PROJECT ON

INFORMATION SECURITY MANAGEMENT

J-COMPONENT PROJECT REVIEW

FINAL REVIEW

ON

SECURITY IN IOMT USING FEDERATED LEARNING

UNDER THE GUIDANCE OF

DR. SUMAIYA THASEEN I

FACULTY, VIT UNIVERSITY, VELLORE.

SUBMITTED BY

RITHIKA A – 20MIS0018

LITHIKAA B- 20MIS0061

VIGNESH M - 20MIS0175

SADHANA S - 20MIS0185

SEMESTER

WINTER – 2023~2024

PROGRAMME

M.TECH (Integrated) SOFTWARE ENGINEERING

SCHOOL

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS (SCORE)

COURSE CODE

CSE 3502

SLOT

F2

TABLE OF CONTENTS

1. ABSTRACT:

This project investigates the application of deep learning models for predicting the next heartbeat in electrocardiogram (ECG) signals. We explore the effectiveness of two prominent architectures: Convolutional Neural Networks (CNNs) + Long Short-Term Memory (LSTM) networks and convlstm. We examine a combined ConvLSTM model that leverages the strengths of both CNNs and LSTMs. The models are trained and evaluated using data from the publicly available ECG5000 dataset. By comparing the performance of these models, we aim to identify the most effective approach for predicting the next heartbeat in ECG data. This project has the potential to contribute to advancements in real-time cardiac health monitoring and arrhythmia detection.

Keywords: *ECG signal detection, Deep learning, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Convolutional LSTM (ConvLSTM), Time series analysis.*

2. INTRODUCTION:

Electrocardiograms (ECGs) are a vital diagnostic tool used to assess heart health by recording the electrical activity of the heart. Accurately predicting the next heartbeat in an ECG signal holds significant potential for advancements in cardiac care [2]. This project investigates the application of deep learning models for this purpose.

We focus on two prominent architectures: Convolutional Neural Networks (CNNs) + Long Short-Term Memory (LSTM) networks, and Convolutional LSTM (ConvLSTM) networks. The ECG5000 dataset serves as the foundation for this study. This dataset comprises a 20-hour-long ECG recording from a patient diagnosed with a cardiac condition [5]. The rich temporal information within this data offers a valuable resource for training and evaluating our models [1].

CNNs excel at capturing spatial features within data, making them suitable for identifying patterns in the ECG signal itself. LSTMs, on the other hand, specialize in learning long-term dependencies between sequential data points [3]. This capability is crucial for understanding the relationships between consecutive heartbeats. ConvLSTMs, by combining convolutional and LSTM layers, aim to leverage the strengths of both approaches, extracting spatial features while effectively modeling the sequential nature of the ECG signal [9].

By comparing the performance of these models in predicting the next heartbeat, this project seeks to identify the most effective and efficient approach for ECG signal prediction [7].

This advancement has the potential to revolutionize various aspects of cardiac care. Applications include:

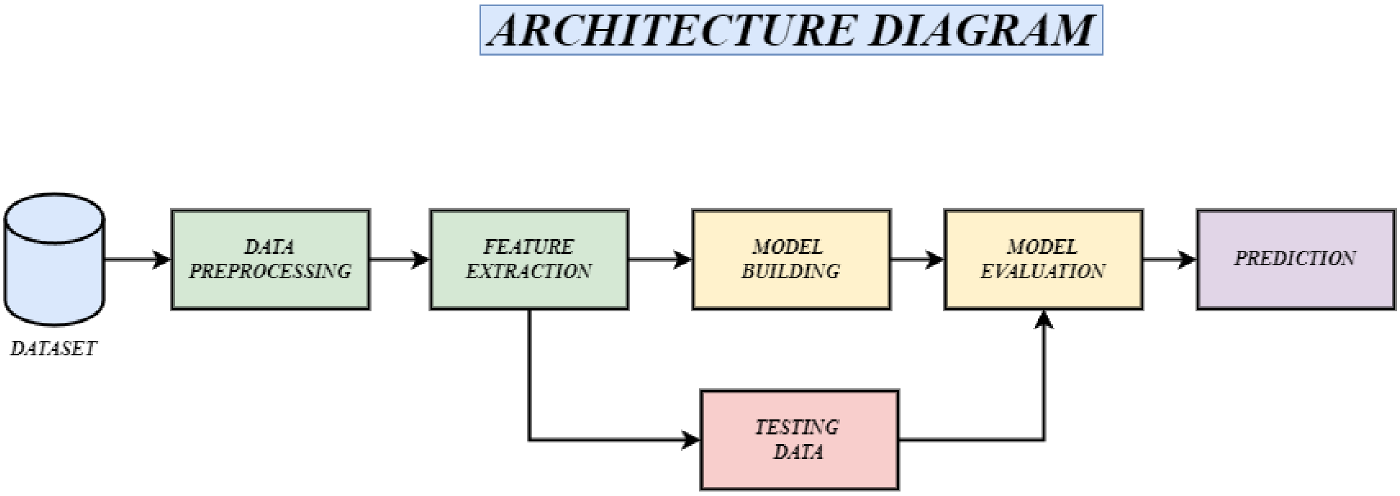
- **Arrhythmia Detection:** Early and accurate detection of abnormal heart rhythms can be crucial for timely intervention and improved patient outcomes [11].
- **Cardiac Health Monitoring:** Real-time monitoring of predicted heartbeats could enable continuous assessment of a patient's cardiac health, potentially leading to earlier diagnosis and treatment of heart conditions [4].

- **Improved Diagnostic Tools:** Integrating heartbeat prediction into existing diagnostic tools could enhance their accuracy and efficiency [10].

This project could pave the way for the development of novel ECG-based applications that significantly contribute to improved cardiac health monitoring and diagnosis.

3. PROPOSED METHODOLOGY:

3.1.ARCHITECTURE DIAGRAM:



3.2. ARCHITECTURE EXPLANATION:

This project aims to develop a system for ECG signal detection using a combination of deep learning architectures: Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and Convolutional LSTMs (ConvLSTMs). Here's a breakdown of the proposed methodology:

3.2.1. DATA ACQUISITION AND PREPROCESSING:

- Collect ECG signal data from a reliable source. This could be a standard ECG dataset or real-time recordings from patients.
- Preprocess the ECG signals to ensure consistency and remove noise. This may involve filtering, normalization, and segmentation into appropriate lengths for analysis.

3.2.2. FEATURE EXTRACTION:

- ***CNN LAYERS:*** Utilize CNN layers to extract spatial features from the ECG signals. These features could represent specific ECG wave components (P, Q, R, S, T) or patterns within the signal.

  Employ convolutional operations with different kernel sizes to capture features at various granularities.Use pooling layers for dimensionality reduction and capturing dominant features.

- ***LSTM OR CONVLSTM LAYERS:***
  - ***LSTM:*** After feature extraction by CNN, an LSTM layer can be introduced to capture the temporal dependencies within the ECG sequence. This is crucial for understanding the relationships between different ECG components and identifying patterns over time.
  - ***CONVLSTM:*** Alternatively, a ConvLSTM layer can be used. ConvLSTMs combine the strengths of CNNs and LSTMs, enabling them to learn spatiotemporal features directly from the ECG data. This can be particularly beneficial for capturing the evolving characteristics of ECG signals.

3.2.3. MODEL TRAINING:

- Divide the preprocessed ECG data into training, validation, and testing sets.
- Train the CNN-LSTM or ConvLSTM model on the training data. The model will learn to associate specific features and temporal patterns with different ECG signal categories (e.g., normal vs. abnormal).
- Use the validation set to monitor the model's performance and prevent overfitting. Adjust hyperparameters (learning rate, number of layers, etc.) based on validation results.

3.2.4. MODEL EVALUATION:

- Evaluate the trained model's performance on the unseen testing data. Metrics like accuracy, precision, recall, and F1-score can be used to assess the model's ability to detect ECG signals accurately.

3.2.5. OPTIMIZATION:

- Based on the evaluation results, further refine the model architecture or training process to improve performance.
- To achieve optimal performance, the models will be trained with a large dataset for multiple epochs, with batch size being another hyperparameter to consider. Finally, a comprehensive analysis will be conducted to identify the model that achieves the best detection accuracy on unseen testing data.

3.3. CNN+LSTM MODEL EXPLANATION:

The CNN-LSTM combination offers a powerful approach for ECG signal prediction and various time series analysis tasks. Its ability to capture both spatial and temporal features makes it a valuable tool for applications requiring accurate prediction from sequence data.

3.3.1. ADVANTAGES:

- **Feature Extraction and Temporal Learning:** CNNs excel at extracting spatial features from the ECG signal, identifying crucial wave components like the PQRST complex. LSTMs, on the other hand, are adept at capturing temporal dependencies within the signal, learning the sequential patterns over time.
- **Sequential Data Handling:** ECG signals are inherently sequential, with information unfolding over time. LSTMs are specifically designed to handle such sequential data, effectively leveraging past information to predict future events. This makes them ideal for tasks like arrhythmia detection or beat classification in ECG analysis.

3.3.2. SUITABILITY FOR ECG PREDICTION:

- **ECG's Complex Nature:** ECG signals contain rich information encoded in both the wave shapes (spatial features) and their temporal relationships. The CNN-LSTM combination effectively addresses this complexity by capturing both aspects.
- **Accurate Prediction:** By understanding both spatial and temporal characteristics, the model can learn subtle variations that might indicate abnormalities or predict future signal patterns, leading to more accurate predictions in ECG analysis.

3.3.3. APPLICATIONS:

- **Time Series Forecasting:** This approach is beneficial for various time series forecasting tasks beyond ECG. It can be applied to areas like stock market prediction, weather forecasting, or even traffic flow analysis, where understanding both the underlying patterns and temporal trends is crucial.
- **Video Analysis:** In video analysis tasks like action recognition or anomaly detection, CNNs can identify objects and their movements (spatial features), while LSTMs can capture the flow of actions over time. This combination is valuable for various video analysis applications.

3.3.4. DISADVANTAGES:

- **Computational Cost:** Training CNN-LSTM models can be computationally expensive due to the large number of parameters involved. This might necessitate powerful GPUs or specialized hardware.

3.4. CONVLSTM MODEL EXPLANATION:

The ConvLSTM model offers a unique approach that combines the strengths of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) into a single architecture. This makes it particularly suitable for tasks like ECG signal prediction, where understanding both spatial and temporal information is crucial.

3.4.1. WHY CONVLSTM WORKS FOR ECG PREDICTION:

- **Single Model, Dual Power:** ConvLSTMs eliminate the need for separate CNN and LSTM blocks. They leverage convolutions to extract spatial features directly within the LSTM framework. This allows the model to learn the relationship between nearby data points while also capturing the sequence information within the ECG signal.
- **Focus on Local Patterns:** ConvLSTMs can inherently focus on local patterns in the ECG signal due to the convolutional nature. This is important for identifying specific characteristics like the PQRST complex.

