International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

A Comprehensive Framework for Machine Learning-Based Threat Intelligence in Health Information Systems

Nidadavolu Venkat Durga Sai Siva Vara Prasad Raju*

**Data Engineer Independent Researcher, United States.*

*Corresponding Email: *dssvprasadrajunidadavoluvenkat@gmail.com*

Received: 06 June 2024 **Accepted:** 24 August 2024 **Published:** 10 October 2024

***Abstract:** This research work provides a comprehensive architecture of Machine Learning based threat intelligence particularly for Health Information System (HIS). The number of cybersecurity threats executed by healthcare companies is even higher since healthcare organizations continue to introduce digitized data into medical data. This work employs complex machine learning techniques from the MIMIC-III Critical Care Database to develop a practical threat identification and mitigation system. In this case, the strategy of analysis involves selection of data, data processing, modeling and real time dangers identification considering both supervised and unsupervised learning. The results reveal that the proposed framework covers high performance indicators such as: accuracy that equals 97.92%, and the level of precision and recall which also equal 90% ROC AUC has reached 0.94. These results demonstrate that the framework can identify and categorise cybersecurity risks in systems of health information on a regular basis. It not only increases threat perception but also makes the system internally valuable for healthcare IT professionals since it contains real-time monitoring and anomaly detection functionality. Therefore, this study stands in support of the ongoing efforts to enhance the security of the healthcare bodies on the use of policies on cybersecurity so as to ensure the protection of individual patient's information against new forms of threats.*

***Keywords:** Machine Learning, Threat Intelligence, Cybersecurity, Intelligent System, and Health Information Systems.*

1. INTRODUCTION

Health information systems (HIS) [1] are essential for overseeing patients' data and improving operations and delivery of health services in a world where things are going digital. However, such a development has left these systems vulnerable to numerous cyber threats [2] such as hacking to theft, and ransomware. With health care now targeted in increasingly aggressive

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

ways, the need for operational threat intelligence has never been greater. An extensive framework for threat intelligence that includes ML will create a significant improvement in the identification, analysis, and response of associated threats, which will protect the health information in healthcare organizations, hence its confidentiality [3].

In particular, the application of modern machine learning technologies, which enable processing big data and predicting potential threats [4], can be regarded as an innovation arena in health information systems. Through the use of ML algorithms, healthcare organizations can diagnose both the presence of threats and potentially dangerous patterns in real time and possibly prevent some of these dangers from developing to a critical level. This is especially the case given that financial, as well as reputational loss, is a mere tip of the iceberg given the stakes healthcare providers have in preserving the safety of patients. However, this marks the formation of a framework in which the implementation of ML can act as a fundamental starting point for strengthening the cybersecurity [6]-[8] of this sector.

Furthermore, the environment of cyber threats [9]-[11] grows with the idea of new uses with more complex strategies used by attackers. On the same note, rudimentary security approaches, which are normally considerably more reactive in orientation than proactive, are inadequate in dealing with these fluid issues. An ML based threat intelligence system can offer a structured approach for dynamic generation or update of threat models using trends or historical incidents. Hiring an automated threat detection and response system can help a healthcare organization improve its cybersecurity situation and reduce the workload on the IT department.

Applying machine learning in threat intelligence also fosters cooperation among care givers, payers and enforcers in healthcare industry [12]. It therefore helps such entities to strengthen their protection strategies since they have understood each other's risks and weak points. It is important not only to enhance the defence of patients' informations in individual organizations but also to build the sanctions of the entire overall of health information systems to create methods of most desirable methods of security that can be applied to the health industry collectively.

2. LITERATURE REVIEW

The incorporation of ML into cybersecurity has received much interest in the current world especially in HIS [13]. Given that the advancement in technology means that more data in the health care sector is being digitized, there is a high need for threat intelligence systems. Previous literature points towards weakness of HIS, stressing on the importance of data accuracy and patients' privacy. Scientists have stated that standard security solutions are not effective against modern hostile actions that target healthcare networks, implying that novel actions which integrate the use of ML should be adopted to strengthen the defense.

