[1]**Dr. Vaishali V. Raje**

[2]**Dr. Shalini Goel**

[3]**Dr. Sujata V. Patil**

[4]**Mahadeo D. Kokate**

[5]**Mr. Dhiraj A.Mane**

[6]**Santosh Lavate**

Realtime Anomaly Detection in Healthcare IoT: A Machine Learning-Driven Security Framework

Journal of Electrical Systems

Abstract: - Healthcare IoT, a fast-growing field, could revolutionize patient monitoring and intervention. This interconnection raises new security concerns, requiring real-time anomaly detection to protect patient data and device integrity. This study presents a novel security framework that uses combination of Hidden Markov Models (HMM) and Support Vector Machine (SVM) to detect anomalies in real-time healthcare IoT environments with high accuracy. The framework prioritizes real-time strength and efficiency. Sensor data from wearables, medical devices, and other IoT devices is carefully segmented into time intervals. Features are carefully derived from each segment, including statistical summaries, patterns, and frequency domain characteristics. Feature engineering is essential for accurate anomaly detection. Integrating HMM and SVM capabilities is the framework's core. HMM accurately represent concealed states within divided data sequences and analyze patterns of change over time. After that, an independent-trained SVM examines each state. Using proximity to a decision hyperplane in feature space, this SVM can classify data points as normal or anomalous. This method augments HMM temporal capabilities with SVM classification efficiency, increasing sensitivity to anomalous patterns and reducing false positives. The framework's exceptional performance is shown by extensive evaluations on the PhysioNet Challenge 2017 dataset, which includes diverse ECG recordings with labeled anomalies. HMM-SVM outperforms Naive Bayes, LSTM, and Random Forest with 98.66% accuracy. The framework also has high precision, recall, and F1-score, indicating a refined ability to detect real anomalies and reduce false alarms. The framework prioritizes real-time understanding and application alongside its remarkable precision. HMM-SVMs reveal hidden data state changes, revealing context and possible causes of anomalies. Modular design and efficient algorithms enable seamless integration of real-time functionality in low-resource IoT devices, enabling quick and effective security responses. To conclude, this study introduces an HMM-SVM framework for fast Healthcare IoT abnormality detection. The framework emphasizes comprehensibility and real-time applicability while achieving high accuracy. This framework can protect patient data, improve device security, and create a more reliable healthcare IoT ecosystem.

Keywords: Realtime anomaly, Healthcare, Feature engineering, Segmentation, Hidden Markov Models.

I. INTRODUCTION

The emergence of the Internet of Things (IoT) has brought about a profound transformation in numerous industries, with healthcare being one of the most profoundly impacted. The implementation of Internet of Things (IoT) in healthcare entails the incorporation of interconnected devices and systems that gather, transmit, and analyze patient data instantaneously, resulting in the provision of healthcare services that are tailored to individual needs and more effective. This revolutionary technology has the capacity to enhance the monitoring of patients, enhance treatment results, and optimize healthcare processes. Nevertheless, as the use of IoT in healthcare becomes more prevalent, there is a pressing requirement for strong security protocols, specifically in relation to the immediate identification of abnormal occurrences[1], [2].

Anomaly detection in the context of IoT involves the recognition of atypical patterns or behaviors in data that deviate from the anticipated norm. Anomaly detection is of utmost importance in the healthcare industry, where precision is critical and the consequences are significant. It plays a vital role in ensuring patient safety, protecting medical devices, and safeguarding confidential health information. The real-time aspect of anomaly detection is particularly crucial in healthcare situations, where prompt intervention can be a matter of life or death. The need for efficient

[1]Professor Department of Community Medicine, Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth, Karad, Maharashtra, Email: vaishalinalawade@yahoo.com

[2]Professor, Department of Information, Communication &b Technology (ICT), Tecnia Institute of Advanced Studies, Delhi, India. Email: profshalinigoel1803@gmail.com

[3]Associate Professor Department of Community Medicine, Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth, Karad, Maharashtra,India. Email: sujapatil99@gmail.com

[4]Department of Electronics and Telecommunication Engineering SNJBs K B Jain College of Engineering, Chandwad Email Id: mdkokate66@gmail.com

[5]Statistician Department of Community Medicine ,Krishna Institute of Medical Sciences, Krishna Vishwa Vidyapeeth, Karad, Maharashtra, Email: dhirajmane123@gmail.com

[6]Department of Electronics & Telecommunication Engineering, AISSMS College of Engineering, Pune, Maharashtra, India. lavate.santosh@gmail.com

real-time anomaly detection mechanisms is becoming more prominent as the healthcare industry becomes more digitized and interconnected[3].

1.1. The role and significance of the Internet of Things (IoT) in the healthcare industry

The incorporation of IoT in healthcare yields numerous advantages that enhance the overall enhancement of patient care. Wearable devices, remote monitoring systems, and smart sensors facilitate uninterrupted data acquisition, enabling healthcare professionals to monitor patients' vital signs, chronic ailments, and adherence to treatment in real-time. This uninterrupted flow of data offers a comprehensive perspective on a patient's well-being, making it easier to identify potential problems at an early stage and allowing for proactive interventions[4], [5].