3.4.2. ADVANTAGES OF CONVLSTMS:

- **Efficiency:** ConvLSTMs can be more efficient than separate CNN-LSTM models as they combine feature extraction and temporal learning into a single step. This can potentially reduce training time and computational resources.
- **Direct Feature-Sequence Learning:** The model can directly learn how spatial features evolve over time within the ECG sequence, leading to potentially more robust predictions.

3.4.3. OTHER APPLICATIONS:

- **Video analysis:** Analyzing video sequences for object detection, activity recognition, or anomaly detection.
- **Sensor data analysis:** Processing data from sensors in autonomous vehicles, robotics, or environmental monitoring to understand spatial patterns and their temporal changes.
- **Sign language translation:** Analyzing the spatial configuration of hands and their movement over time for accurate sign language understanding.

3.4.4. DISADVANTAGES:

- **Complexity Tuning:** While efficient, ConvLSTMs can be more complex to design and tune compared to separate CNN-LSTM models. Finding the optimal hyperparameters for the convolutional and LSTM aspects might require additional effort.
- **Limited Research:** ConvLSTMs are a relatively new architecture compared to separate CNN-LSTM models. There might be less research and established best practices for specific tasks compared to the more traditional approach.

4. BACKGROUND (LITERATURE REVIEW):

NAME: *RITHIKA A* ***REGISTER NUMBER:*** *20MIS0018*

1. **XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks**

This study introduces a new security model for IoMT networks that uses bidirectional SRU units and skip connections. The model can identify various cyber threats, including data poisoning, injection attacks, and denial-of-service attacks, that target IoMT-powered smart health systems (SHSs). To improve trust management, the authors use explainable AI (XAI) techniques to help humans, security professionals, and administrators understand the model's reasoning and evidence behind its decisions. Compared to existing methods, the proposed model effectively detects cyber threats with high accuracy. The paper also provides background information on the IoMT ecosystem and existing research on attack detection in IoMT systems. Finally, this method is unique because it offers a reliable AI solution for healthcare systems, allowing security experts and network personnel to make informed decisions and take timely actions when cyber threats are detected.

2. **Recurrent Neural Network Model for IoT and Networking Malware Threat Detection**

This paper proposes a novel approach for detecting malware threats in IoT networks using an optimized deep learning architecture. The core of the system is an LSTM-based RNN model that can analyse various forms of network data and continuously adapt to identify new emerging threats. The authors highlight the significance of intelligent threat detection mechanisms and acknowledge the limitations of their proposed system. They suggest integrating the RNN-LSTM classifier with the NAdam optimization algorithm to enhance network security for Android devices. Additionally, the system employs a swarm intelligence-based prioritization scheme to prioritize incoming data based on its relevance. The paper concludes by emphasizing the proposed system's exceptional efficiency, requiring minimal computing power and energy resources.

3. **Federated Learning Driven Secure Internet of Medical Things**

This paper introduces a framework called FLDIoMT that combines federated learning with the Internet of Medical Things (IoMT)**.** This system aims to provide a flexible and privacy-preserving platform for deploying various medical applications. The paper showcases how different technologies can be integrated within IoMT solutions for diverse healthcare needs. Additionally, a practical example is presented through iSmile, a mobile application for sleep monitoring developed using FLDIoMT. Experimental results validate the effectiveness and feasibility of the proposed approach. The paper concludes by discussing the challenges associated with large-scale deployment of federated learning and outlines potential future directions for research.

4. 6G-Enabled IoT Home Environment Control Using Fuzzy Rules

This paper proposes a smart home system utilizing 6G communication to deliver enhanced comfort, security, and protection for residents. The system leverages fuzzy logic rules to monitor various home parameters and trigger appropriate actions in response to potential threats or discomfort. Designed for the next generation of IoT based on 6G networks, the system prioritizes the number of occupants present and requires user login through smartphones for control. It employs various modules to safeguard against wind intrusion, water leaks, and rising CO2 levels. Furthermore, the infrastructure is adaptable to future 6G communication standards, enabling faster data exchange within the home network and with external devices.

NAME: *LITHIKAA B* ***REGISTER NUMBER:*** *20MIS0061*

1. Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey

This comprehensive survey delves into Federated Learning (FL) as a method for safeguarding privacy in smart healthcare systems. It explores the security and privacy challenges within the Internet of Medical Things (IoMT) and elucidates the rationale and structure of FL within IoMT networks. The article also delineates advanced FL architectures with a focus on privacy, alongside discussing FL applications. It underscores the significance of preserving end-user privacy in contemporary electronic healthcare systems and the imperative of addressing cybersecurity concerns within healthcare. Additionally, the piece examines various standard protocols devised to mitigate privacy risks and outlines three types of secure access methods users can employ. Overall, it underscores the necessity of securing networks with a privacy-centric approach and the criticality of safeguarding user identities and information.

2. Industrial Internet of Things: Challenges, Opportunities, and Directions

The content delves into the hurdles and prospects associated with the Industrial Internet of Things (IIoT). IIoT aims to facilitate data sharing and interoperability among closed subsystems and applications within and across industries. Communication protocols in IIoT need to support efficient, timely, and widespread information aggregation and availability. Standardization plays a vital role in the viability of IIoT, with security and privacy emerging as major concerns. IIoT underscores the integration and interconnection of previously isolated plants, working islands, or machineries. Messaging solutions ensure scalability, with Message Queue Telemetry Transport being the predominant messaging protocol. Privacy in IIoT entails a threefold guarantee: awareness of privacy risks, individual control over information collection and processing, and awareness and control over subsequent use and dissemination to external entities. When designing a secure IIoT infrastructure, key security properties to consider include tamper resistance, encrypted storage, secured communication networks, and efficient identification and authentication mechanisms.

3. A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks

This research paper presents a novel framework designed to detect cyber threats within Industrial Internet of Things (IIoT) networks. It underscores the critical need for robust security solutions in IIoT-based Industrial Control and Supervisory Systems (IICSs), given the potential devastation that cyberattacks can inflict on essential infrastructure. The proposed framework amalgamates Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models to extract pertinent high-level information, thus offering insight into prediction decisions. The paper also explores prior research on Recurrent Neural Networks (RNNs) and CNNs, elucidating the theoretical underpinnings of CNNs. Moreover, it introduces the application of a method known as LIME to interpret prediction decisions and the underlying data evidence. Additionally, the paper delves into the significance of Time Series Data Mining (TSDM) and the challenges associated with mining high-dimensional time-series data. Overall, it puts forth a new, interpretable deep learning framework tailored for uncovering cyber threats in IIoT networks, aiding security administrators in comprehending the causal reasoning behind prediction decisions and the associated data evidence.

4. (ReLBT): A Reinforcement learning-enabled listen before talk mechanism for LTE-LAA and Wi-Fi coexistence in IoT

This research paper focuses on the coexistence of LTE-LAA and Wi-Fi in wireless communication systems. It introduces a novel mechanism that employs reinforcement learning to dynamically adjust channel access parameters, thereby mitigating channel collisions and promoting fairer access to the channel. The proposed approach entails minimal modifications to existing Listen-Before-Talk (LBT) technologies, offering a practical and efficient solution. The paper delves into the complexities arising from the diverse physical layer and medium access control (MAC) layer configurations of LTE-LAA and Wi-Fi, which pose challenges for effective coexistence. By aiming to optimize the performance of wireless User Equipment (UE) within LTE-LAA environments, the proposed mechanism seeks to enhance overall system efficiency and user experience.

NAME: *VIGNESH M* ***REGISTER NUMBER:*** *20MIS0175*

1. ***Feature data processing: Making medical data fit deep neural networks***

The paper proposes a systematic method of feature data processing to make it more suitable for deep neural network (DNN) training. The proposed approach can use fewer training data and a simpler model architecture achieves better performance compared with other existing methods. The paper discusses some problems faced during the experiment, such as serious over-fitting and insufficient generalization ability. To address these issues, the paper proposes further optimization of the model architecture to reduce training time and improve the robustness of the model. The paper also provides some specific suggestions on how to choose an appropriate DNN model architecture. The proposed FDPS is optimal for DNN-based feature data analysis, and can greatly expand the application field of deep learning.

2. ***Feature data processing: Making medical data fit deep neural networks***

The paper proposes a systematic method of feature data processing to make it more suitable for deep neural network (DNN) training. The proposed approach can use fewer training data and a simpler model architecture achieves better performance compared with other existing methods. The paper discusses some problems faced during the experiment, such as serious over-fitting and insufficient generalization ability. To address these issues, the paper proposes further optimization of the model architecture to reduce training time and improve the robustness of the model. The paper also provides some specific suggestions on how to choose an appropriate DNN model architecture. The proposed FDPS is optimal for DNN-based feature data analysis, and can greatly expand the application field of deep learning.

3. ***Federated machine learning for detection of skin diseases and enhancement of internet of medical things (IoMT) security***

The paper titled "Decentralized Datasets" discusses the use of federated learning to address the problems of data privacy and data distribution in skin disease detection and classification. The paper proposes a novel CNN model and employs a hyper-parameter tuning technique to optimize the parameters. The proposed model is compared with different CNN benchmark algorithms. The paper also explores the use of federated learning to enhance the security of medical imaging using a custom dataset. The proposed work is expected to assist dermatologists in correctly detecting skin diseases in a short period of time while ensuring data security.

4. *Fedhealth: A federated transfer learning framework for wearable healthcare*

This paper discusses the use of decision trees in ensemble learning to create lightweight models that can be deployed on computation-restricted wearable devices. The authors use a public human activity recognition dataset called UCI Smartphone to construct the problem situation in FedHealth, where they extract five subjects and regard them as isolated users who cannot share data due to privacy concerns. The paper also evaluates the classification accuracy and macro F1 score on the collected dataset and presents a detailed discussion of the potential of FedHealth from specific technical improvements to healthcare applications. The authors plan to extend FedHealth with incremental learning to achieve more personalized and flexible healthcare. The paper also includes references to related works in the field of wearable healthcare and transfer learning methods.

NAME: *SADHANA S* ***REGISTER NUMBER:*** *20MIS0185*

1. A Federated Reinforcement Learning Framework for Incumbent Technologies in Beyond 5G Networks

The paper titled "Federated Reinforcement Learning Framework for WiFi Channel Resource Allocation in 5G/B5G Networks" proposes a framework for optimizing WiFi performance in terms of throughput by collaborative channel access parameter selection. The study also discusses six potential applications for the proposed framework in incumbent technologies in 5G/B5G networks. The proposed framework uses reinforcement learning (RL) to train the model using cooperation and feedback, where several learners perceive and interpret their environment, take actions, and interact with it. The proposed mechanism optimizes contention parameters based on observed collision probability, which was iteratively optimized using the QL algorithm. The paper encourages researchers from institutions and industry to consider the proposed FRL model for potential research and practical applications.

