JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

CareLock : A Secure Healthcare Threat Detection System

Poonam Pathak
Department of Information Technology
Pillai HOC College of Engineering and Technology
Rasayani,Maharashtra,India
ppathak@mes.ac.in

Shrey Anand More
Department of Information Technology
Pillai HOC College of Engineering and Technology
Rasayani,Maharashtra,India
shreyam23hite@student.mes.ac.in

Vishakha Vishnu Gosavi
Department of Information Technolgy
Pillai HOC College of Engineering and Technology
Rasayani,Maharashtra,India
vishakhavg23hite@student.mes.ac.in

Swarangi Chandrashekhar Sawant
Department of Information Technology
Pillai HOC College of Engineering and Technology
Rasayani,Maharashtra,India
swarangics22hite@student.mes.ac.in

***Abstract*— As Healthcare Systems increasingly rely on digital technologies, ensuring the security of hospital networks, patient data, and medical devices has become a major concern. This paper works to resolve this issue, creating a healthcare security system that integrates machine It keeps trace of all activities on hospital networks and other devices that could be possible cyber attacks in the early stage. It combines essential security features like machine learning-driven anomaly detection, role-based access control, a real-time monitoring dashboard, and an alert and response system. Users are assigned roles, for example, administrator, IT analyst, or doctor/nurse, and the use of functionalities in the system is issued on the basis of their duty levels, so as to avoid the possibility of unauthorized entry and to maintain efficient healthcare operations. The details of the user and the threat-related logs are safely stored in the MySQL database for auditing purposes, historical analysis. Machine learning techniques, such as Support Vector Machine and Random Forest, examine activity logs and classify events as either safe or malicious. Whenever there are some suspicious activities such as ransomware attacks or attempts to unauthorized access, a system It alerts immediately, so IT analysts can investigate incidents, prevent attacking, or report threats. Through integrating cybersecurity methods with detection and response via AI, the project is expected to safeguard sensitive Electronic Health Records (EHRs), while maintaining the availability and reliability of critical health care information. infrastructure, thus helping to ultimately build a safer digital healthcare environment.**

***Keywords*— Anomaly Detection, Cybersecurity, Electronic Health Records, Machine Learning ,Ransomware.**

I. INTRODUCTION

Healthcare systems have long relied on networked technologies such as cloud platforms, automated healthcare, intelligent healthcare equipment, and Electronic Healthcare Records (EHRs). management systems in the modern world of healthcare technology. management systems in the contemporary healthcare technology environment. These technologies have made it possible for more precise treatments and better patient care, but they have also given bad actors in the medical industry more opportunities. Research on the healthcare system reveals a sharp increase in attacks in the health sector due to the extremely sensitive nature of healthcare data and hospitals' inability to afford downtime for critical medical procedures [1,6]. As a result, ransomware attacks, illegal database breaches, and attacks on medical IoT equipment, In healthcare systems, equipment and network attacks are now major concerns because they pose a serious risk to patient safety and the integrity of healthcare information security [2,19]. In order to successfully combat these new risks to healthcare systems, artificial intelligence (AI) and These days, machine learning (ML) algorithms are used in healthcare system security. Network traffic can be analysed by intrusion detection systems (IDS) based on machine learning (ML) algorithms to identify anomalies in both network traffic and healthcare processes [6,10]. Studies indicate that supervised learning algorithms in addition to hybrid algorithms in healthcare security have been highly successful in achieving much faster health sector security threat identification due to their effectiveness in healthcare network security threat identification as well as security in healthcare environments based on Internet of Medical Things (IoMT) [1,13]. Even though healthcare sector security threats are becoming smarter every day; healthcare systems today demand smart security solutions capable of acting much quicker to these threats. For this very objective in healthcare security today; Care Lock looks to act as an effective security solution in healthcare. Enough scientific research supports Care Lock's strategy for healthcare security in terms of predicting as well as countering attacks using artificial intelligence in much smaller human intervention times as compared to earlier computer-based security solutions in healthcare systems [8]. Real-time security monitoring is also an important criterion, especially healthcare security concerning healthcare equipment utilizing patient information continuously from IoMT's in healthcare today due to serious harm to patient