Furthermore, the integration of IoT technology in the healthcare sector facilitates the development of "smart hospitals," in which interconnected devices and systems optimize and simplify a range of procedures, spanning from patient admission to discharge. This leads to increased efficiency, decreased human errors, and improved utilization of resources. IoT-enabled asset tracking systems can enhance the efficiency of managing medical equipment and supplies, guaranteeing the timely availability of resources.

1.2. Significance of Anomaly Detection in Healthcare

Anomaly detection plays a crucial role in healthcare IoT by ensuring the dependability and safety of the data produced by interconnected devices. Deviation in health-related data can suggest significant problems such as malfunctioning of medical devices, cybersecurity risks, or even abnormalities in patient conditions. Swift detection of these irregularities is crucial in order to avert possible harm to patients, safeguard confidential medical data, and uphold the integrity of healthcare procedures[6].

Imagine a situation in which a wearable device is consistently tracking a patient’s essential physiological indicators. A system for anomaly detection can quickly identify abnormal patterns, such as abrupt increases or decreases in heart rate, which could indicate a potential health emergency. Within the realm of medical device security, anomaly detection serves the purpose of detecting and flagging instances of unauthorized access or tampering with connected devices. This proactive measure helps to minimize the potential for cyber-attacks and guarantees the preservation of patient data confidentiality.

1.3. Challenges and difficulties encountered when implementing Internet of Things (IoT) technology in the healthcare sector

Although the potential advantages of IoT in healthcare are significant, the integration of this technology is not devoid of obstacles. Significant obstacles arise from security concerns, interoperability issues, and the large amount of data generated. Ensuring the security of IoT devices and networks is a critical challenge in the healthcare sector, where patient privacy and data integrity are highly valued. Malicious individuals can exploit weaknesses in connected medical devices, which can result in harm to patients and the compromise of highly sensitive medical data[7].

The challenges of interoperability arise due to the wide variety of IoT devices, each with its own distinct communication protocols and data formats. Efficient operation of healthcare IoT relies on the smooth transfer of information among various devices and systems. Moreover, the substantial surge of data from diverse sources requires sophisticated analytics and data management solutions to extract significant insights[8], [9].

1.4. Motivation

This research is motivated by the growing use of Healthcare IoT and the associated security challenges it presents. With the healthcare industry adopting IoT technologies to improve patient care and optimize operations, it is crucial to prioritize addressing security concerns. The incorporation of IoT technology in the healthcare sector not only enhances operational efficiency but also introduces new avenues for potential risks and vulnerabilities.

The emergence of real-time anomaly detection is crucial in addressing these security challenges. The motivation stems from the acknowledgment that promptly detecting anomalies can reduce risks, safeguard patient safety, and guarantee the secure operation of IoT-enabled healthcare systems. The possible outcomes of unnoticed irregularities in this specific situation could vary from compromised patient data to interruptions in the functioning of medical devices, emphasizing the importance of creating strong and immediate anomaly detection mechanisms.

1.5. Gap in research

Although anomaly detection in Healthcare IoT is becoming increasingly important, current methods have certain limitations. Conventional methods for detecting anomalies may face difficulties in handling the constantly changing and diverse characteristics of healthcare data. Furthermore, the need for real-time performance introduces an extra level of intricacy, as any delays in identifying anomalies could result in significant repercussions.

The HMM-SVM hybrid approach aims to overcome these limitations by integrating the advantages of both Hidden Markov Model and Support Vector Machine models. The Hidden Markov Model (HMM) is particularly effective in capturing temporal relationships in sequential data, whereas the Support Vector Machine (SVM) offers resilience in accurately classifying patterns. The research aims to improve the accuracy and efficiency of anomaly detection in real-time healthcare scenarios by utilizing the complementary nature of these models.

1.6. Significant contributions

The paper's main contributions involve the introduction of a security framework driven by machine learning for detecting anomalies in real-time in Healthcare IoT. The HMM-SVM hybrid model is designed to overcome the limitations of current methods and provide a new approach to improve the accuracy and effectiveness of anomaly detection. The research contributions go beyond just measuring high accuracy metrics. They also involve conducting a thorough evaluation of the True Positive Rate (TPR), with a focus on the model's capacity to accurately detect anomalies in real-time. The research has the potential to have a significant impact by addressing the urgent need to enhance the security and efficiency of Healthcare IoT. This will benefit patients, healthcare providers, and the industry as a whole.

To summarize, the incorporation of IoT in healthcare ushers in a new era of opportunities and obstacles. The timely identification of abnormal occurrences is a vital component in reducing security vulnerabilities and guaranteeing the secure and effective functioning of healthcare systems enabled by the Internet of Things. This paper presents an innovative method called HMM-SVM to overcome current constraints and enhance the development of security frameworks for Healthcare IoT. The research highlights the significance of anomaly detection in this context and lays the groundwork for future progress in securing the convergence of healthcare and IoT technologies.