2. On the Physical Layer Security of Federated Learning Based IoMT Networks

This is describing the challenges of transmitting big health-related data in a reliable and secure manner. The paper proposes the use of federated learning (FL) as a promising technique that uses a distributed and collaborative approach of data sharing and learning. FL reduces the amount of shared data, and only important model parameters are shared, thus preserving data privacy. The paper also discusses security issues in FL-based smart healthcare systems and proposes physical layer security (PLS) techniques to improve the security of the links. The paper concludes by presenting numerical results to compare the secrecy performance of a fully centralized and hierarchical setup of the residential area.

3. Multi-level feature fusion for multimodal human activity recognition in Internet of Healthcare Things

This paper proposes a multi-level feature fusion approach for multimodal human activity recognition (HAR) that efficiently processes and recognizes human activities recorded by multiple sensors and stationary cameras embedded in a variety of Internet of Things (IoT) devices. The proposed system enhances the efficiency of multimodal HAR for smart healthcare applications by exploiting ConvLSTM capabilities to model long-term temporal representation from raw multi-sensory information and using multi-head CNN with CBAM to effectively retrieve channel and spatial dimension features from visual information. The extensive experimental findings demonstrated the efficiency and practicability of the proposed fusion architecture compared with two baseline models and state-of-the-art frameworks.

4. A Stable AI-Based Binary and Multiple Class Heart Disease Prediction Model for IoMT

This paper proposes a Bagging-Fuzzy-GBDT approach for heart disease prediction and diagnosis in the Internet of Medical Things (IoMT). The proposed approach achieved binary and multiple classification prediction of heart disease. The authors introduced the fuzzy logic and bagging algorithm into the GBDT algorithm to reduce the complexity of data and avoid overfitting. The stability of the model was greatly improved after the parameters were determined by the grid search. The evaluation results showed that the proposed model achieves good performance in terms of accuracy, stability, AUC, and other indicators compared with other traditional algorithms. The paper also presents related work, system architecture, and details of the proposed algorithm.

5. *EXPERIMENTAL ANALYSIS:*

5.1. DATASET DESCRIPTION:

The dataset for this project is ECG5000 which consists of a 20-hour-long electrocardiogram (ECG) signal containing 5,000 individual heartbeat records. Each record has 140 data points. This data originates from the BIDMC Congestive Heart Failure Database (chfdb) on Physionet, as described in the paper "A general framework for never-ending learning from time series streams" (DAMI 29(6)).

5.2. DATA PREPROCESSING:

- **Reshaping:** The data has 5000 rows and 140 columns. This data likely represents multiple features extracted from each heartbeat. In preprocessing, you might reshape this data into a single column of 700,000 entries (5000 rows * 140 columns). This essentially stacks all the features from each heartbeat signal one after another.
- **Min-Max Normalization:** After reshaping, you apply min-max normalization. This scales each heartbeat signal (represented by its features in the reshaped data) to a specific range, typically between 0 and 1. This ensures all signals have a consistent scale regardless of the patient's original heart activity levels. By normalizing, the models focus on learning the underlying patterns in the signal itself, not just its magnitude, which can improve model performance.

5.3. FEATURE EXTRACTION (SLIDING WINDOW APPROACH):

To capture the temporal dynamics of the ECG signal for heartbeat prediction, we employ a sliding window approach during feature extraction. This method involves segmenting the continuous ECG data into smaller, fixed-length windows.

In our project, we set the window size to 60 data points. This window size represents a specific time interval of the ECG signal, potentially capturing a single or multiple heartbeats. By sliding this window one data point at a time across the entire ECG recording, we obtain multiple segments, each containing a short sequence of the ECG signal.

These segments serve as the input features for our deep learning models. This approach allows the models to learn the patterns within these short ECG sequences, ultimately aiding in predicting the next heartbeat.

5.4. MODEL 1 - ConvLSTM:

5.4.1. MODEL DESCRIPTION:

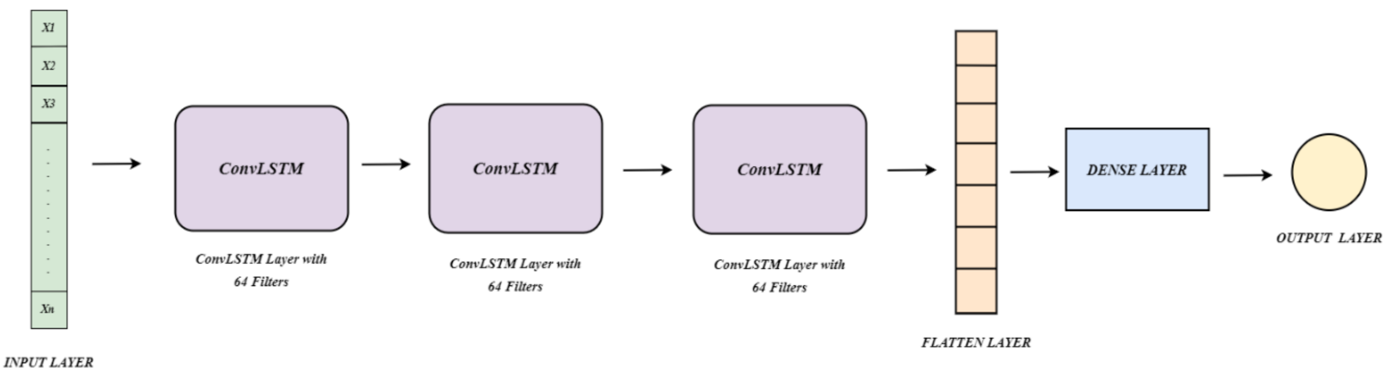
ConvLSTM combines the strengths of Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTMs) networks, making it particularly suitable for 1D data time series forecasting like ECG signals.

CNNs within the ConvLSTM can identify spatial patterns within each heartbeat segment (the 60 data point window), effectively capturing the unique characteristics of a heartbeat. LSTMs excel at modeling sequential relationships, allowing the ConvLSTM to learn the dependencies between consecutive heartbeats within the ECG signal.

This combined ability makes ConvLSTMs adept at understanding both the individual characteristics of a heartbeat and the flow of information throughout the entire ECG recording, ultimately improving the accuracy of heartbeat prediction.

5.4.2. MODEL ARCHITECTURE DIAGRAM:

ARCHITECTURE DIAGRAM - ConvLSTM



5.4.3. PARAMETERS USED:

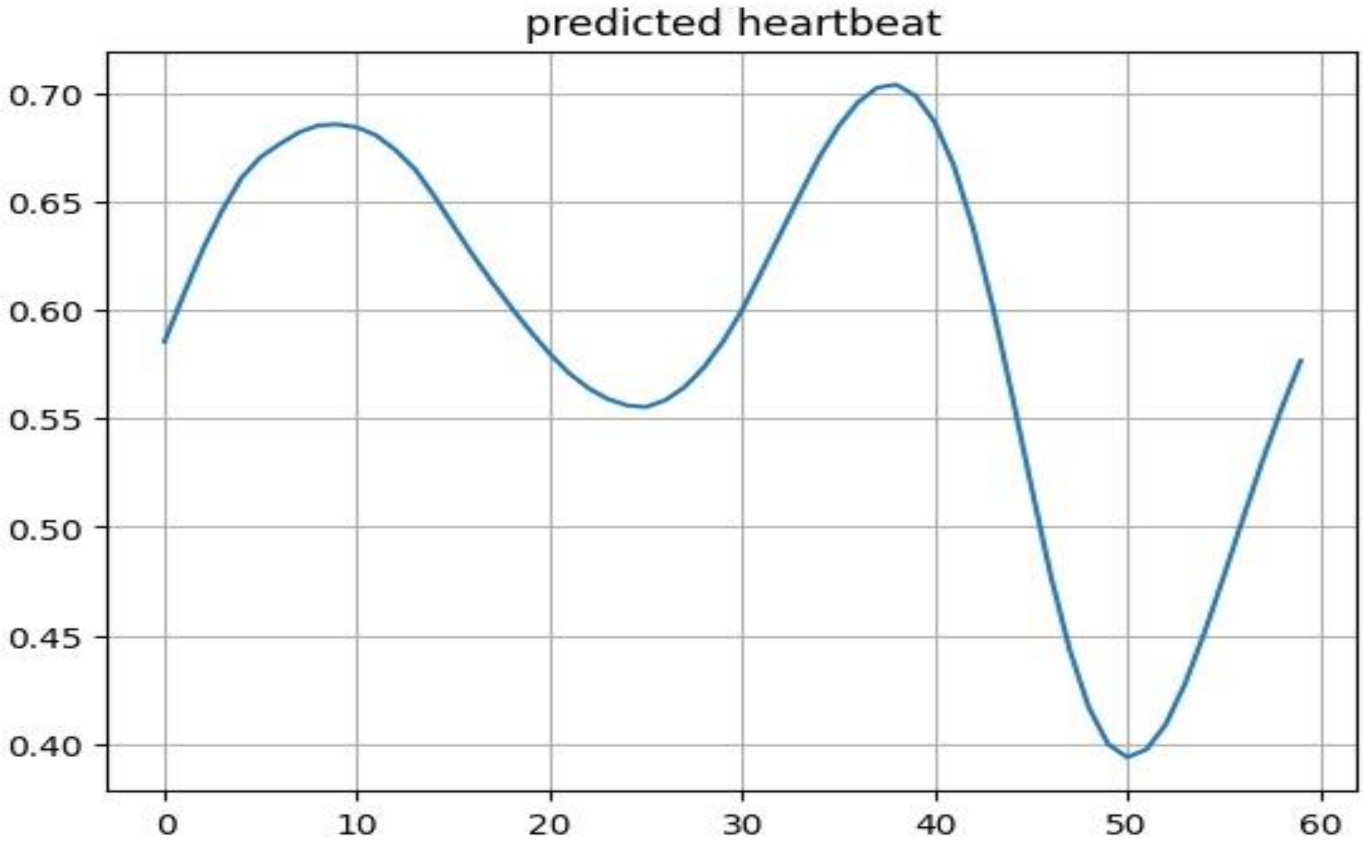
Our ConvLSTM model utilizes three convolutional LSTM layers, each containing 64 filters. The model expects input data in the format (1, 60, 1). This signifies:

