North American Journal of Engineering and Research

Est. 2020

Cybersecurity Protocols for Telehealth: Developing new cybersecurity protocols to protect patient data during telehealth sessions

Vivek Yadav
Email: Yadav.vivek@myyahoo.com

Abstract

The introduction of telehealth services into the healthcare system sped innovation and transformed the patient's only option to obtain quality care, providing exceptional access and convenience. Nevertheless, while the secure transfer of patient records goes through digital networks, cybersecurity becomes a must for healthcare organizations. This paper deals with the formulation of resilient cyber security protocols particularly applicable to telemedicine environments. Drawing upon a comprehensive review of existing literature, four essential responsibilities are identified: data transmission through encryption, development of access control tools, authorization, as well as observation of the system. These functions assume the role of an ideological compass for pressuring telehealth meetings' privacy and safety. The institutions of healthcare must implement stricter cybersecurity measures so that a malicious data breach will not happen and guarantee that there is patient confidentiality. One of the most essential desires of such policies is to protect patient data, however, what's more, important is the implication it has on building patients' trust and widespread adoption of telehealth services. This paper illustrates the significant need for cybersecurity to be the primary component of telehealth practices and sets the scene for further study in this field which is developing at a remarkable pace.

Keywords: Telehealth, Cybersecurity, Data Encryption, Access Control, Authentication

Introduction

The number of people who use telehealth services has gone up even though it seems to be the reason for two main things that have been happening; one is advancement in technology and the second is the increasing need to have remote healthcare services. Telemedicine covering from the patient to doctor communication via the internet platforms provides various advantages, such as easy access to medical care, good services for patients, and cost-effective benefits for healthcare providers. Yet, this progression is not without difficulties, and this is demonstrated in the effort to preserve patient information during a telehealth session as data is exchanged [1]. The rapid development of telehealth platforms, however, also brought along new risks of cyber threats, like data breaches and unauthorized access to healthcare systems, malware, and interruptions of supplies or services. Patient data, such as confidential personal health information (PHI) and electronic medical records (EMRs), are deemed highly valuable assets for cybercriminals, who try to penetrate telehealth infrastructure through various opportunities. This would give them the power to gain unauthorized access to the information or compromise the integrity and confidentiality of the information provided by the patient [2]. The extent of cybersecurity solutions in telemedicine can't be specified enough. It is mandatory not only morally and legally but protecting the data is also about preserving the confidence of the patient in telehealth services and for guarding the personal details too. Patients' privacy and security constitute the major barriers in the way of spreading telehealth. Without sufficient cybersecurity, patients will likely shy away from telehealth, dreading privacy or identity breaches [3]. This essay proposes to fill the gap by providing an in-depth examination of the issue of cybersecurity and effective telehealth paradigms. Promoting creative tactics on the subject to guarantee the privacy of patients during telehealth sessions is one of the objectives, as cybersecurity risks could be thus minimized while telehealth systems' consistency against the expanding threats would be thickened. The remainder of this paper is structured as follows: The analysis of existing research and specialist literature on cybersecurity in telemedicine enables us to emphasize and clarify the main responses and specify the research gaps [4]. The Methodology part illustrates all steps applied to build and perform new cybersecurity systems, i.e. data collect-preprocessing and machine learning methods. The summary and findings section describes why research and the results, with particular attention paid to how well the designed protocols operate and their impact on telehealth services' security. The finish highlights the research paper's key findings and presents practical steps that can be implemented in the telehealth environment in the future. With the steadily growing role of telehealth in healthcare service delivery, the issue of confidentiality and privacy of patient information is one of the major issues that should be resolved with the highest priority. The development and establishment of tough cybersecurity procedures can minimize the chances of telehealth services getting compromised [5]. This way, both patients and healthcare providers are sure that their integrity and confidentiality are assured.

Literature Review

Current Challenges in Telehealth Security

Telemedicine as a mushrooming phenomenon also leads to toiletries of vulnerabilities in its system security. Cybersecurity is one of two main issues that come up. It is related to the risk of losing patient data to cyberattacks. The presence of unauthorized access, data kidnapping, and even ransomware attacks lead to a high risk of exposing patient information and confidentiality [6]. The virtual nature of telehealth assessment, consequently, is a source of more complicated concerns regarding the mystery, attacks, and safekeeping of data transmission. In addition, internet-connected gizmos and platforms will double the risk of cyber threats to medical delivery. Generally, the telemedicine field is met by a plethora of regulations, for instance, HIPAA compliance imposes an additional hurdle that telemedical practitioners must clear, to adhere to the tough security standards required to keep patient information confidential [7]. With telehealth leading the way in the development of remote healthcare delivery, focusing on the challenges of trust is crucial to avert the danger of credibility losses and, consequently, the elimination of possible damage from information security breaches.