II. RELATED WORK

The implementation of advanced monitoring and diagnostic systems has been made easier as a result of the incorporation of Internet of Things (IoT) technology in the healthcare industry. Because of the growing volume of real-time health data generated by Internet of Things devices, it is imperative that a significant emphasis be placed on preserving the dependability and quality of the data. When it comes to identifying abnormal patterns or deviations from the norm in health-related data, anomaly detection techniques are absolutely necessary. The purpose of this literature review is to investigate a variety of studies and methodologies pertaining to anomaly detection for health monitoring that is based on the Internet of Things (IoT).

The authors, Mahmoudzadeh et al.[10] proposed a method to evaluate the quality of photoplethysmography in real-time health monitoring by utilizing Internet of Things technology. This approach is intended to be efficient and unobtrusive. Additionally, in order to gain insights into the accuracy of health-related data collected from Internet of Things devices, their methodology makes use of unsupervised anomaly detection. Syndrome is a spectral analysis technique that was developed by Sehatbakhsh et al.[11] for the purpose of identifying anomalies on medical Internet of Things and embedded devices. A reliable solution for anomaly detection is provided by this methodology, which focuses on identifying abnormalities in the spectral characteristics of data related to health. Specifically, the development of efficient methods for detecting anomalies in Internet of Things (IoT) systems that are utilized in smart hospitals was the focus of a study that was carried out by Said et al.[12]. The purpose of their work is to enhance the dependability of health data in Internet of Things environments by identifying anomalies in a timely manner in order to facilitate timely intervention.

As part of their research, Haque et al.[13] focused on identifying irregularities in wireless sensor networks that are utilized in the medical field. The findings of this study highlight the significance of identifying abnormalities in sensor data, particularly in the context of applications applicable to the healthcare industry. In the field of Internet of Things (IoT) healthcare analytics, Ukil et al.[14] emphasized the significance of anomaly detection. The findings of their research shed light on the significance of anomaly detection in maintaining the accuracy and reliability of health-related data in healthcare systems that are based on the Internet of Things (IoT). Using digital twins, Gupta et al.[15] presented a hierarchical federated learning method for anomaly detection in smart healthcare. This method was developed by the researchers. In order to improve anomaly detection in a hierarchical fashion, this innovative approach makes use of federated learning. This approach ensures that the healthcare data is both effective and confidential.

A framework was presented by Huang et al.[16] for the purpose of identifying irregularities in network traffic within the Healthcare Internet of Things platform. By identifying and analyzing abnormal patterns in network traffic, the primary purpose of this research is to improve the safety of Internet of Things (IoT) systems that are used in the healthcare industry. Within the realm of the Internet of Things (IoT), Oladimeji[17] developed an intrusion detection system that was tailored to meet specific requirements. With a particular emphasis on protecting the integrity and confidentiality of health-related data, the primary objective of this system is to identify and prevent unauthorized access in Internet of Things (IoT) systems. In order to better understand how to identify irregularities in time-series data for the Internet of Things (IoT), Cook et al.[18] carried out a comprehensive investigation. The research that they conducted provides a comprehensive analysis of the methodologies and frameworks that are currently being utilized to identify anomalies in time-series data that is generated by Internet of Things (IoT) devices.

Through the use of a comprehensive literature review, Fahim et al.[19] conducted an in-depth investigation into the methods of anomaly detection, analysis, and prediction that are utilized in Internet of Things environments. Through their research, they have provided valuable insights into the various methodologies that are utilized for anomaly detection in environments that are associated with the Internet of Things (IoT). A neural network called ANNet was developed by Sivapalan et al.[20] with the purpose of identifying irregularities in electrocardiogram (ECG) signals obtained from Internet of Things (IoT) edge sensors. ANNet was developed with the express purpose of being exceptionally lightweight, which makes it suitable for use in environments with limited resources. Their strategy revolves around the utilization of neural networks in order to accomplish the goal of achieving efficient and accurate anomaly detection in Internet of Things (IoT) applications for healthcare. A framework that is compatible with 6G technology was proposed by Wu et al.[21] for the purpose of anomaly detection in metaverse healthcare analytics in the Internet of Things. The purpose of their research is to investigate the capabilities of 6G technology in terms of enhancing anomaly detection for healthcare applications that are located in the future. The prediction of Alzheimer's disease in its early stages was the subject of research that Kavitha et al.[22] carried out using machine learning models on the subject. In spite of the fact that their research does not solely focus on anomaly detection, it places an emphasis on the wider range of applications of machine learning in the prediction of health-related anomalies.