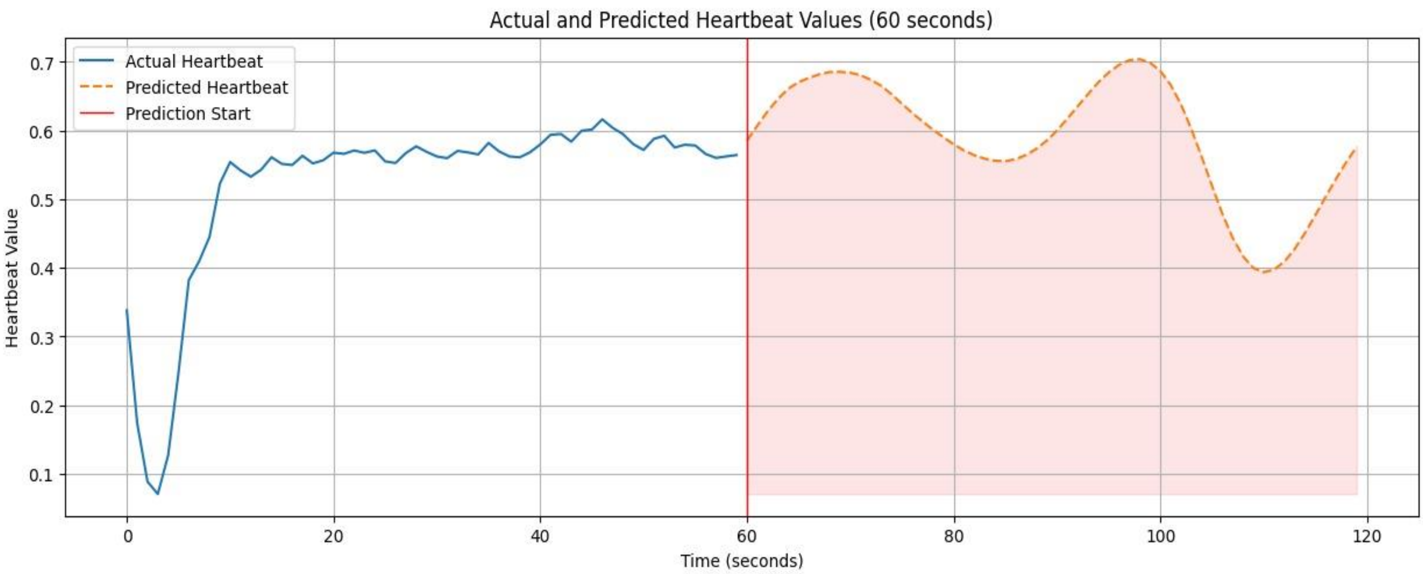
- 1: There's one feature channel, representing the ECG signal itself.
- 60: The window size is 60 data points, capturing a segment of the ECG signal.
- 1: There's only one channel of data, as ECG signals are typically single-channel recordings.
- For training, we leverage the first 10,000 data points from the dataset, which translates to roughly an hour of ECG data. This data is then split, with 80% designated for training the

model and 20% reserved for testing its performance on unseen data. The training process itself involves 15 epochs, where the model iterates through the training data 15 times, and 8 batches, which dictate how many data points are processed at once during training.

5.4.4. PREDICTION:

For prediction, the model utilizes the last 60 seconds of ECG data as input. This data is reshaped to match the model's expected format (likely one channel for the ECG signal and a window size of 60 data points). The model then predicts the next 60 seconds of heartbeat values. These predicted values can be visualized by plotting them on a graph, allowing for an analysis of the model's forecasted heartbeat pattern compared to the actual ECG signal.





5.4.5. MODEL EVALUATION:

The ConvLSTM model's performance was evaluated using several metrics:

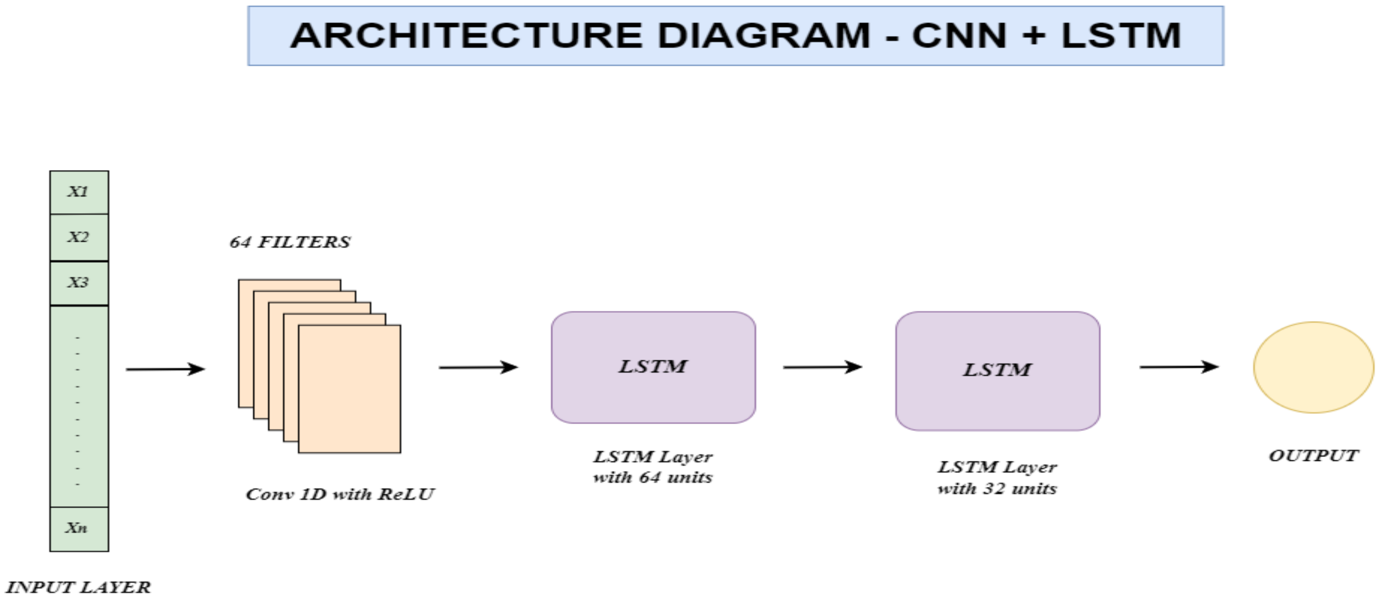
- ***Mean Squared Error (MSE):*** 0.00140 - This indicates a very low average squared difference between the predicted and actual heartbeat values.
- ***Mean Absolute Error (MAE):*** 0.01709 - This signifies an average absolute difference of 0.017 between predicted and actual heartbeats, which is a small error in real-world ECG units.
- ***Root Mean Squared Error (RMSE):*** 0.03741 - This is the square root of MSE, providing a measure of error in the same units as the original data (heartbeat values). A value of 0.037 suggests a small typical error.
- ***R-squared (R^2):*** 0.88181 - This represents 88.18% of the variance in the actual heartbeat data being explained by the model's predictions. This indicates a good fit between the model and the data.
- ***Mean Absolute Percentage Error (MAPE):*** 27.911% - This reflects an average absolute percentage error of 27.9% between predicted and actual heartbeats. While higher than the other metrics, MAPE can be sensitive to outliers in heartbeat values, so a lower emphasis might be placed on it in this context.

5.5. MODEL 2 – CNN + LSTM:

5.5.1. MODEL DESCRIPTION:

The model is composed of a single Conv1D layer followed by two LSTM layers. The Conv1D layer comprises 64 filters, while the first LSTM layer contains 64 units and the second LSTM layer contains 32 units.

5.5.2. MODEL ARCHITECTURE DIAGRAM:



5.5.3. PARAMETERS USED:

The input format accepted by the model is (60, 1). In this format, "60" indicates that each segment of the ECG signal contains 60 data points. The final "1" signifies that only one channel of data is provided as input, indicating that ECG signals are single-channel recordings.

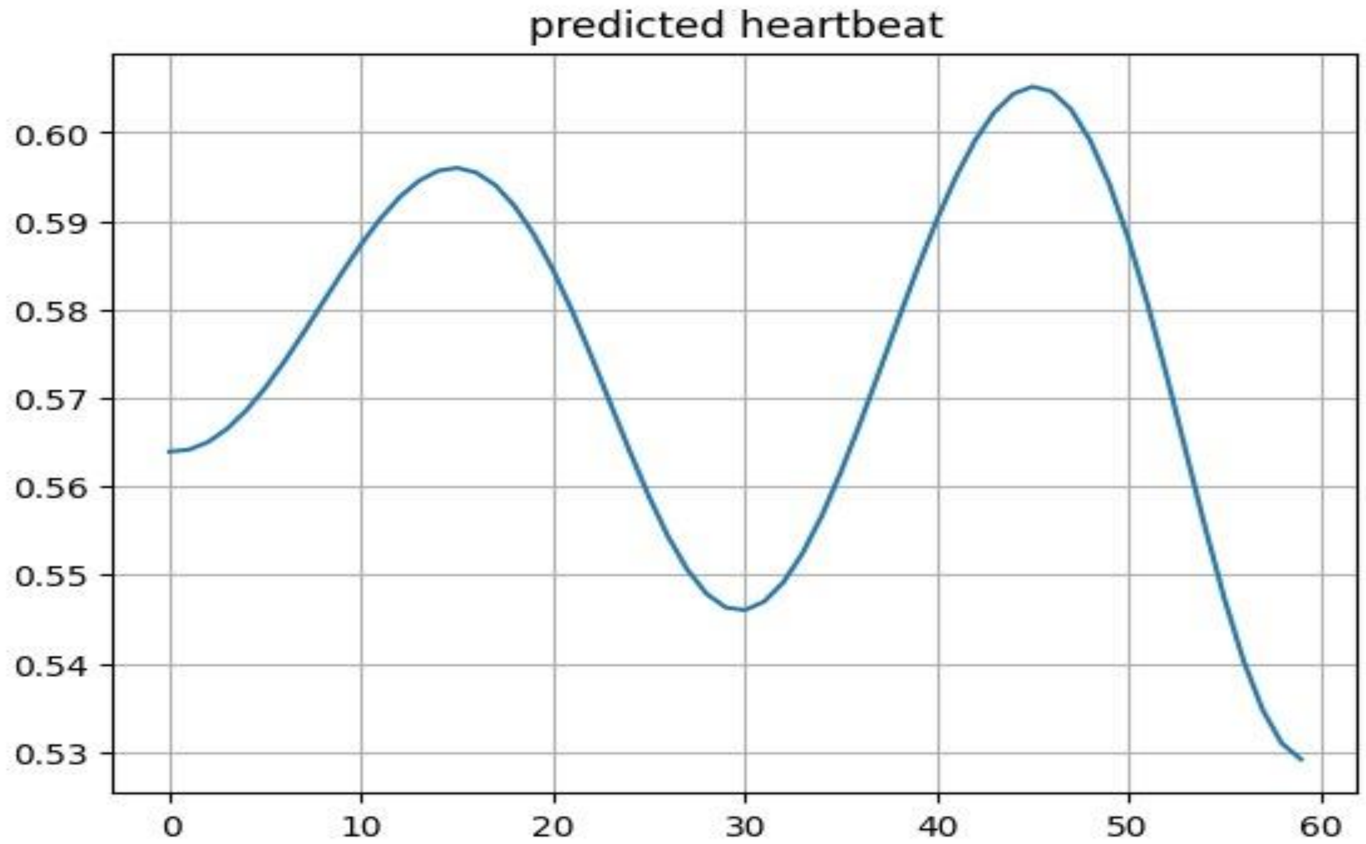
Throughout the training phase, we utilize the first 10,000 data points from the dataset, equivalent to roughly one hour of ECG data. Following this, the dataset is partitioned, with 80% allocated for training the model and the remaining 20% set aside for assessing its performance on unseen data.