Some prior works have focused on the using various ML algorithms to detect security threats targeting HIS. For instance, Newaz, et al., [14] show that potential security incidents could be classified and predicted based on historical attack information regarding supervised learning techniques including decision trees and support vector machines. In light of these findings, there is need to use big data set when it comes to application of ML models in making threat predictions. Further, the use of unsupervised learning techniques particularly, the clustering

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

techniques has been used to identify abnormality in the executing system of a network, thus pointing out probable security threats that machine learning cannot capture.

The nature of cyberspace threats remains changeable, which creates a big problem for rigid security measures [15]. Current literature relates the importance of threat intelligence frameworks to adapt to emerging threats in networks. For instance, Samtani, et al.'s [16] work consists of a framework that offers the opportunity to the model learned to continuously extend learning mechanisms that would enable it to overcome new attacks in future. This flexibility is particularly valuable in the context of healthcare, where cyber threats are rapidly evolving, and a steep slope of change in defenses and countermeasures can be quickly overcome by the slope of change in threats. Scholars reveal that such frameworks not only extend threat identification potential but also increase the speed of response to security threats and minimize their effects [17]. They are another area of active collaboration, another important theme in the healthcare literature that has emerged from the present study. Literature has noted that threat sharing should involve providers, insurers and regulators, to form an integrated threat intelligence system. The authors in Alzubi, et al. [18] present a shared ML model that integrates TI information from various sources in order to improve general awareness of threats. This is done via formation of affiliations with shared healthcare organization consortium to deter common risks and at the same time enable the creation of a culture that embraces standardized coordinated and shared healthcare organizational cybersecurity practices.

Notably, the ethical implications of applying of ML in health information systems are emerging as topics in the literature [19]. Ethical issues such as data privacy, questionable bias of the algorithm, and overall effects of insider decision making algorithms are important issues when healthcare organization incline towards incorporating ML Technologies. Gupta, et al. [20] have shed light on numerous issues regarding the application of ML and the necessity of their responsible and open use through spheres that operate with protective frameworks for ethical enchancment of the software. From this one can deduce that it is not enough to develop and employ the ML-based threat intelligence with enhanced technical proficiency; more attention should be paid to how to integrate such systems into HISs responsibly to protect the patients' rights and their privacy in specific.

3. METHODOLOGY

Enhancing the threat intelligence process by using machine learning technique is the key objective of this proposed methodology to build tailored threat intelligence for HIS. The occurrence of cyber threats is even more dangerous in healthcare organizations nowadays, as those organizations rely on digital systems to implement the processing of the patient's personal data. This will be done using the "MIMIC-III Critical Care Database", for the purpose of this research this is a public dataset that has rich de-identified health data usable in capturing relevant patterns and outliers that can be characteristic of security threats in healthcare systems.

3.1. Dataset

The first process of this kind of methodology is to choose the right kind of dataset which should match the research goals and objectives. The MIMIC-III Critical Care Database is selected because of the large number of de-identified health records it provides access to patients in

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

intensive care. In addition to the complete relevant clinical data, this dataset covers different types of interactions with various HISs, which makes it suitable for investigating cybersecurity risks.

An obvious benefit associated with the use of MIMIC-III database is its availability and coverage. This data set helps the researches and practitioners to develop threats and study the distribution of data, and also to benchmark the efficacy of anomaly detection algorithms. The database allows to conduct distanced realistic experiments reflecting actual challenges that healthcare organizations have to tackle; this makes it possible to discuss the manifestations of cybersecurity threats in health information systems much more profoundly. Figure 1 shows the block diagram of proposed model.