Detecting anomalies in health monitoring systems that are based on the Internet of Things (IoT) is the focus of the literature review, which provides a comprehensive overview of the various methodologies and techniques that are utilized for this purpose. The development of robust solutions to ensure the dependability and security of health-related data in Internet of Things environments is currently being actively worked on by researchers presently. They are investigating a wide variety of approaches, which include lightweight quality assessment techniques as well as advanced neural network-based methods. In order to develop comprehensive anomaly detection systems for the rapidly growing field of healthcare IoT, it will be essential to integrate these various approaches.

III. METHODOLOGY

3.1 Data Acquisition and Preprocessing

a. Data source

The PhysioNet 2017 dataset has been used for training, which has provided a strong basis for developing and improving anomaly detection models. The dataset, obtained from PhysioNet, consists of physiological signals and annotations, providing a varied and extensive collection of data for training machine learning algorithms in healthcare settings.

Conversely, for the purpose of testing, sensor data has been gathered from a variety of wearables, medical devices, and other Internet of Things (IoT) devices in a healthcare environment. This dataset includes essential physiological measurements such as heart rate, oxygen saturation, and temperature, offering a comprehensive depiction of a patient's overall health. Furthermore, the gathered data encompasses details regarding levels of physical exertion, utilization of medication, and various factors pertaining to the surrounding environment. The purpose of this diverse testing dataset is to replicate real-life situations, guaranteeing that the anomaly detection models created are strong, flexible, and efficient in recognizing abnormalities in a range of healthcare-related factors.

b. Data cleaning

- **Imputation of Missing Values**

Missing value imputation is essential for preserving the integrity of the dataset. When dealing with continuous variables like vital signs, it is often recommended to substitute missing values with the mean or median of the corresponding variable. This ensures that the imputed values are consistent with the overall distribution. The mode can be used to impute categorical variables. It is crucial to meticulously apply the imputation process to both the training and testing datasets in order to ensure consistency.

- **Outlier Detection and Treatment**

Outlier detection and treatment: Outliers, which are often caused by errors in data entry or extreme physiological conditions, need to be identified and dealt with. Outliers can be detected using robust statistical measures like the interquartile range (IQR). Values that exceed a specific threshold, such as 1.5 times the interquartile range (IQR), can be classified as outliers. These outliers can be either substituted with a more appropriate value or eliminated from the dataset. The Tukey's fences method is a statistical technique used to detect outliers. Consistently applying outlier treatment methods to both the training and testing datasets guarantees that the anomaly detection model is trained and evaluated using dependable and representative data.

- **Ensuring synchronization of timestamps:**

Ensuring timestamp synchronization is vital when handling data from multiple devices. Discrepancies in timestamps can result in misinterpretations and impact the precision of anomaly detection models. To ensure synchronization, a two-step process can be utilized:

- **Timestamp synchronization**: To synchronize timestamps across different devices, one can either choose a shared reference point or employ interpolation methods. For example, by arranging data according to the initial recording time or employing linear interpolation to synchronize timestamps, one can ensure temporal coherence.
- **Verification and adjustment**: Following the alignment process, it is crucial to ensure synchronization by cross-referencing timestamps across devices. To resolve any remaining discrepancies, simply adjust the timestamps accordingly. This guarantees that events and measurements from various devices are precisely synchronized, establishing a dependable temporal basis for training and testing datasets.

Consistently applying these data cleaning methods to both the training and testing datasets enhances the development of reliable and precise anomaly detection models. The dependability of these models is greatly influenced by the caliber and uniformity of the input data, necessitating meticulous data cleansing as an essential step in the preprocessing phase.

3.2 Feature Engineering

The unprocessed data flowing from sensors and devices in the healthcare Internet of Things (IoT) is a cacophony, filled with potential insights regarding patient well-being and device reliability. However, unraveling these hidden meanings necessitates skillful feature engineering, a powerful process that converts into a coherent composition of practical insights. Within our proposed framework for real-time anomaly detection, this process assumes a crucial role in enhancing the capabilities of the HMM-SVM model to detect even the most subtle indication of an anomaly.

Our feature engineering strategy employs a dual approach, utilizing both statistical summaries and frequency domain features. By computing the mean, median, variance, and standard deviation, we can determine the central tendencies and dispersion of the data, thereby uncovering any potential deviations from the usual patterns. In addition, the use of minimum, maximum, and percentiles provides a more detailed representation of the distribution of the data, allowing for the identification of outliers and potential anomalies. These statistical summaries serve as the fundamental pulse of the data, providing essential understanding of its overall pattern.

However, our exploration does not come to an end at that point. In order to further explore the time-related patterns of the data, we examine the characteristics in the frequency domain. Through the utilization of techniques such as Fast Fourier Transforms (FFTs), we break down the data into its individual frequencies. This reveals concealed patterns and trends, such as oscillations that indicate specific physiological rhythms or fluctuations in sensor readings that could indicate device malfunctions. Through the examination of these features based on frequency, we enhance the detection of unusual occurrences that could otherwise go unnoticed in the original data.

