgate.net/publication/348220261_The_Internet_of_Things_for_Healthcare_Applications_Selected_Cases_and_Challenges (accessed Jun. 22, 2024).

[19] S. Abdulmalek et al., "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review," Healthcare, vol. 10, no. 10, pp. 1993–1993, Oct. 2022, doi: https://doi.org/10.3390/healthcare10101993.