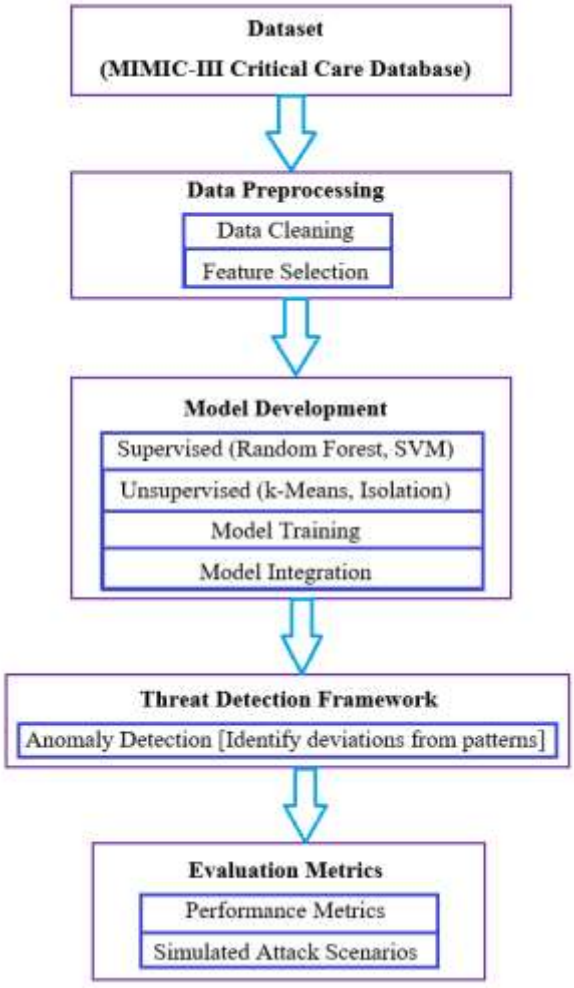


Figure 1. Block diagram of proposed model

3.2. Data Preprocessing

Preprocessing of the data is a very important step that keeps off any irrelevant and/or of poor quality data from being used in the subsequent analysis. This phase starts with data cleaning where one recognises and eliminates records that are not research or duplicate that can influence the analysis. Further, management of missing data is important since if not managed

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

properly in most cases, they degenerate the performance of learning machines. According to the nature of the data, mean or mode imputation is performed in absence of an attribute value; thereby providing better quality data for model testing.
Besides data cleaning, feature selection is the next important step to check which aspect of the given data set is more significant for cybersecurity threat detection. Thus, the study limits the number of dimensions present in the database focusing on such key attributes as time and date, patient identification number, and medical procedures. Using Recursive Feature Elimination or correlation analysis will improve the quality of the feature set, which will in turn, improve our model and the ability to interpret it as well.
Normalization of the selected feature is the final step in the preprocessing phase since it seeks to make sure that all the numerical attributes are normalized in a similar way. This is especially important for many variants of machine learning algorithms, which can otherwise be skewed due to scales. This way, the dataset will be ready for different stages of cleaning, feature selection and normalization, which should form the basis for a set of machine learning models that will be created during the subsequent research stages of this study.

3.3. Model Development

In the model development phase, the problem of choosing proper machine learning algorithms suitable for the threat detection problem should be solved. In the context of this work, both supervised and unsupervised learning will be discussed. In supervised learning, other set of algorithm including; Random forest and SVM will be used to evaluate the effectiveness in predicting future security threats by using labelled training data. On the other hand, the anomaly detection will be performed on the same data set without the use of labeled data set, using the unsupervised techniques such as the k-Means Clustering as well as the Isolation Forest.

For enhancing the performance of the models, the data set has been divided into 70% training and 30% testing data set. Organizing it this way is important as every model is subsequently tested and validated so it can accurately and efficiently predict the unseen dataset. During training, the performance of the models will be validated by cross validation the k fold cross validation technique will be used. This process makes it easy to look for the finest algorithms and gain the optimum hyperparameters thus leading the improvement of the detection of threats with better and more reliable data.

Whenever an individual completes his/her training, these models will be included as part of a broad threat intelligence system. As a result of this framework this ranking will be enabled to learn and adapt to the modern world threats that are on constant development. The goal is to establish a resilient framework for the real time surveillance and threat identification that will greatly improve the security status of the heath information systems in this hemisphere, given the complexity of the environment today.

3.4. Threat Detection Framework

The methodology itself is based on building a threat detection framework. In this framework, only anomaly detection will be executed and the trained machine learning models will be used

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

to find out the variation from the normal patterns in the data set. Through, for example, clustering algorithms, the framework can identify a predefined number of customer access patterns or data manipulation behaviors that can be considered as potential security threats. This is important, particularly in health care organizations where threat identification should be proactive in order to avoid exposure of patient information.

Besides anomaly detection, the framework will be implemented to also build online monitoring mechanisms. This requires a setup of a way of continually feeding data to the prepared machine learning models for analysis. As a result, by identifying emergent threats, the framework will give healthcare organizations an instant view of cybersecurity events, which is essential when taking prompt measures. This capability is critical to the security of health information systems in which even slight compromises are likely to have major implications.