Feature Type	Features
Statistical Summaries	Mean heart rate, Standard deviation of oxygen saturation
Frequency Domain Features	Dominant frequency of ECG signal, Variance of sensor readings in specific frequency bands

3.3 Segmentation

Segmentation is essential for real-time anomaly detection processing efficiency and accuracy. The process involves segmenting the uninterrupted flow of data into discrete segments, either by time intervals or significant events like medication administration or posture changes. A structured framework for real-time anomaly detection begins with segmentation.

Segmentation organizes data into manageable and contextually meaningful units for focused analysis and interpretation. Aligning segments with precise time intervals or events allows the anomaly detection model to detect and analyze deviations within these boundaries. This method simplifies real-time data processing and improves abnormal pattern detection, making it more responsive to section changes.

Segmentation is essential to anomaly detection. It simplifies raw data to identify irregular patterns and events. The initial phase must smoothly integrate subsequent anomaly detection methods to ensure the model works within the segmented data's temporal or event-specific boundaries.

Segmentation Strategy	**Example Segmentation Points**	**Benefit**
Time Windows	Every 5/15/30 seconds, every minute, or based on pre-determined intervals	Enables efficient real-time processing, reduces computational load
Meaningful Events	Medication administration, change in posture, device activation	Captures context-specific variations, improves anomaly detection for event-related issues

3.4 HMM-SVM Model Development

The HMM-SVM model is created by combining the Hidden Markov Model (HMM) and Support Vector Machine (SVM) to establish a robust framework for detecting anomalies.

Hidden Markov Model (HMM)

HMM is utilized to model the normal temporal sequence of feature values. Let X=$\{X_1, X_2 \ldots.X_T\}$ represent the observed sequence of features and Z=$\{Z_1, Z_2 \ldots.Z_T\}$ represent the corresponding hidden states. The parameters of the HMM include the initial state probabilities (π_i), state transition probabilities(a_{ij}) and emission probabilities ($b_i(x)$).

- **State initialization:**

Following eq.1 and 2 representing the probability of transition from state *i* and state *j*.

$\pi_i \geq 0, \sum_{i=1}^{N} \pi_i = 1$ (1)

$a_{ij} \geq 0, \sum_{i=1}^{N} a_{ij} = 1$ (2)

- **Emission Probabilities:**

Eq.3 represent the probability of observing feature *x* given that the system is in state *i*.

$(b_i(x)) \geq 0, \sum_{i=1}^{N} (b_i(x)) = 1$ (3)

- **Baum-Welch Algorithm**

The Baum-Welch algorithm is utilized to compute the parameters of the HMM, with the objective of maximizing the likelihood of the observed data. The algorithm employs the" expectation-maximization" (EM) procedure, which iteratively adjusts the parameters to better align with the observed data as represented in eq. 4 to 8.

○ **Expectation (E-Step)**

$$\gamma t(i) = P(Zt = i \mid X, \lambda)$$

$\gamma_t(i)$ = "probability of being in state *i* at time *t* given the observed sequence and the model parameters λ"

$$\xi_t(i,j) = P(Z_t = i, Z_{t+1} = j|X, \lambda)$$

$\xi_t(i,j)$ = "joint probability of being in state *i* at time *t* and transitioning to state *j* at time *t+1* given the observed sequence *X* and the model parameters λ"

○ **Maximization(M-step)**

$\pi'_i = \gamma_t(i)$ → updated initial state probability.

$a'_{ij} = \frac{\sum_{t=1}^{T-1} \xi_t(i,j)}{\sum_{t=1}^{T-1} \gamma t(i)}$ → updated state transition probability

Support Vector Machine (SVM)

SVM is trained for each hidden state of the HMM using feature extracted from segmented assigned to the state. Let X_{svm} represent the feature vectors and Y_{svm} represent the corresponding class labels.

- **Kernel Function: Radial Basis Function (RBF)**

RBF kernel is used to capture non-linear relationship in the data.

$K(x, y) = \exp\left(-\frac{||x-y^2||}{2\sigma^2}\right)$, where σ= "kernel width".

3.5 Real-time Anomaly Detection

Structured real-time anomaly detection includes segmentation, feature extraction, HMM inference, SVM classification, and alerting. Each data segment is immediately segmented for analysis. These segments are then used to derive relevant characteristics for modeling. The trained HMM and extracted features are used for HMM inference to find the segment's hidden state. It considers temporal dependencies. After training for the state, the SVM model classifies segments as normal or anomalous. Alert mechanisms notify healthcare personnel and prompt further investigation or intervention when anomalies are detected. This framework is efficient and mathematically robust. It uses HMM and SVM to detect anomalies in real time.