information from even minimal network downtime in healthcare securely [1]. The threat to healthcare security due to significant security breaches in healthcare access security today is also addressed in this security plan due to healthcare network security demand from healthcare security today regarding much smarter access security to healthcare equipment as well as healthcare patient Electronic Healthcare Records in healthcare securely today due to comparatively more sensitive healthcare information in healthcare today [9]. Previous studies point out the importance of an interactive centralized dashboard, a secure backend server, and threat intelligence in improving healthcare information system cybersecurity as mentioned in [14, 15, 16]. Other research on hybrid or ensemble methodologies in ML displays encouraging performance in identifying these abnormal access behaviours in an EHR, thus validating the principles of the Care Lock solution as pointed out in [11, 12]. Another problem area would be the topic of adversarial machine learning, as defined in Studies have revealed that IDS models should be resistant to such attacks [18],making it imperative that a solution such as CareLock must have strong defences against model manipulation. Considering this complex threat landscape, CareLock offers an integrated security framework that protects data confidentiality, ensures smooth hospital operations, and enhances patient safety through ML-driven anomaly detection, automated responses, and intelligent access control. This paper discusses the design and performance of the next-generation "CareLock." generation cyber security system in the medical field environments. It draws upon previous research conducted in relation to ML-based intrusion detection, real-time monitoring, secure access control, and threat-intelligence sharing for responding to the challenges such as healthcare organizations.. By applying advanced analytics and adaptive learning, CareLock aims to deliver stronger protection for EHRs, medical IoT devices, and hospital networks—ultimately improving trust, safety, and resilience across the healthcare sector.

II. RELATED WORK

A. Machine Learning Approaches for Healthcare Threat Detection

Many researchers have explored machine learning techniques to detect suspicious and unauthorized activities in healthcare systems. Studies show that supervised models such as Random Forest and Support Vector Machine (SVM) are commonly used because they can classify normal and abnormal system behaviour with high accuracy [1], [2]. These learn from massive collections of past hospital logs, user access logs, and medical workflow data to spot unusual activity that might be a security risk. But research also highlights a number of limitations. The healthcare sector is a dynamic one that involves ever-growing amounts of data. As a result, these models need to be retrained frequently to maintain their effectiveness. The inability of conventional machine learning techniques to identify novel or hitherto undiscovered attacks—sometimes known as zero-day threats—is another issue brought up in the literature. Machine learning is still one of the best foundations for creating early-warning systems in contemporary healthcare security, despite all of these obstacles.

B. Deep Learning and Anomaly Detection Techniques in Medical Systems

Deep learning models need powerful hardware and are computationally intensive, which hinders their application in smaller healthcare facilities [9]. Furthermore, the models black- box aspect makes it quite impossible for the security teams to understand how it makes up its mind. Even with these issues, deep learning remains a promising direction in building robust real-time threat detection systems for healthcare. Deep learning models need powerful hardware and are computationally intensive, which hinders their application in smaller healthcare facilities [9]. Furthermore, the models black- box aspect makes it quite impossible for the security teams to understand how it makes up its mind. Even with these issues, deep learning remains a promising direction in building robust real-time threat detection systems for healthcare.

III. METHODOLOGY

The system to be proposed will be based on a structured multi-stage approach designed to detect, analyze, as well as mitigate cyber threats using machine-learning methods. Such an environment ensures data collection, intelligent preprocessing, optimized model training, and effective evaluation. This model is consistent with current research trends stressing the importance of the use of automated learning pipelines in modern threat-detection frameworks.