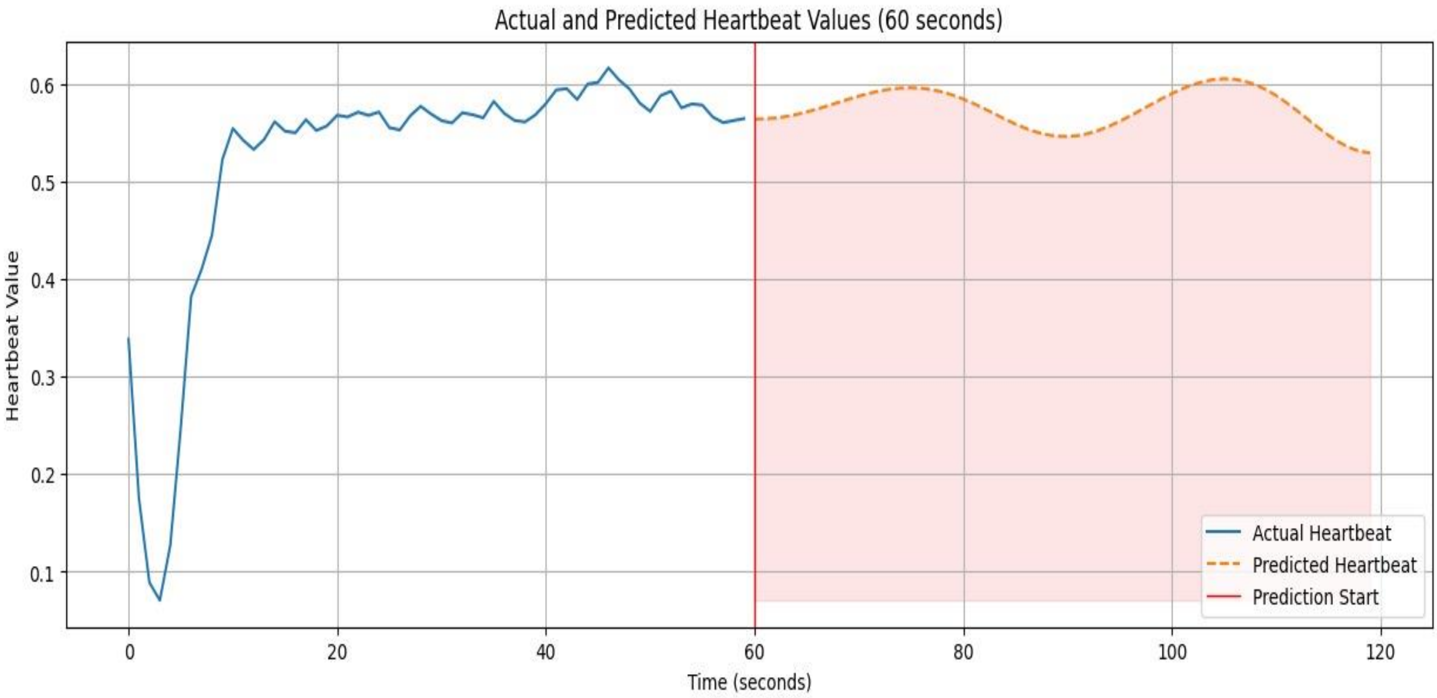
The training process spans 15 epochs, wherein the model iterates through the training data 15 times. Additionally, it encompasses 8 batches, dictating the number of data points processed concurrently during each training iteration.

5.5.4. PREDICTION:

For prediction, the model utilizes the last 60 seconds of ECG data as input. This data is reshaped to match the model's expected format (likely one channel for the ECG signal and a window size of 60 data points). The model then predicts the next 60 seconds of heartbeat values.

These predicted values can be visualized by plotting them on a graph, allowing for an analysis of the model's forecasted heartbeat pattern compared to the actual ECG signal.





5.5.5. MODEL EVALUATION:

The CNN + LSTM model's performance is summarized by these metrics:

- **R^2:** indicating 87.44% of the actual heartbeat data variance is explained by the predictions.
- **MSE:** of 0.00148 signifying a very low average squared difference between predicted and actual heartbeats.
- **MAE:** of 0.0158 reflecting an average absolute error of 0.0158 in predicted heartbeat values.
- **RMSE:** of 0.0385 suggesting a typical error around 0.0385 in the same units as the ECG data.
- **MAPE:** of 28.14%, representing an average absolute percentage error of 28.14% between predicted and actual heartbeats.

Overall, these metrics point towards good model performance in predicting the next heartbeat.

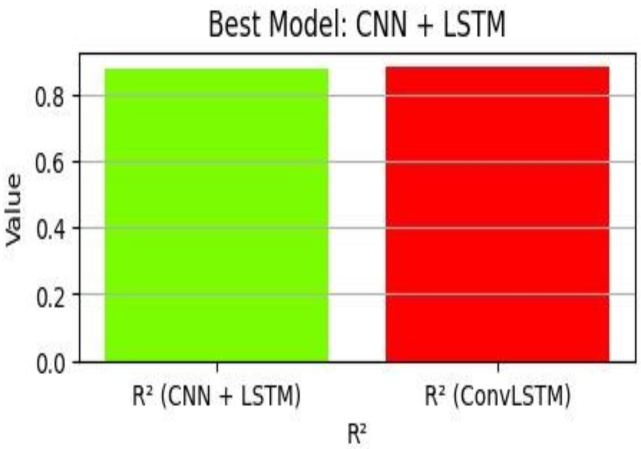
5.6. MODEL COMPARISION:

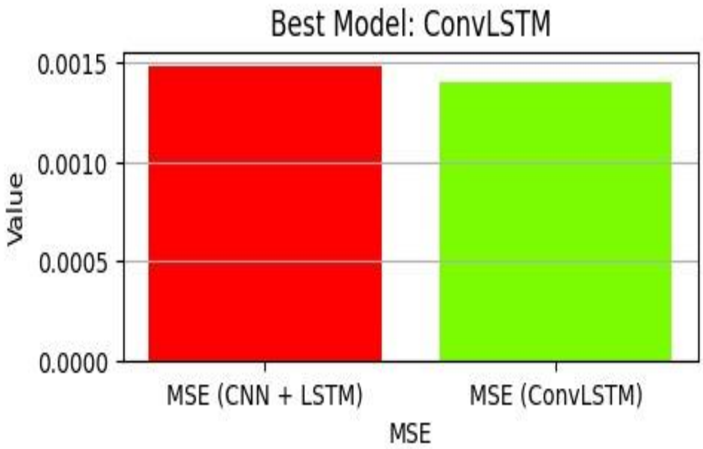
Both the CNN + LSTM and ConvLSTM models achieved good performance in predicting the next heartbeat based on the evaluation metrics you provided. Here's a breakdown of the comparison and some inferences:

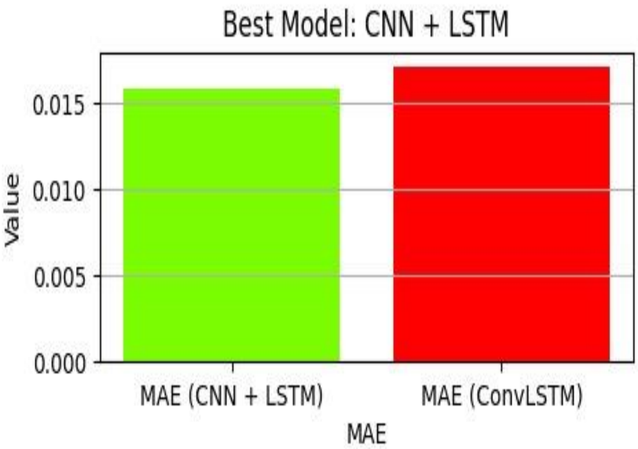
METRICS COMPARISION TABLE:

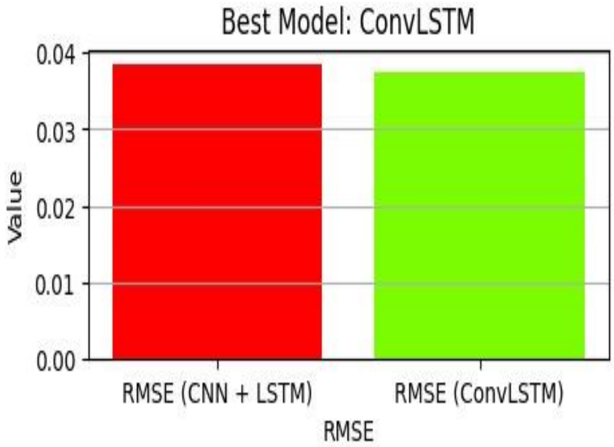
Metric	***CNN + LSTM***	***ConvLSTM***	***Inference***
R²	*0.87441*	*0.8818*	*ConvLSTM performs slightly better (0.74% higher) in explaining the variance in actual heartbeat data with its predictions.*
MSE	*0.00148*	*0.0014*	*Both models have very low average squared errors, indicating similar performance in this aspect.*
MAE	*0.0158*	*0.01709*	*ConvLSTM has a slightly higher average absolute error (0.0012 more), but the difference is negligible.*
RMSE	*0.0385*	*0.0374*	*ConvLSTM has a marginally lower root mean squared error, suggesting a hint of better typical error on average.*
MAPE	*28.136*	*27.911*	*ConvLSTM has a slightly lower average absolute percentage error (0.225% lower). However, MAPE can be sensitive to outliers, so this difference might not be significant.*

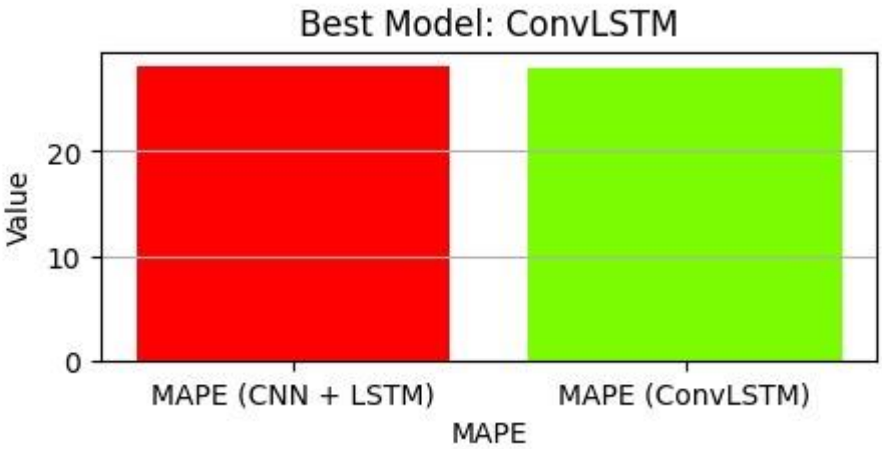
METRICS COMPARISION GRAPH:











5.7. CONCLUSION:

ConvLSTM appears to perform slightly better than the CNN + LSTM model based on R^2, RMSE, and MAPE. The differences are minimal, but they suggest that the ConvLSTM architecture might be better suited for capturing the nuances of the ECG data for heartbeat prediction in this specific case.