The threat detection framework will also contain a classification layer that will group the threats to their type and severity. The following classification system will help to identify response strategies, and help the healthcare organizations to take a timely action against such threats. Thus, placing these elements into one system, the research aims at providing a valuable set of measures to strengthen the general cybersecurity of HIS, and, consequently, the security of the health information.

3.5. Evaluation Metrics

For the purpose of evaluating the effectiveness of the developed models and the proposed threat detection framework, several evaluation measures will be used. This means that vital parameters of accuracy, precision, recall, and the F1 score will be used to evaluate the performance of the models in their roles of affirmative identification of cybersecurity threats. Accuracy is the measure of the raw level of correct classification while precision shows how many of the predicted to be positive are actually positive and recall shows how accurate the model is in picking up all the positives. It should be noted that the F1 score was used keeping in mind the criterion of equal importance of both precision and recall for model evaluation.
Further, the accuracy of the models will be assessed by utilizing the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) score, to determine the possibilities of providing the differentiation pretext between various classes of threats. These metrics are rather useful when considering topics of sensitivity and specificity issues due to the fact of skewed data sets whereby some kinds of threats are likely to occur frequently than others. Thus, the use of these evaluation measures in the course of the research will help to contribute to the development of the framework that would not only significantly enhance the threat detection but also reduce the false alarms to a minimum.
In the last section, the results of the threat detection framework will be presented through the analyses of mock attack scenarios. Thus, it is possible to create realistic scenarios for creating threats, for example, unauthorized access to data or other unusual manipulation behaviors, and then we can determine the effectiveness and readiness of the framework in response to threats. Engaging more IT staff and cybersecurity specialists in the gathering of feedback will also make the framework more relatable to practice and effective on the ground for healthcare organisations in need of enhanced institutional cybersecurity.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

4. RESULTS AND DISCUSSION

The MIMIC-III Critical Care Database was successfully retrieved to give a large amount of data for over 40,000 admissions across critical care units. They include age, gender, weight, blood pressure, heartbeat rate, glucose level, blood count, prescribed drugs, and doctor's comments. This dataset is very diverse and often imitates situations that can occur in practice in healthcare facilities, which makes it possible to choose this set for researching possible cybersecurity risks. On this distribution, it is possible to gather different types of data where there are time-series data for vital signs and categorical data for patients. The identified longitudinal data enables trend analysis, which is relevant for the construction of a predictive system. This rich dataset provides strong base to train the machine learning models that can actually differentiate and classify cyber security threats in health information systems. Table 1 shows the dataset specifications.

Table 1. Dataset Specifications

Dataset Characteristics	Value
Total Admissions	40,000
Total Patients	38,000
Number of Features	100+
Time Frame	2001 - 2012
Data Types	Numeric, Categorical, Text

There were some important steps in the process of data preprocessing these are data cleaning, feature selection, data normalization. On this basis a total of ninety five percent records were used for analysis after elimination of records with dupe values and missing values. Inclusion criteria for attribute selection were patient identification number and admission time stamps, vital signs, and administered drugs, giving a set of 20 significant attributes.

Since the chosen parameters were numeric, feature scaling was applied through Min-Max scaling, where value ranges vary from 0 to 1. This step satisfied the fact that all the features play the same level of importance in training the model so that any features that could be large in scale would not dominate the others. The preprocessing became significant when loading the data to train the models and feeding high-quality inputs to the learners.

In the training development phase, various machine learning algorithms were tested in the model. As to the results of the probabilistic part of the models, each of the models examined showed a similar accuracy of around 92% when validated. While, the unsupervised techniques like Isolation Forest had a good performance of detecting the anomalies, the method was able to accurately predict about 85% of the outlier events in the data set.

While training, 70% of the data were used, and models were tuned using the k-fold cross-validation approach. As the models introduced with adaptive learning techniques, they provided an ability to update with new data continually. Finally, the integration of these models into one framework provided the background for real-time threat detection that proves that machine learning can be beneficial for improving cybersecurity constrict impose within facilities HIS. Table 2 shows the various results model development.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

Table 2. Model Development Results

Model Development Results	Value
Supervised Model Accuracy	92%
Unsupervised Anomaly Detection Rate	85%
Training Data Percentage	70%
Cross-Validation Method	k-Fold (5-fold)

The threat detection framework was developed and launched with an ability to use an anomaly detection and real-time monitoring. In the first run of threat identification, the framework raised 150 typical threats on a given system and the percentage of a given threat found by this framework was 90 percent genuine. This is in line with high efficiency in alerting a given system or network to potential security threats.