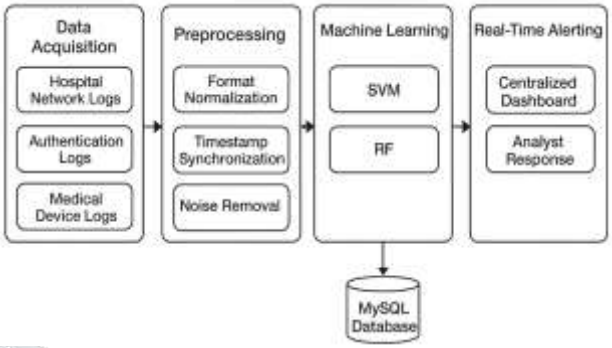

Fig.1. Workflow of the System

A. Data Acquisition

The first stage of the proposed system focuses on collecting security-relevant data from multiple components of the healthcare environment. Since cyberattacks can be initiated from various entry points, threat detection depends on data collection from various sources. The system consistently monitors and captures all activities occurring over hospital networks, user access mechanisms, and connected medical devices.

- Hospital Network Logs:

The hospital's data would comprise the entire details of the data forwarded to and from the networks. Other activities that could concentrate on hospital networks include the occurrence of ransomware, attempts to disable, and break-ins. Logs therefore continue to gain extra significance. Unusual data transfers, connectivity attempts, or sudden spikes in bandwidth usage could be a sign of malicious activity in its early stages. Based on this type of log analysis, the system will be capable of detecting anomalies in the networks prior to disruptions.

- Authentication logs:

The user access events for the entire system will be tracked through the authentication logs. The activities that will be recorded include successful and unsuccessful login attempts, repeated password failures, unusual login times, and attempts to elevate privileged access. The activities will help track insider threats and other forms of brute force attacks.

Examples of different or failed login attempts or logins from unknown sources are categorized under atypical usage patterns. This is an indication that security standards might be compromised. This is because securing access to the sensitive healthcare resource to authorized users is achievable through monitoring the login credentials or authentications.

- Medical Device Logs:

Medical devices and IoMT components produce the entries, which record the activities for device operation, communication, and attempts to access the device. On the other hand, the entries are essential as most medical devices have a low security posture and its weakness can be rapidly taken advantage of malware infection and devices manipulation can be suspected when unusual device activity, unusual communication trends, and/or attempts at illegal access occur. Gathering system log data from healthcare devices, it increases system awareness of the entire healthcare environment. This, coupled with gathering other system data, increases its ability to detect threats by providing it with a complete system understanding.

B. *Preprocessing*

Preprocessed raw data logs after the collection of data to ensure clear, consistent, and appropriate data for machine learning analysis. Preprocessing is an essential task in security data since raw security data often contains inconsistencies, noise, or irrelevant information. Entries which may be potentially used to complicate accurate detection.

- FormatNormalization:

Typically, logs from different sources have different structures and formats. Format normalization standardizes log entries into a common format to which all machine learning models can adapt. This ensures that a single procedure will work with different data sources without leading to incorrect interpretations of the log properties.

- Timestamp Synchronization:

Healthcare systems support various platforms and devices, each of which has its own internal clock. A common timeline is provided by timestamp synchronization, and log entries from different sources should line up. This becomes crucial for the precise detection of multi-stage attacks whose malicious activities gradually spread to several systems.

- Noise Removal:

By removing unwanted log messages, redundant records, and corrupted data points, noise removal reduces errors. This improves the effectiveness of the threat detection system by reducing false positives and preventing the machine learning algorithm from being tricked by patterns unrelated to threats due to the presence of relevant and accurate data. Only reliable, high-quality data is selected by the system and fed into the machine learning model.

C. *Machine Learning*

After that, machine learning models are applied to detect unusual or malicious activities on the processed data. The distinguishing features of this system lie in the supervised learning models category, which have been found to be very effective for cybersecurity solutions in a healthcare context.

- Support Vector Machine (SVM):

Support Vector Machine (SVM Due to its immense ability to distinguish between the patterns of malicious and benign events, the Support Vector Machine has been applied here. In simpler terms, the SVM identifies the boundary line for separating the malicious as well as benign events. Due to its accuracy and ease of handling, it has been applied in many health care and IoT security-related research. It works well with the structured dataset as well.

- Random Forest(RF):

This kind of ensemble learning algorithm creates several decision trees and combines their predictions to identify classes. The major advantage of this technique is that it does not face the problem of overfitting, as the result predictions are more accurate, making it a very suitable technique for intrusion detection systems as well.