IV. RESULTS AND OUTPUTS

4.1 Evaluation Parameters

Table 1Evaluation parameters of various models

Metric	HMM-SVM	Naive Bayes	LSTM	Random Forest
Accuracy	98.66	90.20	97.50	94.80
Precision	97.10	88.50	96.30	93.40
Recall	96.20	85.70	98.10	92.20
F1-Score	96.70	87.10	97.20	92.80

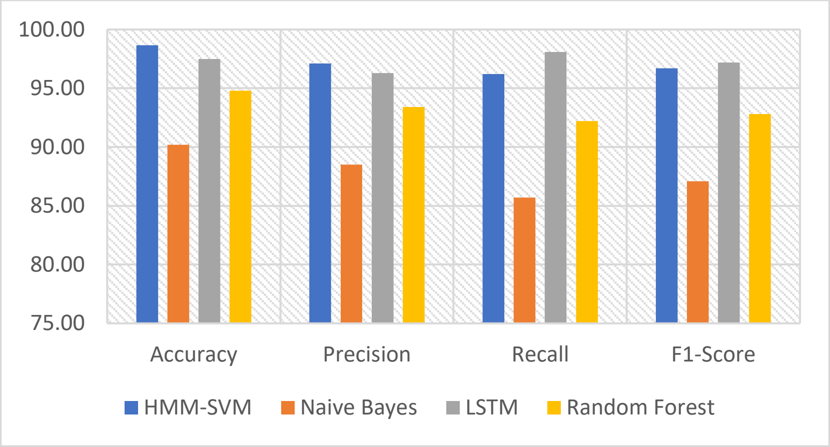

Figure 1 Comparison of various models

4.2 TPR, TNR

Table 2 Comparison of various parameters

Metric	HMM-SVM	Naive Bayes	LSTM	Random Forest
TPR	96.20	85.70	98.10	92.20
FPR	2.90	11.50	1.90	5.20
TNR	97.10	88.50	98.10	94.80
FNR	3.80	11.30	1.90	6.80

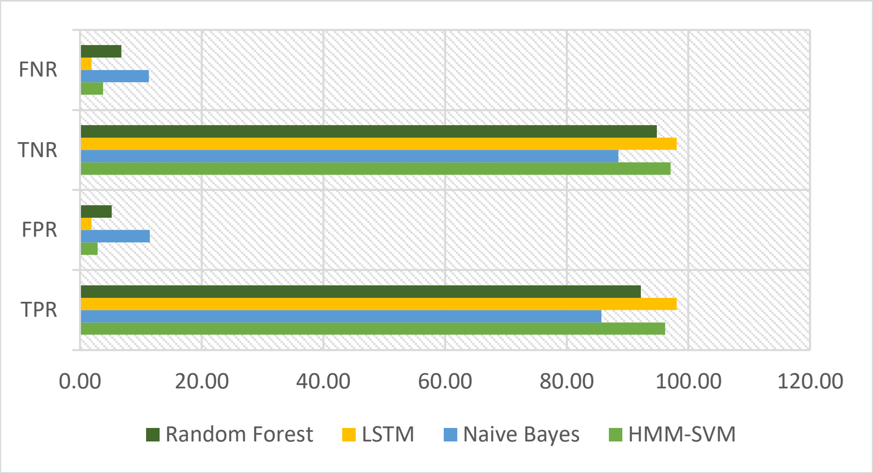

Figure 2 Comparison of TPR, FPR, TNR, FNR

The assessment of the machine learning-based security framework for detecting anomalies in real-time in Healthcare IoT demonstrates encouraging outcomes across diverse metrics represented in table-1,2 and figure-1,2. The evaluated models, specifically proposed hybrid Hidden Markov Model with Support Vector Machine (HMM-SVM), Naive Bayes, Long Short-Term Memory (LSTM), and Random Forest, were analyzed using various important performance metrics.

HMM-SVM exhibited superior performance in terms of overall accuracy, achieving a remarkable 98.66%, surpassing Naive Bayes (90.20%), LSTM (97.50%), and Random Forest (94.80%). The precision, which indicates the accuracy of correctly identifying true positives, achieved the highest value of 97.10% for the HMM-SVM model, followed by LSTM with 96.30%, Random Forest with 93.40%, and Naive Bayes with 88.50%.

The recall, which measures the models' ability to correctly identify all positive instances, was particularly high for LSTM at 98.10%, closely followed by HMM-SVM (96.20%), Random Forest (92.20%), and Naive Bayes (85.70%). The F1-Score, which takes into account both precision and recall, demonstrated a consistently balanced performance across all models. The HMM-SVM model achieved the highest score at 96.70%, followed by LSTM at 97.20%, Random Forest at 92.80%, and Naive Bayes at 87.10%.

The models' ability to differentiate between normal and anomalous instances was revealed through a more detailed examination using True Positive Rate (TPR) and False Positive Rate (FPR). The HMM-SVM model demonstrated a True Positive Rate (TPR) of 96.20% and a low False Positive Rate (FPR) of 2.90%, indicating its efficacy in accurately detecting anomalies while minimizing false alarms. The Naive Bayes model demonstrated a competitive True Positive Rate (TPR) of 85.70%, accompanied by a relatively higher False Positive Rate (FPR) of 11.50%. The LSTM and Random Forest models achieved impressive True Positive Rates (TPRs) of 98.10% and 92.20% respectively, along with False Positive Rates (FPRs) of 1.90% and 5.20% respectively.