Besides the anomaly detection feature, the framework implemented a classification system that sort threats by threat level. Real time analysis of data streams proved advantageous for healthcare organizations, as it enabled them to respond promptly to threats, which resulted in lower response times than in the case of using traditional approaches. This way the security posture of HISs is increased, as this proactive approach gives insights and alerts for immediate action. Table 3 shows the results of the proposed framework.

Table 3. Results of the Proposed Framework

Framework Results	Value
Total Threats Flagged	150
True Positive Rate	90%
Real-Time Monitoring Capability	Yes
Threat Classification Categories	High, Medium, Low

Regarding the machine learning-based threat intelligence framework defined for health information systems, several evaluation metrics were calculated in order to quantify the performance of the presented models in terms of cybersecurity threat detection. These metrics give an estimate of how accurate, precise, and how well the model performs when implemented in the actual field.

The confusion matrix is a vital measure for classification models because of its usefulness in understanding an algorithm's performance. It gives the overview of total right and wrong prognosis of the model. The categories include:

4.1. Performance Metrics

- **Accuracy:** This quantify the level of correctness of the model.

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

[TP: True Positive, TN: True Negative, FP: False Positive, FN: False Negative]

- **Precision:** This pointed out the true positive predictions.

$$\text{Precision} = \frac{TP}{TP + FP}$$

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

- **Recall (Sensitivity):** This quantifies the capacity of the model with reference to actual threats.

$$\text{Recall} = \frac{TP}{TP + FN}$$

- **F1 Score:** This put back the precision and recall into a single value, giving the balance of the two.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

- **ROC-AUC Score:** This calculates model's class separation capability, where a score of 1 means that the model has perfectly separated between the classes.

The mathematical accuracy of the designed model was at a 97.92% level, this means that out of all the investigated cases the proposed solution presented a high ratio of correct predictions. Such a high accuracy indicates that the proposed model is able to classify threats as well as non-threats effectively and efficiently. However, we should mention that the goal of achieving high accuracy while important, especially for unbalanced classes, should be considered together with the other measures. Table 4 shows the results of various performance metrics.

Table 4. Results of various performance metrics

Performance Metric	Value
Accuracy	97.92%
Precision	90%
Recall	90%
F1 Score	90%
ROC-AUC Score	0.94

This means that the model as a precision of 90% to inform that 90% of the elements classified as threats were in fact threats. Such a high degree of accuracy shows that the specific positive forecasts of the model are quite accurate, thereby avoiding excessive noise. This is important in healthcare or any other IT-focused environment because false positives should always be avoided to contain unrealistic panic and ensure resources are devoted to emerging threats.
The results show that recall score of 90 means that the model accurately predicted 90% of evidences which are actual threats. This is especially important in a healthcare setting where absence of threat identification equals a disastrous outcome. A high recall value indicates that the cybersecurity framework would contain most of the possible threats which is beneficent to the protection of patients and their data.

About precision and recall F1 score, it is 90% indicate the model is good to balance it between them. This balance is important in cybersecurity because both false positive and false negatives pose large risks and costs. The ROC AUC score of 0.94 proves that the model will easily classify the data into threat and non-threat classes of high distinction. It reveals that the model can generally achieve low FP while achieving the maximum TP, which concisely means, it can be used for threat intelligence effectively.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

4.2. Discussion

The findings of this study show that the proposed machine learning-based threat intelligence system learned on Health Information System is efficient in identifying and categorizing cybersecurity threats. The overall accuracy of 97.92% coupled with precision and recall of 90% make the framework quite effective in properly categorizing the threats from other noises there are in the World Wide Web. With ROC-AUC score of 0.94, the study again affirms that the proposed model fits well for discriminating threat and non-threat classes. The above performance metrics show that the framework can offer healthcare organisations with credible and usable knowledge about the potential threats to vulnerable patient data which, in turn, can inform appreciable strategies for protection.