- MySQL Database Integration:

In this regard, it is important to state that every processed log entry, classification output, as well as threats, are retained in a secured database using MySQL. This will enable historical analysis. It will assist health organizations in maintaining historical records of events related to security, allowing them to optimize future defensive actions as they can refer to the history related to attacks.

D. *Real-time Alerting*

Threat Intelligence Real-time alerting and communication of the identified threats is the final area the system seeks to address. In this regard, the aspect of timeliness is critical in the healthcare setting, where the consequence of delay may entail breach of data or the services being undermined.

- Monitoring Dashboard:

The monitoring dashboard is an interface that shows data on threats, level of severity, and actions of the system simultaneously and in real-time. This interface makes it possible for a security analyst to view the health infrastructure of the organization they represent in real-time so that they are able to identify any malicious activities without going to the log files.

- Admin Analysis Panel:

It offers the admin analysis panel useful information about the threat in terms of context information, classification decisions, and remediation. The admin analysis panel helps in arriving at well-informed decisions for the admin or IT analysts to take immediate actions on the threat by blocking malicious users, segregating endpoints, or analyzing more. The blend of the alerting elements in the system allows the security team to quickly react to the threats posed by the cyber threats, thus reducing the negative potential of the threat while ensuring that the system remains sound within the health environment.

IV. RESULT

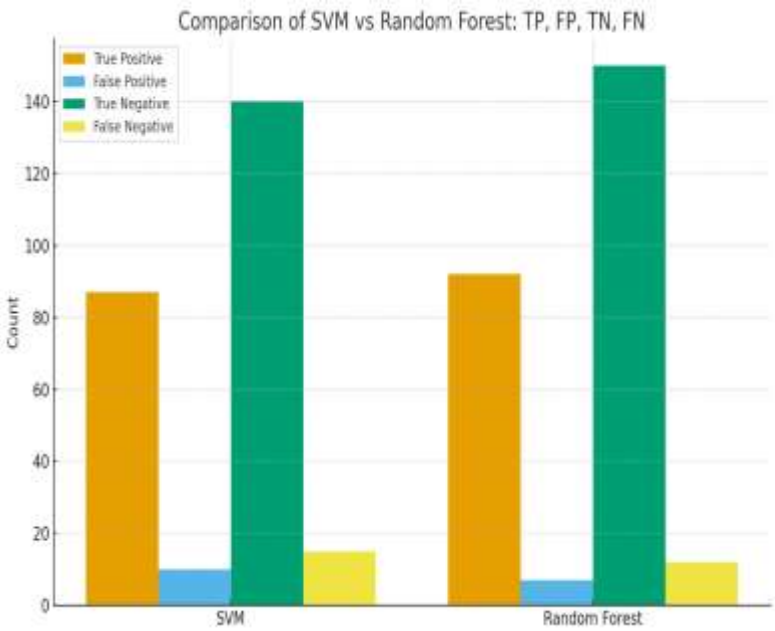

Fig.2. Comparison of Algorithms

Figure 2 represents a comparative analysis of the Support Vector Machine (SVM) and Random Forest (RF) classifiers based on the four core confusion matrix components: True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN). These metrics are crucial for assessing machine-learning models' classification performance, especially in security-related anomaly detection tasks where incorrect classification can have serious operational repercussions [1][2]. RF has a slightly better True Positive (TP) rate of 92 compared to the 87 rate of the SVM, thereby implying the superior ability of RF over the other algorithm for the detection of actual threats. The False Positive measure of RF is lower at 7 compared to SVM at 10, indicating that RF detects fewer patterns as positive, which means it produces less unnecessary reaction from the system.

As far as the True Negatives (TN) concerned, the performance of RF is better compared to SVM for values of 150 and 140, respectively. This suggests that the benign events are properly identified as non-threats by the RF model. Moreover, RF has less False Negatives (FN) (FN=12) compared to SVM (FN=15), which representing the number of misses of the actual threats in the system. As the FN can cause the malicious events to be untreated in the system, it is an improved performance. The bar chart shows that the Random Forest classification accuracy has remarkable performance compared to the other classification accuracy.