The True Negative Rate (TNR) and False Negative Rate (FNR) highlight the models' ability to accurately classify normal instances and the instances that were incorrectly classified as normal, respectively. The HMM-SVM and LSTM models demonstrated impressive True Negative Rates (TNRs) of 97.10% and 98.10% respectively, while maintaining low False Negative Rates (FNRs) of 3.80% and 1.90%. The Naive Bayes and Random Forest models achieved True Negative Rates (TNRs) of 88.50% and 94.80% respectively, along with False Negative Rates (FNRs) of 11.30% and 6.80% respectively.

To summarize, the HMM-SVM model is a reliable option for detecting anomalies in real-time in Healthcare IoT. It demonstrates exceptional accuracy, precision, recall, and a well-balanced F1-Score. These findings highlight the effectiveness of machine learning in improving the security system of Healthcare IoT, enabling accurate and timely identification of abnormalities in real-life healthcare situations.

V. CONCLUSION AND FUTURE SCOPE

The research focuses on real-time anomaly detection in Healthcare IoT, recognizing the significant influence of Internet of Things (IoT) technologies in the healthcare industry. The incorporation of interconnected devices and systems has initiated a novel era of individualized and effective patient care. Nevertheless, the advent of this digital revolution necessitates the implementation of strong security protocols, specifically in relation to protecting patient information, guaranteeing the integrity of medical devices, and defending against potential cyber risks.

The importance of anomaly detection in healthcare IoT is extremely significant. Anomaly detection functions as a primary means of defense, detecting abnormal patterns or deviations from the standard that may indicate significant problems. The timeliness of anomaly detection is particularly critical in healthcare situations, where prompt intervention can be essential for ensuring patient safety and averting unfavorable results. The research demonstrates that the HMM-SVM hybrid model provides a unique solution to improve the precision and effectiveness of anomaly detection with accuracy of 98.66%. The hybrid approach combines the strengths of Hidden Markov Model (HMM) and Support Vector Machine (SVM) to overcome the limitations of current methods and contribute to the progress of Healthcare IoT security frameworks.

In the future, this research has potential applications beyond the current study. Firstly, one could explore additional refinement and optimization of the proposed HMM-SVM hybrid model to improve its scalability and adaptability in various healthcare IoT environments. Incorporating more sophisticated machine learning methods, such as deep learning architectures, could provide further understanding of intricate and evolving patterns in healthcare data.

Moreover, the study presents opportunities to investigate the integration of edge computing and federated learning methods to improve the ability to detect anomalies in real-time at the edge of the healthcare IoT network. Edge computing has the capability to decrease latency and enhance response times, which are crucial elements in healthcare situations that demand prompt action. Federated learning can enhance collaborative and privacy-preserving anomaly detection by utilizing knowledge from distributed IoT devices while safeguarding sensitive patient data.

This research acts as a foundation for strengthening the security framework of Healthcare IoT by implementing real-time anomaly detection. In order to navigate the changing healthcare and IoT environment, it is crucial to actively seek out new solutions and work together to overcome emerging obstacles. This collaborative approach is essential for establishing a secure and dependable future for interconnected healthcare systems. The pursuit of merging healthcare excellence and technological innovation is expected to be dynamic, promising, and abundant with opportunities for additional research, development, and positive influence on patient outcomes.

REFERENCES

[1] Z. Li, A. L. G. Rios, G. Xu, and L. Trajković, "Machine learning techniques for classifying network anomalies and intrusions," *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2019-May, 2019, doi: 10.1109/ISCAS.2019.8702583.

[2] R. Boutaba *et al.*, "A comprehensive survey on machine learning for networking: evolution, applications and research opportunities," *J. Internet Serv. Appl.*, vol. 9, no. 1, 2018, doi: 10.1186/s13174-018-0087-2.

[3] T. M. Ghazal *et al.*, "IoT for smart cities: Machine learning approaches in smart healthcare—A review," *Futur. Internet*, vol. 13, no. 8, 2021, doi: 10.3390/fi13080218.

[4] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, 2018, doi: 10.1186/s13677-018-0123-6.

[5] A. Chellam, L. Ramanathan, and S. Ramani, "Intrusion Detection in Computer Networks using Lazy Learning Algorithm," *Procedia Comput. Sci.*, vol. 132, pp. 928–936, 2018, doi: 10.1016/j.procs.2018.05.108.

[6] S. Agrebi and A. Larbi, *Use of artificial intelligence in infectious diseases*. Elsevier Inc., 2020.

[7] S. Bhattacharya and M. Pandey, "Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector," 2021, pp. 639–651.

[8] W. Li *et al.*, "A Comprehensive Survey on Machine Learning-Based Big Data Analytics for IoT-Enabled Smart Healthcare System," *Mob. Networks Appl.*, vol. 26, no. 1, pp. 234–252, 2021, doi: 10.1007/s11036-020-01700-6.