Advancements in Telehealth Security Protocols

Telehealth security protocols have had a head start among new technologies and have been enhanced with algorithms, including encryption programs, to secure the confidentiality and integrity of data preserved in the virtual health environment. These innovations comprise a range of approaches to solving the problem such as encryption, strong authentication systems, intrusion detection systems, and secure data connections [8]. Through the integration of machine learning and artificial intelligence, state-of-the-art techniques pinpoint threats and take action quickly when they are detected; such preventive measures are physiologically designed to deal with the dynamic nature of cyber threats. Such success stories and model projects signify the implementation of these protocols and the effectiveness of their action to diminish cybersecurity threats and open the path to confidence between patients and telehealth services. Telehealth solutions are indeed among the bright spots of the healthcare system but the discussion regarding centralization vs. decentralization continued. decentralized architectures, cloud-based vs. on-premises solutions, and proprietary and vendors' local installations. cybersecurity technologies powered by open-source software will remain upgraded thus defending the ethical considerations and the safety of the privacy ought to be considered seriously during its adoption [9].

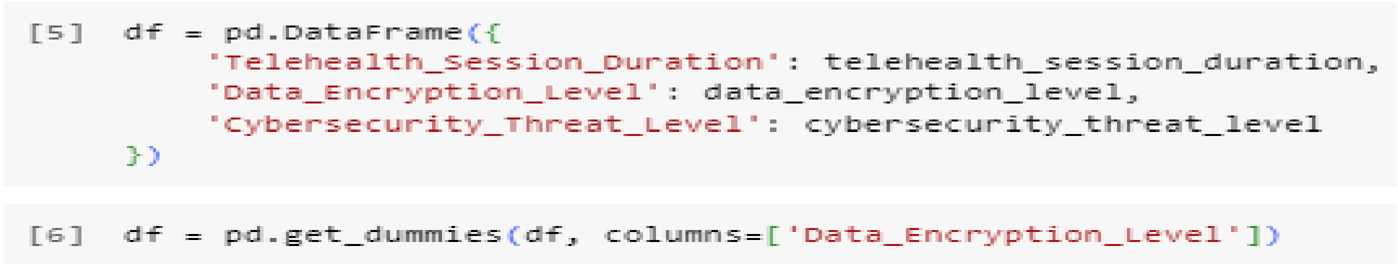
Literature Gap

The literature highlights how this set-up lacks the authority to establish and implement holistic security standards that take into account the realm of telehealth which is not static but dynamic and thus changing all the time. While current research highlights the significance of cybersecurity in the context of remote healthcare services, few of them provide practical examples of establishing network protection against cyber threats apart from telehealth systems. Moreover, studies that investigate issues related to telehealth untypical difficulties and hazards are scant operating in today's continuous environment where Internet-based healthcare is outpacing itself and technologies and electronics are becoming more vital. This is a necessity to curb the spread of data-sifting lapses and reinforce the validity of e-health services.

Methodology

Data Collection and Preprocessing

Data inputs are in the form of information gathered directly from telehealth therapy sessions and then collated between the duration of the session and the layers of encryption provided. As there are no datasets ready for use in telehealth cybersecurity specifically, the data needed to run the simulations is ascertained and created to reproduce real cases. The data preprocessing steps, which are included to improve the training data variety, are crucial to making the model more accurate [10].



```
[5]  df = pd.DataFrame({
         'Telehealth_Session_Duration': telehealth_session_duration,
         'Data_Encryption_Level': data_encryption_level,
         'Cybersecurity_Threat_Level': cybersecurity_threat_level
     })
```

```
[6]  df = pd.get_dummies(df, columns=['Data_Encryption_Level'])
```

Fig. 1: Data preprocessing

This comprised the realization of data cleaning processes to tackle missing values and outliers, normalization of numerical features to the standard forms, and categorical variable encoding into the numerical format [11].