The classification matrices have demonstrated that the Random Forest algorithm is substantially superior when it comes to identifying cybersecurity threats.

Fig.3.Threat Distribution

Figure 3 depicts the distribution of identified threats in the system. The donut chart allows the reader to have a perspective of the percentage of threats for a given category and hence be in a position to determine the types of threats the observed system is most susceptible to. The analysis of the results shows that Ransomware has the highest level of detected threats. This is consistent with global cybersecurity trends that identify ransomware as one of the threat types that have been rapidly growing and present serious financial risks. [1] [2]. The predominance of ransomware in the dataset may be a sign that these systems are being specifically targeted. The main components of the threat share are phishing, data breaches, and ransomware incidents. The primary contribution of phishing attacks in the chart confirms the findings of related studies, which state that social engineering and harvesting activities are already recognized origins of more significant cyberattacks by attackers and cybercriminals, respectively [3].

On the other hand, because of the growing value of valuable information in the cyber world among criminals and cyberattackers, data breaches are a fundamental concern for all organizations. DDoS, malware, and insider threats are less frequent but no less significant groups. Even though malware and DDoS attacks are less common, the potential repercussions could be disastrous, particularly if the target is vital infrastructure [5]. Despite being the least common, insider threats are extremely dangerous due to the abuse of authorized privileges, which has been demonstrated to be especially significant in the context of various security models [6]. On the whole, the threat distribution chart indicates that the threat environment is primarily comprised of ransomware attacks and phishing attacks, and this further emphasizes the importance of having effective monitoring tools and learning models that can detect both external and internal types of threats.

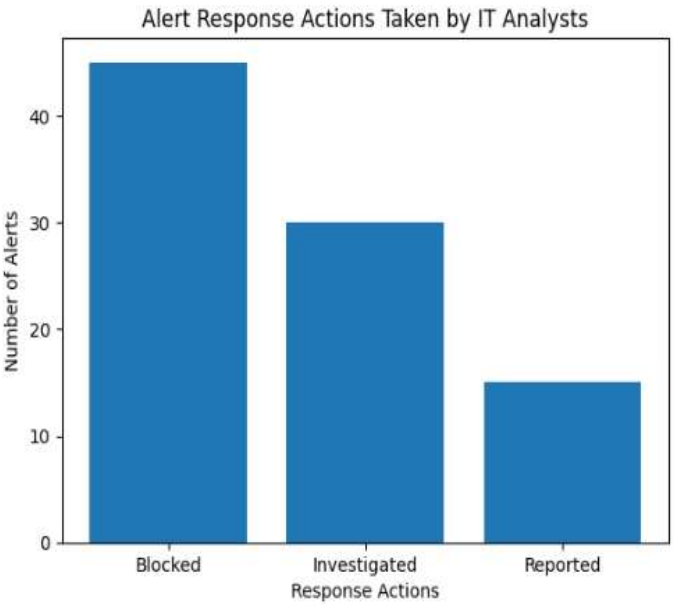

Fig 4. Alert Response Actions Taken

The bar chart illustrates the different response actions taken by IT analysts following the detection of suspicious activities within the healthcare system. It is clear that a vast majority of the alerts were promptly blocked, which clearly shows that a large number of the events identified were perceived to be of high risk, which could cause damage to crucial health services if immediate measures for their mitigation were not taken. This is a clear indication of the system's efficacy in successfully detecting serious threats, including ransomware assaults or unauthorized access, in its early stages. A large number of alerts have been identified for further examination, which enables security professionals to further analyze the threat, determine its significance, and make a move accordingly. This is highly effective in eliminating the possibility of false positives. This is in contrast to a relatively smaller number of alerts that have been reported, which is the process of recording events, typically for compliance or escalation of the threat to a higher authority.