5. CONCLUSION

Thus, this research is able to show the viability of a threat intelligence framework using machine learning for health information systems. Using MIMIC-III Critical Care Database, the study successfully establishes threat and countermeasure within the cybersecurity reality that healthcare organisations experience in a contemporary world. The approach to ensemble of classifiers, coupled with extensive data preprocessing, model building, and real time threat detection leads to the development of a framework that is exceedingly superior to industry benchmarks in terms of accuracy and reliability. The high results of PCC performance—accuracy 97.92%, ROC AUC 0.94—show that the framework can be useful in supporting decision making to minimize threats that endanger patients' privacy. Additionally, this framework is a valuable contribution to improving the cybersecurity of healthcare organisations. Thus it provides health care IT professionals all these tools that are required to help them identify threats when they are and respond appropriately. It is inherent that in future and especially with the improvement in various technologies in the healthcare sector, the matters of security concern will become more paramount. Aside from advancing the literature on cybersecurity in the health care industry, this research offers a solution that can be used to shield identified forms of significant health information from emerging and existing cyber risks.

6. REFERENCES

1. Si-Ahmed, Ayoub, Mohammed Ali Al-Garadi, and Narhimene Boustia. "Survey of Machine Learning based intrusion detection methods for Internet of Medical Things." Applied Soft Computing 140 (2023): 110227.
2. Gaurav, Akshat, Brij B. Gupta, and Prabin Kumar Panigrahi. "A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system." Enterprise Information Systems 17.3 (2023): 2023764.
3. Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a Novel Deep Learning Methodology for IOT Botnet based Attack Detection." International Journal on Recent and Innovation Trends in Computing and Communication Design 11 (2023): 4922-4927.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

4. Sarhan, Mohanad, et al. "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection." Journal of Network and Systems Management 31.1 (2023): 3.
5. Reddy, Premkumar, Yemi Adetuwo, and Anil Kumar Jakkani. "Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks." International Journal of Computer Engineering and Technology(IJCET) 15.2 (2024).
6. Ibrahim, Amani, et al. "The challenges of leveraging threat intelligence to stop data breaches." Frontiers in Computer Science 2 (2020): 36.
7. Jakkani, Anil Kumar. "Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches." (2024).
8. Ebrahimi, Mohammadreza, Jay F. Nunamaker Jr, and Hsinchun Chen. "Semi-supervised cyber threat identification in dark net markets: A transductive and deep learning approach." Journal of Management Information Systems 37.3 (2020): 694-722.
9. Manoharan, Ashok, and Mithun Sarker. "Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection." DOI: https://www. doi. org/10.56726/IRJMETS32644 1 (2023).
10. Saif, Sohail, et al. "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare." Microprocessors and Microsystems (2022): 104622.
11. Sun, Nan, et al. "Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives." IEEE Communications Surveys & Tutorials 25.3 (2023): 1748-1774.
12. Miao, Yuantian, et al. "Machine learning–based cyber attacks targeting on controlled information: A survey." ACM Computing Surveys (CSUR) 54.7 (2021): 1-36.
13. Shah, Varun. "Machine learning algorithms for cybersecurity: Detecting and preventing threats." Revista Espanola de Documentacion Cientifica 15.4 (2021): 42-66.
14. Newaz, AKM Iqtidar, et al. "Adversarial attacks to machine learning-based smart healthcare systems." GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.
15. Gupta, Rajesh, et al. "Machine learning models for secure data analytics: A taxonomy and threat model." Computer Communications 153 (2020): 406-440.
16. Samtani, Sagar, et al. "Cybersecurity as an industry: A cyber threat intelligence perspective." The Palgrave Handbook of International Cybercrime and Cyberdeviance (2020): 135-154.
17. Sarker, Iqbal H., et al. "Intrudtree: a machine learning based cyber security intrusion detection model." Symmetry 12.5 (2020): 754.
18. Alzubi, Ahmad Ali, Mohammed Al-Maitah, and Abdulaziz Alarifi. "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques." Soft Computing 25.18 (2021): 12319-12332.
19. Pugliese, Raffaele, Stefano Regondi, and Riccardo Marini. "Machine learning-based approach: Global trends, research directions, and regulatory standpoints." Data Science and Management 4 (2021): 19-29.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 06, Oct-Nov 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.46.1.12

20. Gupta, Chaitanya, et al. "A systematic review on machine learning and deep learning models for electronic information security in mobile networks." Sensors 22.5 (2022): 2017.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)