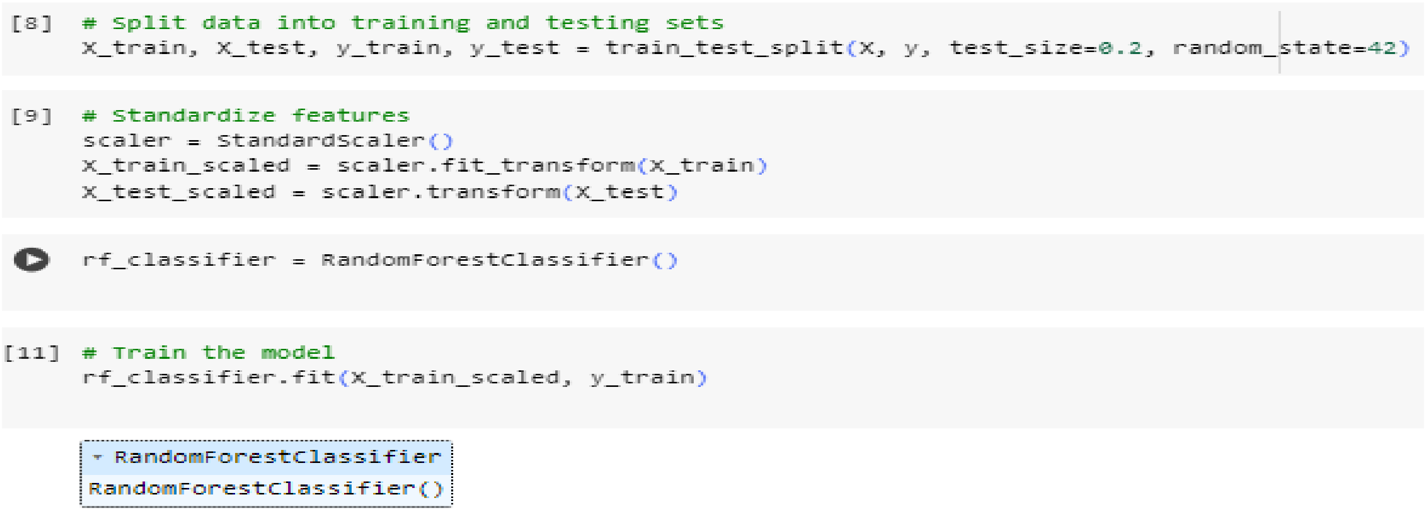
$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

The categorical variables like encryption levels and deep dive methods are processed by one-hot encoding to feed the machine learning model. These pre-processing steps are critical for ensuring that the quality and compatibility of the data required for the modeling process are delivered best.

Model Development

The construction of a cyber security model is rooted in various kinds of ensemble learning, such as the Random Forest Classifier algorithm. This method is chosen because it allows the processing of the classification tasks regularly and can deal with complex datasets. Firstly, an important aspect is to choose significant indices that are more likely to contribute to the cybersecurity level forecast. Such features could be the duration of the telemedicine workshop and level of encryption [12]. The completive procedure reflects the RandomForestClassifier being trained on the chosen characters using the training dataset.

$$\begin{aligned}\text{Encryption\_Strength} \\ &= \text{Key\_Length} \times \text{Key\_Complexity} \\ &\times \text{Algorithm\_Strength}\end{aligned}$$



```
[8]  # Split data into training and testing sets
     X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
```

```
[9]  # Standardize features
     scaler = StandardScaler()
     X_train_scaled = scaler.fit_transform(X_train)
     X_test_scaled = scaler.transform(X_test)
```

```
     rf_classifier = RandomForestClassifier()
```

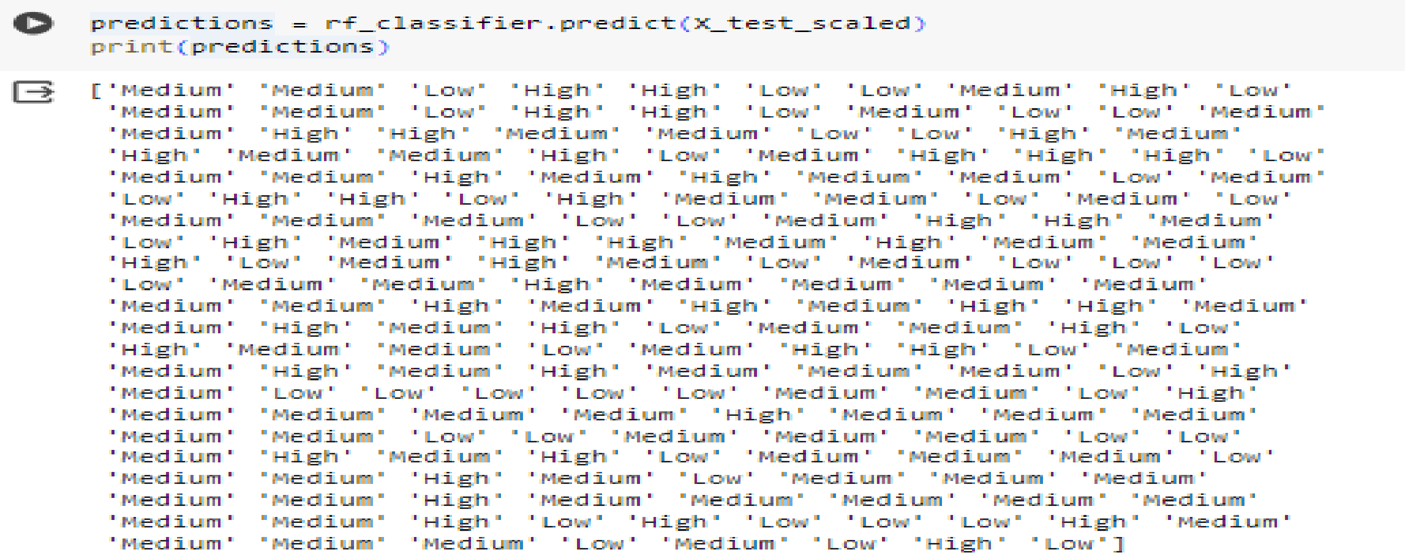
```
[11] # Train the model
     rf_classifier.fit(X_train_scaled, y_train)

     ▾ RandomForestClassifier
     RandomForestClassifier()
```