6. MODULES FOR REVIEW 3:

6.1. EXPLORING MODEL PARAMETER MODIFICATIONS:

- In the second review of the project, the training dataset employed comprised 10,000 data points. To enhance the model's generalizability and robustness, the current review (review 3) leverages a significantly larger dataset containing 100,000 data points
- To determine the optimal training configuration, the models were trained with different hyperparameters, specifically epochs (30, 20, 15) and batch sizes (8, 16). This systematic exploration allows us to identify the combination that yields the best performance on the validation set.

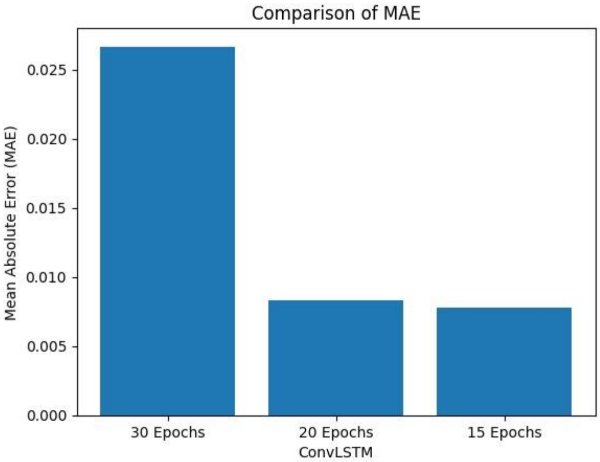
6.2. COMPARATIVE ANALYSIS OF MODEL:

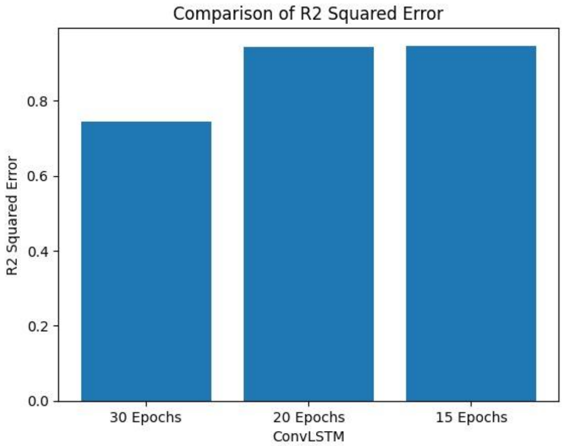
6.2.1. OVERALL REPORT OF THE MODEL:

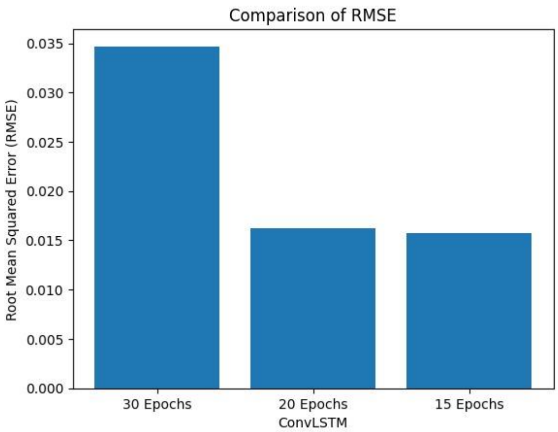
MODEL NAME	CNN + LSTM Model			ConvLSTM Model		
METRICS	15 EPOCH	20 EPOCH	30 EPOCH	15 EPOCH	20 EPOCH	30 EPOCH
Mean Square Error (MSE)	0.0002093	0.00022175	0.00021355	0.0002489	0.0002636	0.001203
Mean Absolute Error (MAE)	0.0068087	0.00770783	0.00698958	0.0078049	0.0083396	0.026658
Root Mean Square Error (RMSE)	0.0144692	0.01489127	0.01461355	0.0157768	0.01623672	0.0346856
R^2 Error	0.9553571	0.95271423	0.95446156	0.9469229	0.94378353	0.743453
Mean Absolute Percentage Error (MAPE)	15.696206	16.0154708	15.9253866	15.918789	15.7503256	16.58365

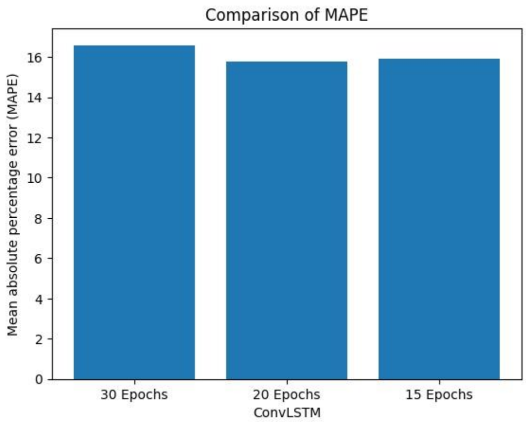
6.2.2. EPOCHS VS METRICS GRAPH:

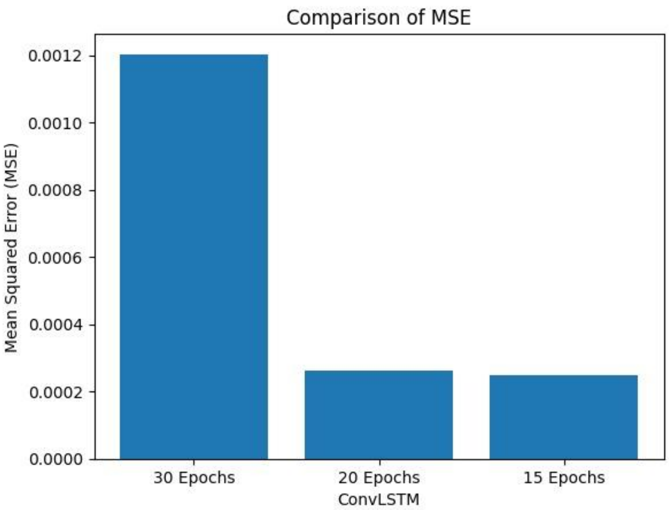
- ***MODEL 1: CONVLSTM:***



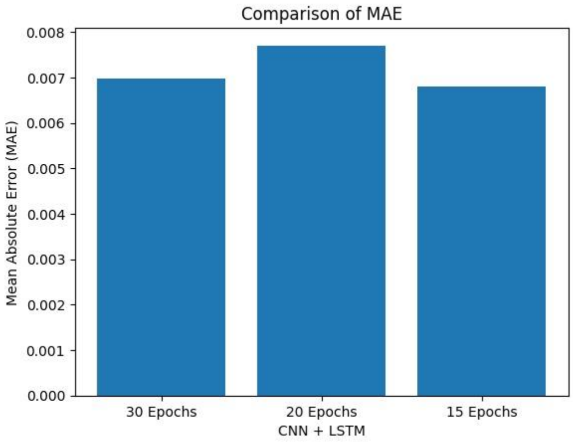


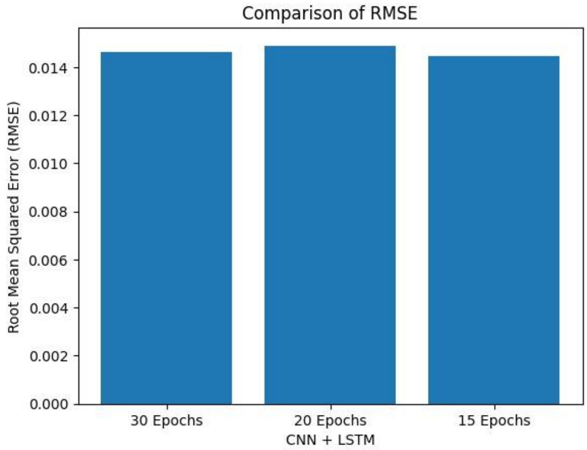


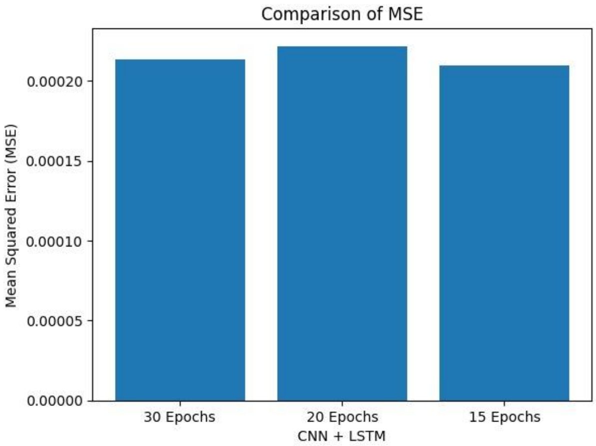


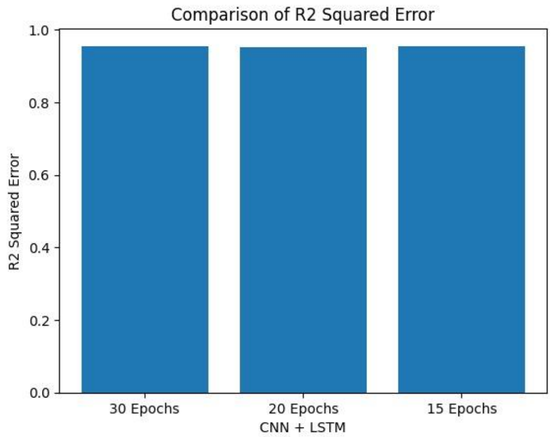


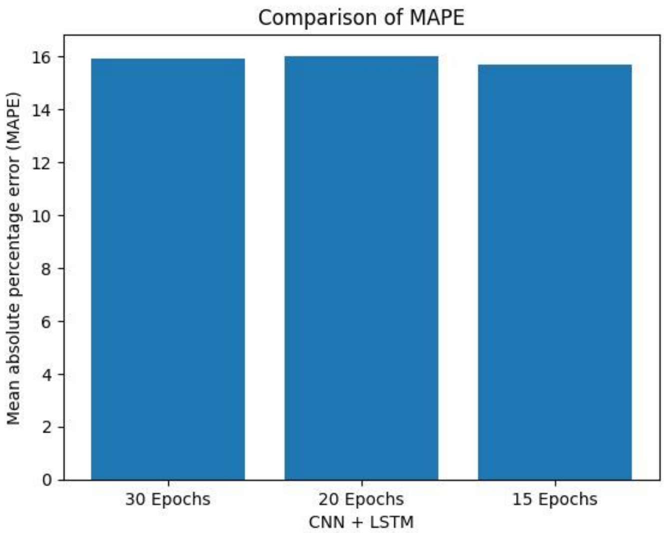
MODEL 2: CNN + LSTM:



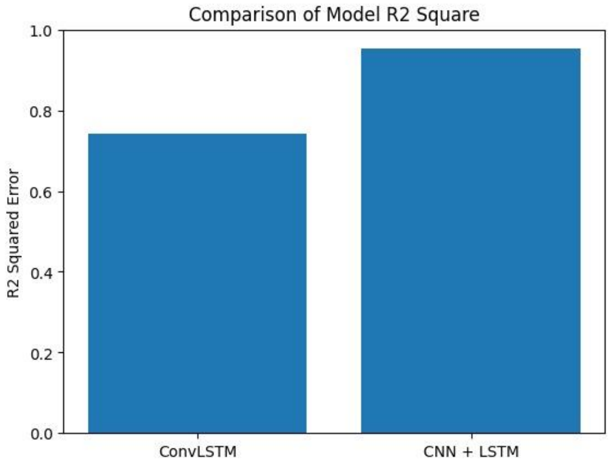


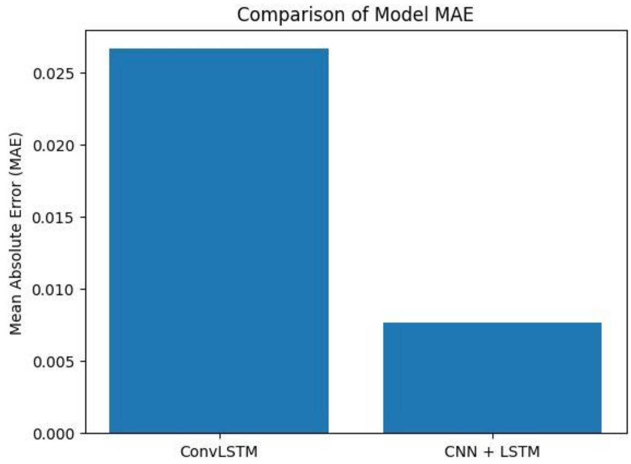


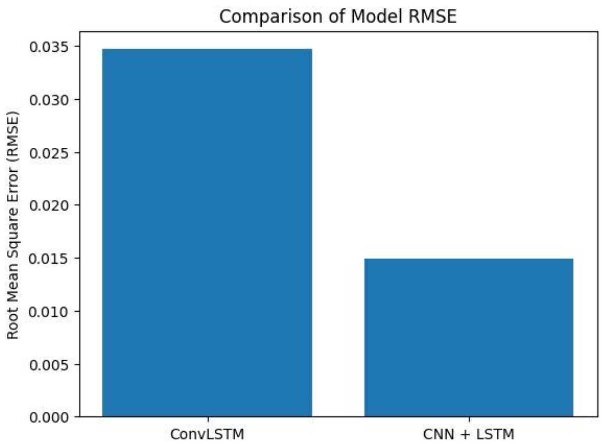


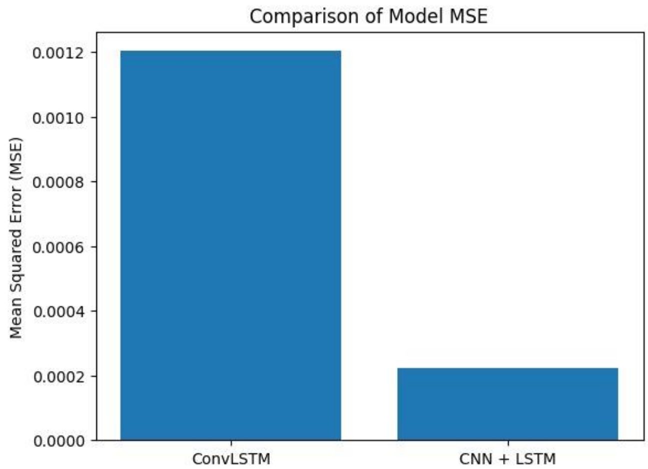


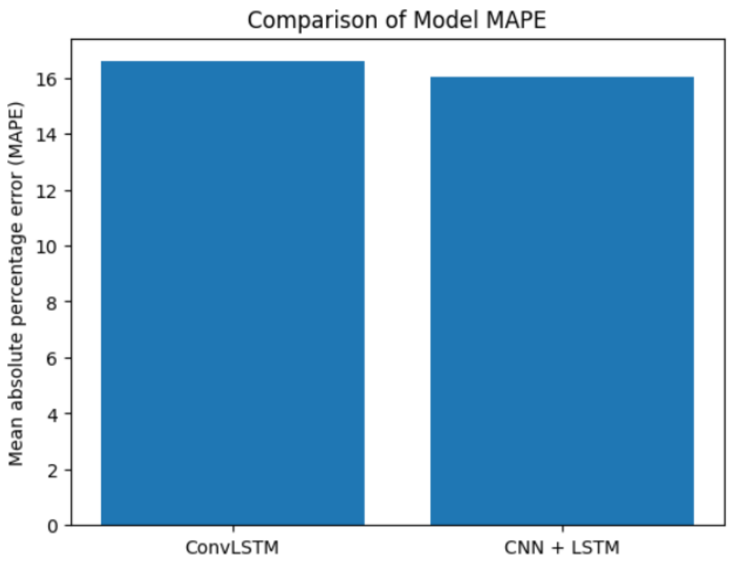
6.2.3. TWO MODEL VS METRICS GRAPH:











OVERALL INFERENCE:

- While all models achieved comparable performance, a detailed comparative analysis revealed that the ConvLSTM model trained with 30 epochs and a batch size of 16 yielded slightly superior results.

6.3. ANOMALY DETECTION:

- To adapt the model to the classification dataset, the window size of the input data was increased to 140 samples to match the classification task's format.
- A separate classification model is then employed to utilize the extracted features from stage 1. This classification model is trained to distinguish between normal and anomalous ECG signals based on the learned features.
- The predicted outputs from the initial CNN-LSTM or ConvLSTM models serve as the input to the classification model.

ANOMALY DETECTION - DATA PREPROCESSING

```
from tensorflow.keras.utils import to_categorical  # Utility for one-hot encoding
```

```
data = dataframe.iloc[:,:-1]
labels = dataframe.iloc[:,-1]
```

```
train_data, test_data, train_labels, test_labels = train_test_split(data, labels, test_size=0.2, random_state=21)
```

```
def normalize_ecg_data(data):
  min_val = np.min(data)
  max_val = np.max(data)
  return (data - min_val) / (max_val - min_val)
  data = (data - min_val) / (max_val - min_val)
  data = tf.cast(data, tf.float32)
  return data
```

```
train_data = normalize_ecg_data(train_data)
test_data = normalize_ecg_data(test_data)
```

```
sequence_length = 140  # Length of ECG sequences in ECG5000
num_features = 1  # Assuming single-channel ECG data
num_classes = 2
epochs = 10
batch_size = 32
```

```
from tensorflow.keras.layers import Conv1D, Dropout, LSTM, Dense  # Model layers
```

ECG_signal_Prediction (3).ipynb

colab.research.google.com/drive/1K6XEbbEMIqTM9XoUzn3x9SLLgM5OrNXo#scrollTo=LHkBm2yigei2

ANOMALY DETECTION - MODEL BUILDING

```
model = Sequential([
  Conv1D(filters=32, kernel_size=3, activation='relu', input_shape=(sequence_length, num_features)),
  Dropout(0.2),
  LSTM(units=64, return_sequences=True),  # Use LSTM for temporal dependencies
  Dropout(0.2),
  LSTM(units=32),
  Dropout(0.2),
  Dense(units=2, activation='sigmoid')
])
```