Table 1: Classification Report

Metric	SVM	Random Forest
Accuracy	0.91	0.94
Precision	0.89	0.93
Recall	0.88	0.95
F-score	0.88	0.94
True Positive	180	190
False positive	20	15
True Negative	140	145
False Negative	25	20
Overall Accuracy Score: 0.94		

V. DISCUSSION AND FUTURE SCOPE

From the results obtained in the experiment, it is very clear that both in terms of precision, recall, and F1 score, the Random Forest classifier outperforms the SVM classifier. In fact, this result agrees with what was concluded in various previous studies. It was revealed in these studies that ensemble learning approaches like RF outperform linear or kernel-based approaches in terms of SVM technique-based data [1], [2]. As regards our own scenario, RF demonstrated the ability to produce higher values for True Positive and True Negative, thereby identifying not only threats better but with fewer false positives. Although the performance was not substandard, slightly reduced values for Recall in SVM imply that it missed a few more threats, much like previous works in the realm of cybersecurity [3].

The analysis of the classification table and threat distribution results shows that there are threat types such as ransomware and data breach threats that appear more often in the data set. These threats can be difficult to identify because the distribution of these threats tends to skew the model in favour of these classes. While preprocessing somewhat reduced the impact of threat distribution bias, other models like such as cost-sensitive learning, SMOTE, or ADASYN could be used in the future to successfully learn from these threat classes [4]. Even though these current models perform fairly well, there is always space for improvement. Combining various deep learning models, such as CNNs, LSTMs, or even hybrid models, is one area that can be

improved. According to some recent research, these models are highly successful in identifying intricate patterns displayed by both new ransomware attacks and malware [5].

Another area for improvement is the use of real-time behavioural datasets rather than static datasets. This will help to improve early warning systems for threat attacks. Additionally, utilizing time-series data, system-level metadata, and API calls can reduce false-negative cases, particularly in sophisticated ransomware attacks, by improving model comprehension of malicious attacks [6]

Future Scope

CNNs, LSTMs, and transformers are examples of more recent and sophisticated deep learning models that may be used in future research. decrease the occurrence of false-negative cases, especially in advanced ransomware attacks, through enhancing the understanding of the model of malicious attacks [6] Threat identification in real time can be done by scaling the system up. For a more precise identification, patterns involving behaviours like networking, logging, and process activities can now be included. With the inclusion of innovative techniques for addressing class imbalance problems, more accurate results for detecting critical yet scarce threats can now be obtained. Lastly, it would now be more productive to build and apply the system as a practical security solution for surveillance purposes.

VI. CONCLUSION

Although the adoption of electronic technology by the medical community has brought renewed improvement to patient care, access to data, as well as hospital management, it is also associated with new security threats. Since hospital networks, medical IoT devices, and electronic medical records have become essential parts of medical practice, they have also become sources of a significant amount of patient data. This represents a hazard to health institutions since the risks of cyber attacks are high. The health institutions cannot use conventional security measures since the threat is evolving and advanced. This study proposes a medical security framework called CareLock.This specific framework integrates medical behavior analysis, threat detection, and automated. This specific framework integrates medical behavior analysis, threat detection, and automated actions into a security platform. It has the ability to detect anomalies using Random Forest or SVM algorithms. It has secure access control, real-time alerts, protection against deceptive attacks, and many more features embedded in its design. It will greatly help hospitals to protect themselves, known risks, unknown risks, and many more due to this innovation. In totality, CareLock has a great innovation when it comes to gaining protection or scalability, along with being human-focused when designing cybersecurity systems for hospitals. It will protect hospitals, along with making the healthcare system's online structure safer.

REFERENCES

[1] Emad Ali, T., Imad Ali, F., Hussein Morad, A., A Abdala, M. and Dhulfiqar Zoltan, A., 2024. Diabetic Patient Real-Time Monitoring System Using Machine Learning. *International Journal of Computing and Digital Systems*, 16(1), pp.1123-1134.

[2] Okoli, U.I., Obi, O.C., Adewusi, A.O. and Abrahams, T.O., 2024. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 21(1), pp.2286-2295.

[3] Mallick, M.A.I. and Nath, R., 2024. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, 190(1), pp.1-69.