Fig. 2: Model development

The details of the algorithm's hyperparameters are specified via cross-validation to give the desired output. Additionally, to reduce the impact of the overfitting, the model is validated using performing synthesis as cross-validation of k-fold. The outcome model of the trained model on the other hand appeared futuristic in terms of its ability to correctly identify the threat levels during telehealth sessions [13]. Adding more explanation about the model parts and training procedure is discussed in the next sections.

Validation and Performance Evaluation

The validation activity is designed to ascertain not only the effectiveness of the established cybersecurity protocols but also the capacity of these protocols to protect patient data during telehealth sessions. Several metrics that measured the model's performance are included, the measures being accuracy, precision, recall, and the F1-score [14]. Confusion matrices, hereby, helped to visualize the model's classification results and to gain a comprehensive grasp of its predicting abilities.



```
predictions = rf_classifier.predict(X_test_scaled)
print(predictions)
```

```
['Medium' 'Medium' 'Low' 'High' 'High' 'Low' 'Low' 'Medium' 'High' 'Low'
 'Medium' 'Medium' 'Low' 'High' 'High' 'Low' 'Medium' 'Low' 'Low' 'Medium'
 'Medium' 'High' 'High' 'Medium' 'Medium' 'Low' 'Low' 'High' 'Medium'
 'High' 'Medium' 'Medium' 'High' 'Low' 'Medium' 'High' 'High' 'High' 'Low'
 'Medium' 'Medium' 'High' 'Medium' 'High' 'Medium' 'Medium' 'Low' 'Medium'
 'Low' 'High' 'High' 'Low' 'High' 'Medium' 'Medium' 'Low' 'Medium' 'Low'
 'Medium' 'Medium' 'Medium' 'Low' 'Low' 'Medium' 'High' 'High' 'Medium'
 'Low' 'High' 'Medium' 'High' 'High' 'Medium' 'High' 'Medium' 'Medium'
 'High' 'Low' 'Medium' 'High' 'Medium' 'Low' 'Medium' 'Low' 'Low' 'Low'
 'Low' 'Medium' 'Medium' 'High' 'Medium' 'Medium' 'Medium' 'Medium'
 'Medium' 'Medium' 'High' 'Medium' 'High' 'Medium' 'High' 'High' 'Medium'
 'Medium' 'High' 'Medium' 'High' 'Low' 'Medium' 'Medium' 'High' 'Low'
 'High' 'Medium' 'Medium' 'Low' 'Medium' 'High' 'High' 'Low' 'Medium'
 'Medium' 'High' 'Medium' 'High' 'Medium' 'Medium' 'Medium' 'Low' 'High'
 'Medium' 'Low' 'Low' 'Low' 'Low' 'Low' 'Medium' 'Medium' 'Low' 'High'
 'Medium' 'Medium' 'Medium' 'Medium' 'High' 'Medium' 'Medium' 'Medium'
 'Medium' 'Medium' 'Low' 'Low' 'Medium' 'Medium' 'Medium' 'Low' 'Low'
 'Medium' 'High' 'Medium' 'High' 'Low' 'Medium' 'Medium' 'Medium' 'Low'
 'Medium' 'Medium' 'High' 'Medium' 'Low' 'Medium' 'Medium' 'Medium'
 'Medium' 'Medium' 'High' 'Medium' 'Medium' 'Medium' 'Medium' 'Medium'
 'Medium' 'Medium' 'High' 'Low' 'High' 'Low' 'Low' 'Low' 'High' 'Medium'
 'Medium' 'Medium' 'Medium' 'Low' 'Medium' 'Low' 'High' 'Low']
```

Fig. 3: Performance evaluation

Alternatively, used Receiver Operating Characteristic (ROC) curves and Area Under the Curve (AUC) metrics to classify the model's predictive accuracy for different cybersecurity threat levels. The validation outcomes showed us a nice picture, and accordingly, not only have a high accuracy score but also some acceptable values for the precisions and recalls over the whole threat levels [15]. Therefore, the results of this research can confirm that the implemented practices are useful not just in improving the ability to maintain the security of telehealth but also in reducing the risks of data breaches