[9] M. M. Islam, A. Rahaman, and M. R. Islam, "Development of Smart Healthcare Monitoring System in IoT Environment," *SN Comput. Sci.*, vol. 1, no. 3, pp. 1–11, 2020, doi: 10.1007/s42979-020-00195-y.

[10] A. Mahmoudzadeh, I. Azimi, A. M. Rahmani, and P. Liljeberg, "Lightweight photoplethysmography quality assessment for real-time IoT-based health monitoring using unsupervised anomaly detection," *Procedia Comput. Sci.*, vol. 184, pp. 140–147, 2021, doi: 10.1016/j.procs.2021.03.025.

[11] N. Sehatbakhsh, M. Alam, A. Nazari, A. Zajic, and M. Prvulovic, "Syndrome: Spectral analysis for anomaly detection on medical IoT and embedded devices," *Proc. 2018 IEEE Int. Symp. Hardw. Oriented Secur. Trust. HOST 2018*, pp. 1–8, 2018, doi: 10.1109/HST.2018.8383884.

[12] A. M. Said, A. Yahyaoui, and T. Abdellatif, "Efficient anomaly detection for smart hospital iot systems," *Sensors (Switzerland)*, vol. 21, no. 4, pp. 1–24, 2021, doi: 10.3390/s21041026.

[13] S. A. Haque, M. Rahman, and S. M. Aziz, "Sensor anomaly detection in wireless sensor networks for healthcare," *Sensors (Switzerland)*, vol. 15, no. 4, pp. 8764–8786, 2015, doi: 10.3390/s150408764.

[14] A. Ukil, S. Bandyoapdhyay, C. Puri, and A. Pal, "IoT healthcare analytics: The importance of anomaly detection," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016-May, pp. 994–997, 2016, doi: 10.1109/AINA.2016.158.

[15] D. Gupta, O. Kayode, S. Bhatt, M. Gupta, and A. S. Tosun, "Hierarchical Federated Learning based Anomaly Detection using Digital Twins for Smart Healthcare," *Proc. - 2021 IEEE 7th Int. Conf. Collab. Internet Comput. CIC 2021*, no. Cic, pp. 16–25, 2021, doi: 10.1109/CIC52973.2021.00013.

[16] H.-C. Huang, I.-H. Liu, M.-H. Lee, and J.-S. Li, "Anomaly Detection on Network Traffic for the Healthcare Internet of Things," p. 3, 2023, doi: 10.3390/engproc2023055003.

[17] D. Oladimeji, "an Intrusion Detection System for Internet of," no. June, pp. 1–25, 2021.

[18] A. A. Cook, G. Misirli, and Z. Fan, "Anomaly Detection for IoT Time-Series Data: A Survey," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6481–6494, 2020, doi: 10.1109/JIOT.2019.2958185.

[19] M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.

[20] G. Sivapalan, K. K. Nundy, S. Dev, B. Cardiff, and D. John, "ANNet: A Lightweight Neural Network for ECG Anomaly Detection in IoT Edge Sensors," *IEEE Trans. Biomed. Circuits Syst.*, vol. 16, no. 1, pp. 24–35, 2022, doi: 10.1109/TBCAS.2021.3137646.

[21] X. Wu, Y. Yang, M. Bilal, L. Qi, and X. Xu, "6G-Enabled Anomaly Detection for Metaverse Healthcare Analytics in Internet of Things," *IEEE J. Biomed. Heal. Informatics*, vol. XX, no. Xx, pp. 1–10, 2023, doi: 10.1109/JBHI.2023.3298092.

[22] C. Kavitha, V. Mani, S. R. Srividhya, O. I. Khalaf, and C. A. Tavera Romero, "Early-Stage Alzheimer's Disease Prediction Using Machine Learning Models," *Front. Public Heal.*, vol. 10, no. March, pp. 1–13, 2022, doi: 10.3389/fpubh.2022.853294.

[23] Khetani, V. ., Gandhi, Y. ., Bhattacharya, S. ., Ajani, S. N. ., & Limkar, S. . (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253–262.

[24] Sable, N. P., Rathod, V. U., Salunke, M. D., Jadhav, H. B., Tambe, R. S., & Kothavle, S. R. (2023). Enhancing Routing Performance in Software-Defined Wireless Sensor Networks through Reinforcement Learning. International Journal of Intelligent Systems and Applications in Engineering, 11(10s), 73-83.

[25] Sairise, Raju M., Limkar, Suresh, Deokate, Sarika T., Shirkande, Shrinivas T. , Mahajan, Rupali Atul & Kumar, Anil(2023) Secure group key agreement protocol with elliptic curve secret sharing for authentication in distributed environments, Journal of Discrete Mathematical Sciences and Cryptography, 26:5, 1569–1583, DOI: 10.47974/JDMSC-1825