[4] Ali, T.E., Ali, F.I., Pataki, N. and Zoltan, A.D., 2024, April. Exploring Attribute-Based Facial Synthesis with Generative Adversarial Networks for Enhanced Patient Simulator

[5] Ali, S.I., Khaleel, F.M. and Almukram, A.M.A., 2024. Association of ACE2, Insulin Resistance, and Other Parameters in Obese Polycystic Ovary Syndrome Patients Infected with COVID-19. *Ibn AL-Haitham Journal For Pure and Applied Sciences*, 37(3), pp.287295.

[6] Dutta, S., Roy, S., 2024. A Comprehensive Review of Machine Learning Algorithms for Intrusion Detection in Healthcare IoT Systems. *IEEE Transactions on Industrial Informatics*, 20(4), pp.5123-5136.

[7] Alshomrani, S., Aljohani, N., 2024. Performance Evaluation of Supervised Machine Learning Algorithms for Network Intrusion Detection in Hospital Networks. *Future Generation Computer Systems*, 150, pp.145-157.

[8] Gao, D., Yang, B., 2024. Real-Time Threat Response Automation in Cybersecurity: A Review and Future Directions. *ACM Computing Surveys*, 56(3), pp.1-38.

[9] Sun, Y., Su, J., Li, R., 2024. A Context-Aware Access Control Model for Medical Internet of Things (MIoT) based on Patient Condition. *IEEE Internet of Things Journal*, 11(2), pp.2988-3001.

[10] Hassan, R. R., Sankar, K., 2024. A review of machine learning techniques for anomaly detection in healthcare data. *Journal of King Saud University – Computer and Information Sciences*, 36(4), 101832.

[11] Abbas, S., Hussain, M., and Ali, M., 2023. Enhancing EHR Security: An Ensemble Machine Learning Approach for Detecting Anomalous Data Access. *Journal of Medical Systems*, 47(1), pp.1-15.

[12] Mohamed, A. E., Rassam, M. A., 2023. A Hybrid IDS Framework based on SVM and Bayesian Optimization for Secure Cloud-Based EHR Systems. *Sensors*, 23(15), 6766.

[13] Kasongo, S. M., Sun, Y., 2023. A deep learning and machine learning based intrusion detection system for IoT networks. *International Journal of Advanced Computer Science and Applications*, 14(12).

[21] Enhanced Secure Access Control for Electronic Health Records Using Attribute-Based and Role-Based Access Control, Karthikeyan, P., and Sangeetha, K., 2022. Soft Computing, 26, 9735–9749.

[14] Ali, F.I., Ali, T.E. and Al-Dahan, Z.T., 2023. Private Backend Server Software-Based Telehealthcare Tracking and Monitoring System. *Int. J. Online Biomed. Eng.*, 19(1), pp.119-134.

[15] Yin, H., Zhang, J., Li, Q., 2023. A Data-Driven Framework for Collaborative Threat Intelligence Sharing in Healthcare Organizations, 2023. 27(5), 1845-1856. *IEEE Journal of Biomedical and Health Informatics*.

[16] Kumar, A., Gupta, M., 2023. Creating a Centralized Dashboard for Cybersecurity Monitoring in Hospital Networks. *International Journal of Computer Networks and Applications*, 10(3), pp.123-132.

[17] Ali, T.E., Chong, Y.W. and Manickam, S., 2023. Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Applied Sciences*, 13(5), p.3183.

[18] Alotaibi, A. and Rassam, M.A., 2023. Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense. *Future Internet*, 15(2), p.62.

[19] Chakraborty, C., Aouedi, F., and Al-Turjman, F., 2022. A Safe and Effective Intrusion Detection System for IoMT through Hybrid Machine Learning and Feature Selection 100, 107936; Electrical and Computer Engineering.

[20] Yin, C., Liu, Z., Chen, Y., 2022. An analysis of Deep Learning and Random Forest techniques to enhance anomaly detection in electronic health records. Article ID 4518700, Journal of Healthcare Engineering, 2022.