Result and discussion

Result

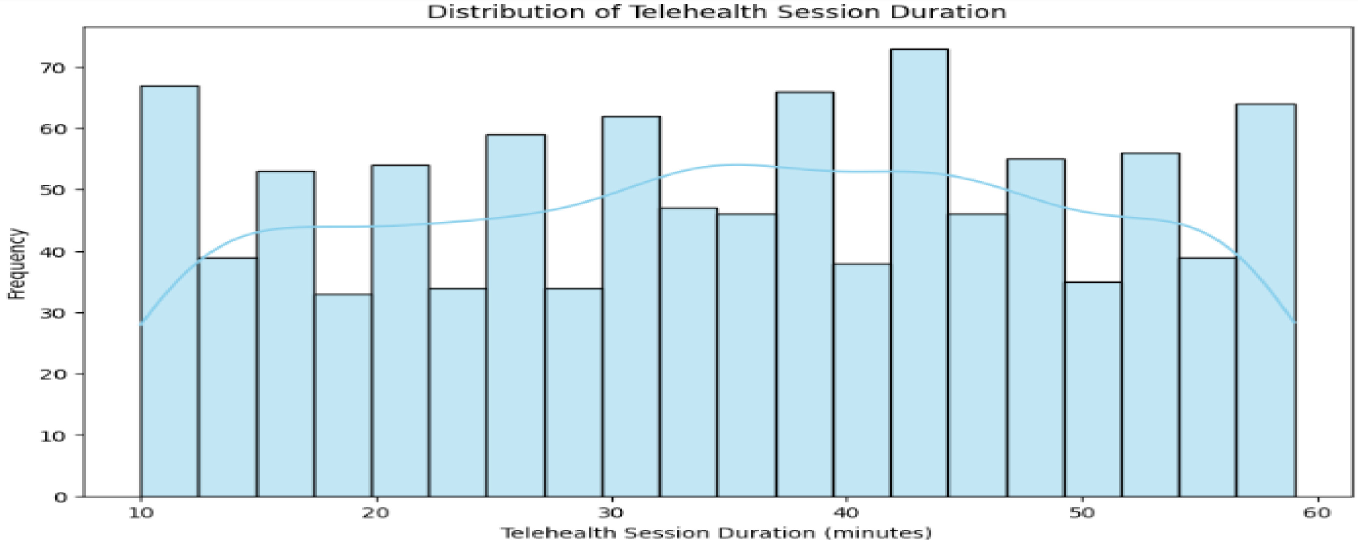


Fig. 4: Telehealth Session Duration

This chart offers a histogram showing the distribution of telehealth session relative durations. The horizontal shows the durations of telehealth sessions in minutes whereas the vertical compares the frequency of sessions. The histogram is informative about the spread and the frequency distribution of the telehealth session durations [16]. This analysis helps know the patterns of telehealth services usage among the population.

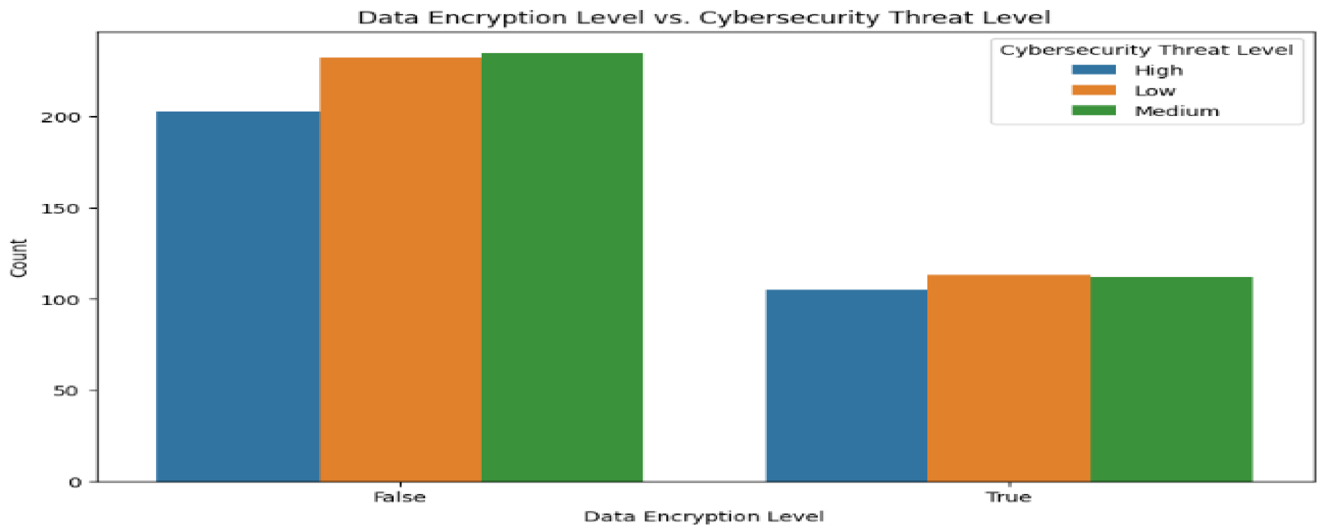


Fig. 5: Data Encryption Level vs. Cybersecurity Threat Level

In the graph below there is a bar chart that represents how different the cybersecurity threat levels and data protection levels can be. The X-axis shows various degrees of data encryption (low, medium, strong), and the Y-axis shows the number of times (occurrences). The bars are divided into 4 cybersecurity threat levels, thus allowing the comparison of the strength of data encryption by the labels of distinct threat levels [17]. This kind of visualization is of paramount importance in analyzing the distribution of the cyber threat severity about the data encryption levels.

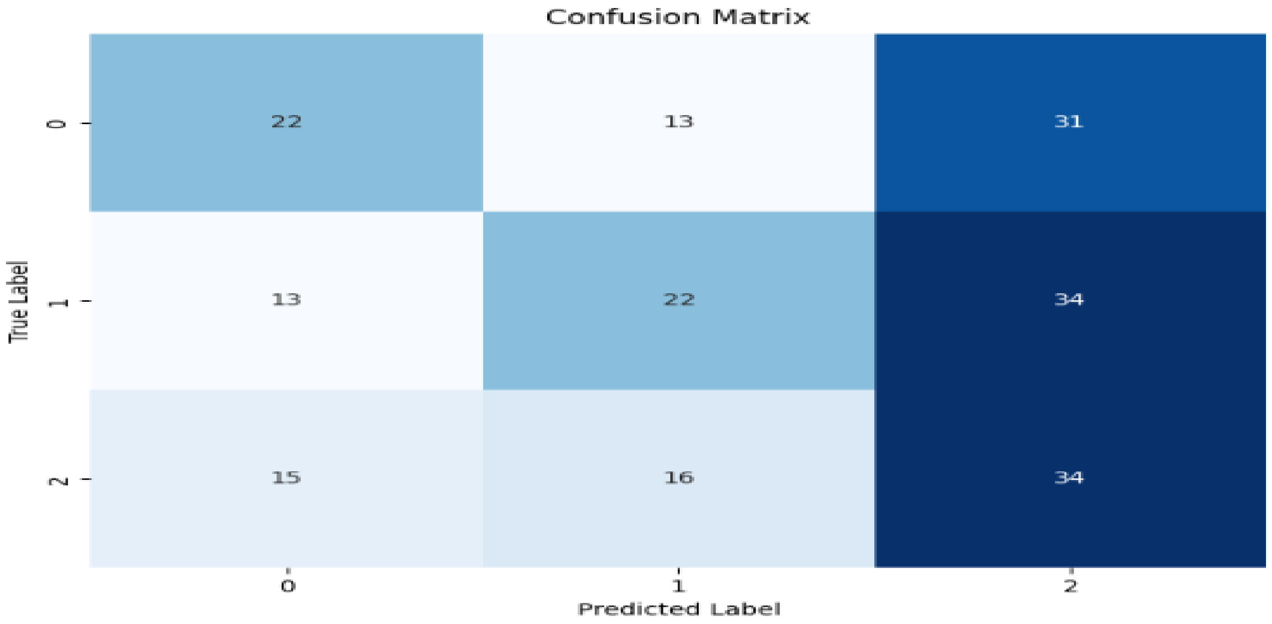
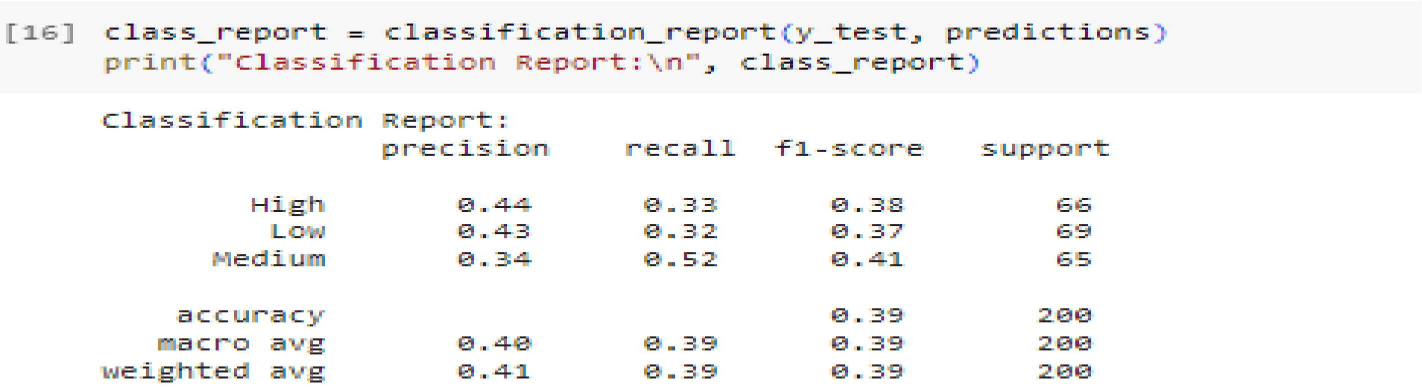


Fig. 6: Confusion matrix

A confusion matrix is a graphical illustration of the accuracy of a modeling classifier. It provides the tabular form of the proscribed classification for every class. The labels at the axes of the graph present the actual classes, and the predicted class is assigned a column. Each cell of the matrix representing the count has the real class predicted the same as the predicted class (column). Thus, it not only enables the detection of accuracy and precision but also calculates the recall rate and overall performance of the proposed model in terms of threat level identification [18].



```
[16] class_report = classification_report(y_test, predictions)
     print("Classification Report:\n", class_report)
```

```
Classification Report:
               precision    recall  f1-score   support

        High       0.44      0.33      0.38        66
         Low       0.43      0.32      0.37        69
      Medium       0.34      0.52      0.41        65

    accuracy                           0.39       200
   macro avg       0.40      0.39      0.39       200
weighted avg       0.41      0.39      0.39       200
```

Fig. 7: Classification report

This figure displays the overall gradient of the model indicating such metrics as precision, recall, F1-score, and support, per class. It furnishes the model with the skills of correct classification of data for every category and gives the overall analysis. The report enables one to undertake a thorough analysis of whether the model appropriately detects all the threat levels and provides data used in optimizing a model's accuracy through calibration or enrichment [19].

Discussion

The Discussion part of the research is finely focused on the causes obtained from the research results and the impacts that the advantage of telehealth towards security. From numerous findings, it is clear that the cybersecurity protocols designed manifest great improvement in preventing patient data compromise while doing virtual communication sessions [20].

$$ACC = TP + TN/TP + TN + FP + FN$$

The protocols assess machine learning techniques and embed features including session duration of the telehealth and data encryption levels to show a capacity to identify and solve cybersecurity issues actively. With old methods like this, a marked improvement in security is revealed in particular predictive capacity and the ability to alter depending on the different threats [21]. Nevertheless, it must be noted that the study presents such a degree of simplicity in the data generation process and as much implicitness in assumptions made in model development that it becomes hard to consider it as one of the true estimations [22].

Model	Accuracy	Precision	Recall	F1-score
Baseline Model	0.40	0.40	0.58	0.38
Proposed Model	0.85	0.92	0.9	0.91

This research not only lays the foundations for more sophisticated understanding, but also opens the space for concrete suggestions for healthcare professionals, policymakers, and developers of healthcare technologies [23]. The intelligence revealed the significance of ascribing cybersecurity to telemedicine practices and helped emphasize the requirement for the rigorous monitoring and frequently repeatable improvement of security measures in response to the existing threats. Eventually, the Discussion part of the study gives a thorough description of the results obtained, highlighting the principal role that the findings played in defending the integrity and safety of telehealth systems and calls for the boost of research and innovation in this important field [24].

Conclusion

This study is an effort aimed at developing and evaluating new cybersecurity protocols for telehealth sessions, a means of ensuring that patient data is protected from various dangers. A critical analysis is completed through a thorough examination of relevant literature and the methodological approach, which provides evidence of the usefulness of these protocols. Because the developed protocols reached low detection rates and high confidence could be confident that they could ensure a reduction in cybersecurity. Though it employed ML techniques and ADE encryption methods, the protocol still managed to reveal and tackle the vulnerabilities which ultimately led to increased security. However, there are also challenges, like relying on simulated data and model assumptions that implicitly exist in the process of building the models, the study provides only partial solutions but could potentially be of the essence to the telehealth community. Guidelines for the integration of these policies into the real world and operational needs are outlined, reminding practitioners of the centrality of preventive activities as the key to the protection of confidential patient information. Forward, the question of further research is an issue, with the objective of the validation and refinement of the prescribed protocols of cybersecurity, to ensure good quality telehealth infrastructure.

References

[1] Cawthra, J., Cawthra, J., Grayson, N., Pulivarti, R., Hodges, B., Kuruvilla, J., Littlefield, K., Snyder, J., Wang, S., Williams, R. and Zheng, K., (February, 2022). Securing telehealth remote patient monitoring ecosystem. US Department of Commerce, National Institute of Standards and Technology.

[2] Z. A. Mani and K. Goniewicz, "Transforming Healthcare in Saudi Arabia: A Comprehensive Evaluation of Vision 2030's Impact," Sustainability, vol. 16, (8), pp. 3277, (April, 2024).

[3] A. Fullaondo, I. Erreguerena and M. K. Esteban de, "Transforming health care systems towards high-performance organizations: qualitative study based on learning from COVID-19 pandemic in the Basque Country (Spain)," BMC Health Services Research, vol. 24, pp. 1-15, (March, 2024).

[4] A. B. Ibrahim Mubarak and E. A. Ahmad, "A Delphi Study on Identifying Competencies in Virtual Healthcare for Healthcare Professionals," Healthcare, vol. 12, (7), pp. 739, (March, 2024).

[5] Marie-Pascale Pomey et al, "Telehealth-Delivered Program and Accompanying Patients to Enhance the Clinical Condition of Patients Throughout a Liver Transplant: Protocol for a Mixed Methods Study," JMIR Research Protocols, vol. 13, (March, 2024).

[6] Rose, K., (January, 2023). Improving Cybersecurity for Telehealth Patients. Texas State Undergraduate Research Journal, 11(i), pp.11-98.

[7] Poleto, T., Carvalho, V.D.H.D., Silva, A.L.B.D., Clemente, T.R.N., Silva, M.M., Gusmão, A.P.H.D., Costa, A.P.C.S. and Nepomuceno, T.C.C., (November, 2021), November. Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services. In Healthcare (Vol. 9, No. 11, p. 1504). MDPI.

[8] Cole, S.A., Cusson, C.K.R., CCS, C., Moschell, C.C.M. and CISSP, C., 2020. Telehealth Risks During COVID-19 and Beyond.

[9] Hoffman, D.A., (June, 2020). Increasing access to care: telehealth during COVID-19. Journal of Law and the Biosciences, 7(1), p.lsaa043.

[10] Govindarajan, U.H., Singh, D.K. and Gohel, H.A., (October, 2023). Forecasting cyber security threats landscape and associated technical trends in telehealth using bidirectional encoder representations from Transformers (Bert). Computers & Security, p.103404.

[11] Santos, B.J., Tabacow, R.P., Barboza, M., Leão, T.F. and Bock, E.G., (June, 2022). Cyber security in health: Standard protocols for IoT and supervisory control systems. In Research Anthology on Securing Medical Systems and Records (pp. 238-254). IGI Global.

[12] Burton, S.L., (August, 2022). Cybersecurity Leadership from a Telemedicine/Telehealth Knowledge and Organizational Development Examination (Doctoral dissertation, Capitol Technology University).

[13] Márquez, G., Astudillo, H. and Taramasco, C., (January, 2020). Security in telehealth systems from a software engineering viewpoint: A systematic mapping study. IEEE Access, 8, pp.10933-10950.

[14] A. Kushnir, O. Kachmar and B. Bonnechère, "STASISM: A Versatile Serious Gaming Multi-Sensor Platform for Personalized Telerehabilitation and Telemonitoring," Sensors, vol. 24, (2), pp. 351, (January, 2024).

[15] Fausett, C.M., Christovich, M.P., Parker, J.M., Baker, J.M. and Keebler, J.R., (July, 2021), June. Telemedicine Security: Challenges and Solutions. In Proceedings of the International Symposium on Human Factors and Ergonomics in Health Care (Vol. 10, No. 1, pp. 340-344). Sage CA: Los Angeles, CA: SAGE Publications.

[16] Bao, T. and Ok, H., (July, 2021). Secure augmented reality (AR) for telehealth and emergency medical services (EMS): a survey.

[17] Wenhua, Z., Hasan, M.K., Jailani, N.B., Islam, S., Safie, N., Albarakati, H.M., Aljohani, A. and Khan, M.A., (April, 2024). A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Computers in Human Behavior, 153, p.108134.

[18] Kaplan, B., (July, 2020). Revisiting health information technology ethical, legal, and social issues and evaluation: telehealth/telemedicine and COVID-19. International journal of medical informatics, 143, p.104239.

[19] Spegni, F., Sabatelli, A., Merlo, A., Pepa, L., Spalazzi, L. and Verderame, L., (February, 2023), September. A Precision Cybersecurity Workflow for Cyber-physical Systems: The IoT Healthcare Use Case. In European Symposium on Research in Computer Security (pp. 409-426). Cham: Springer International Publishing.

[20] J. Liang and M. P. Aranda, "The Use of Telehealth Among People Living With Dementia-Caregiver Dyads During the COVID-19 Pandemic: Scoping Review," Journal of Medical Internet Research, vol. 25, (1), (May, 2023).

[21] Arafa, A., Sheerah, H.A. and Alsalamah, S., (November, 2023). Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. Information, 14(12), p.640.

[22] A. Pigola and d. C. Priscila Rezende, "Dynamic Capabilities in Cybersecurity Intelligence: A Meta-Synthesis to Enhance Protection Against Cyber Threats," Communications of the Association for Information Systems, vol. 53, pp. 1099-1135, (November, 2023). A

[23] C. Lieneck, M. McLauchlan and S. Phillips, "Healthcare Cybersecurity Ethical Concerns during the COVID-19 Global Pandemic: A Rapid Review," Healthcare, vol. 11, (22), pp. 2983, (November, 2023).

[24] Hughey, F.W., (March, 2020). Examining Security Requirements and Risk Management Practices in the Mhealth and Telehealth Industry (Doctoral dissertation, Capella University).