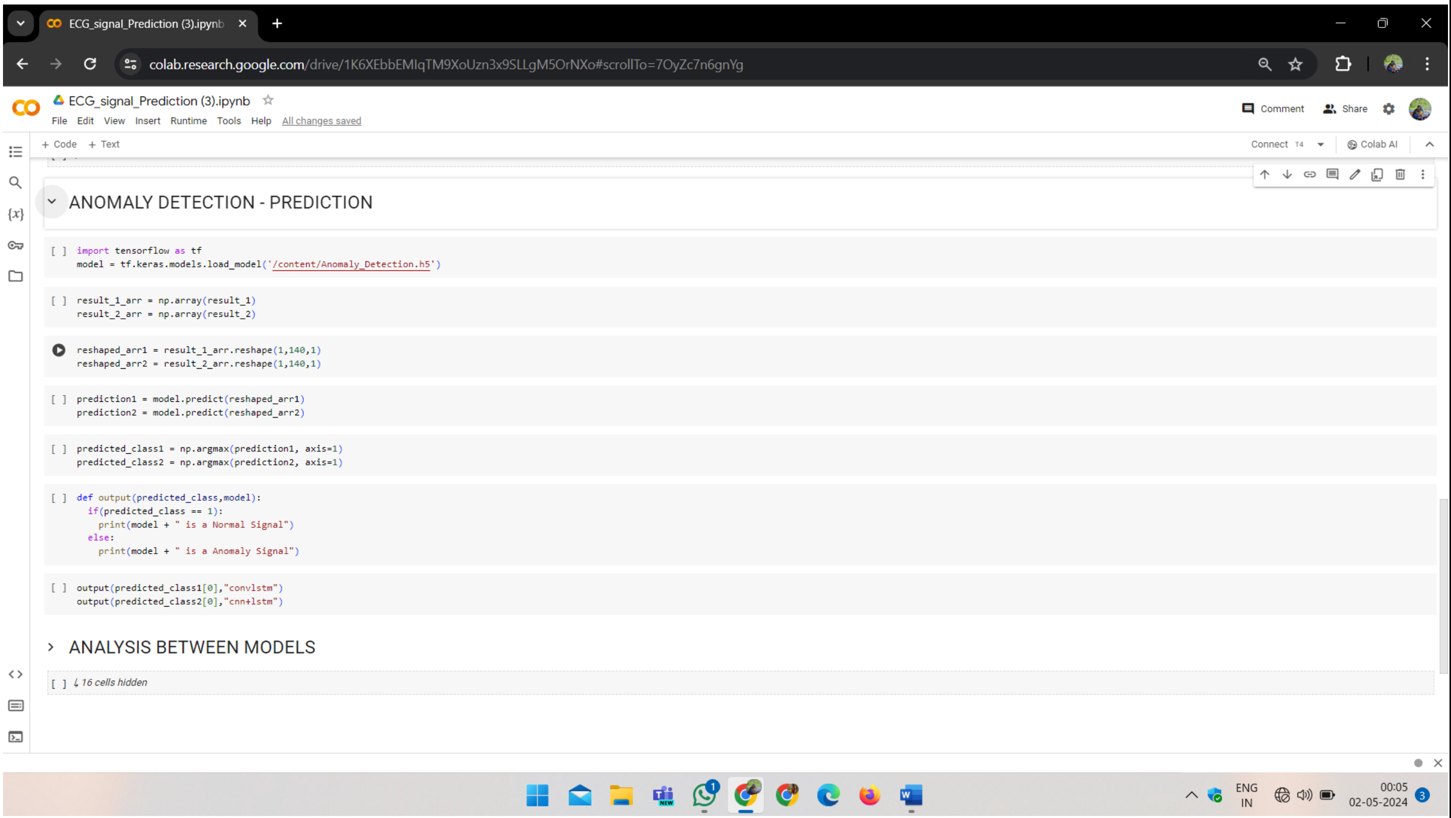
```
train_labels = to_categorical(train_labels)
```

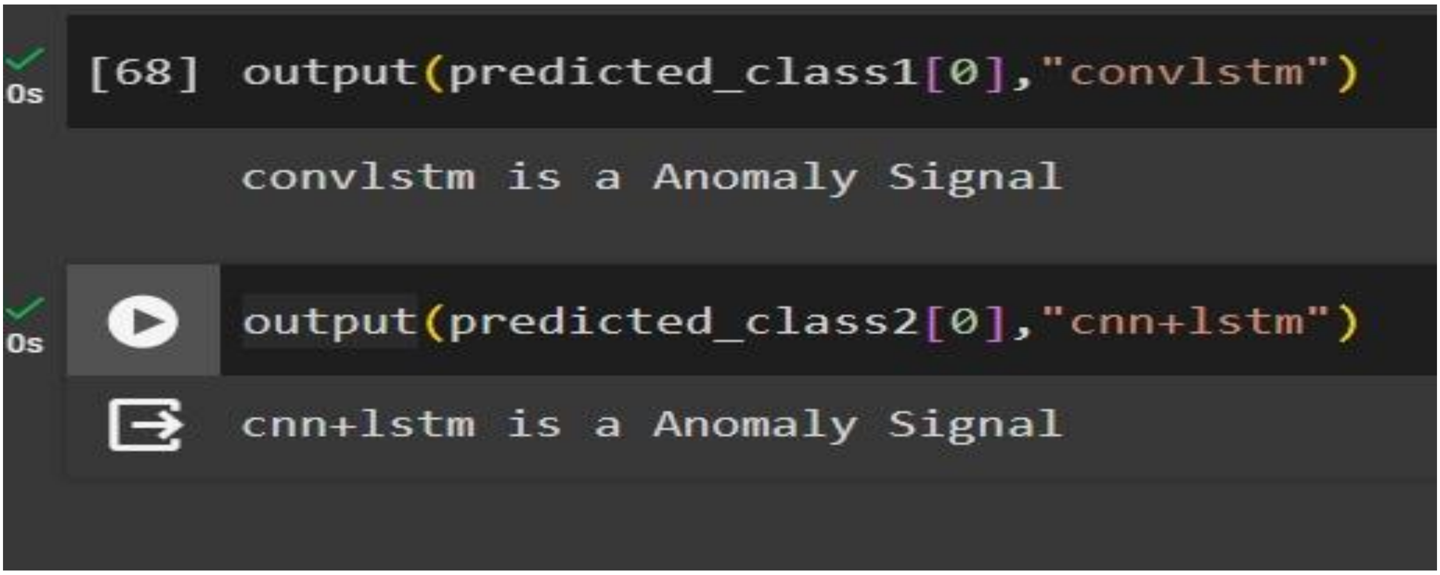
```
model.compile(optimizer='adam', loss='categorical_crossentropy', metrics=['accuracy'])

history = model.fit(train_data, train_labels, epochs=epochs, batch_size=batch_size)
```

```
Epoch 1/10
125/125 [==============================] - 24s 153ms/step - loss: 0.3284 - accuracy: 0.8337
Epoch 2/10
125/125 [==============================] - 18s 145ms/step - loss: 0.0876 - accuracy: 0.9722
Epoch 3/10
125/125 [==============================] - 19s 153ms/step - loss: 0.0808 - accuracy: 0.9760
Epoch 4/10
125/125 [==============================] - 18s 145ms/step - loss: 0.0619 - accuracy: 0.9817
Epoch 5/10
125/125 [==============================] - 20s 163ms/step - loss: 0.0556 - accuracy: 0.9822
Epoch 6/10
125/125 [==============================] - 19s 148ms/step - loss: 0.0514 - accuracy: 0.9845
Epoch 7/10
125/125 [==============================] - 19s 153ms/step - loss: 0.0535 - accuracy: 0.9845
Epoch 8/10
125/125 [==============================] - 18s 146ms/step - loss: 0.0530 - accuracy: 0.9857
Epoch 9/10
125/125 [==============================] - 19s 156ms/step - loss: 0.0489 - accuracy: 0.9855
Epoch 10/10
125/125 [==============================] - 18s 145ms/step - loss: 0.0479 - accuracy: 0.9847
```

```
model.save("Anomaly_Detection.h5")
```





6.4. GUI IMPLEMENTATION:

- The graphical user interface (GUI) features an interactive dashboard designed for comparative analysis of the models.
- The dashboard is divided into three dedicated sections, each corresponding to a specific training epoch (30, 20, and 15).
- Within each section, key performance metrics and results for the model trained with that particular epoch are presented in a clear and concise manner.
- This allows users to easily compare the performance of models trained with different hyperparameters directly on the dashboard.

TOOLS:

- Figma – UI designing
- VS code – coding

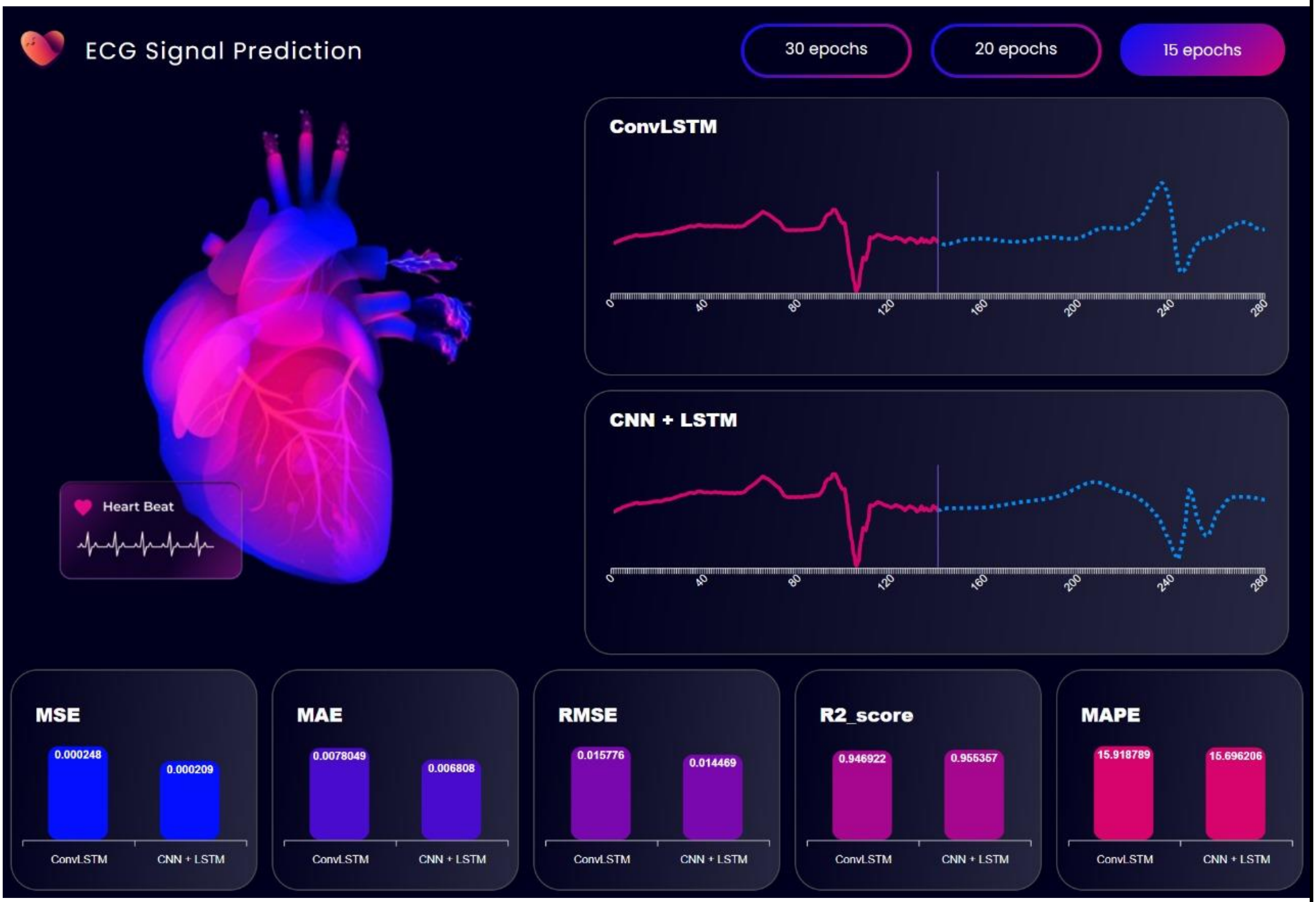
LIBARY:

- ApexCharts.js – for graph ploting

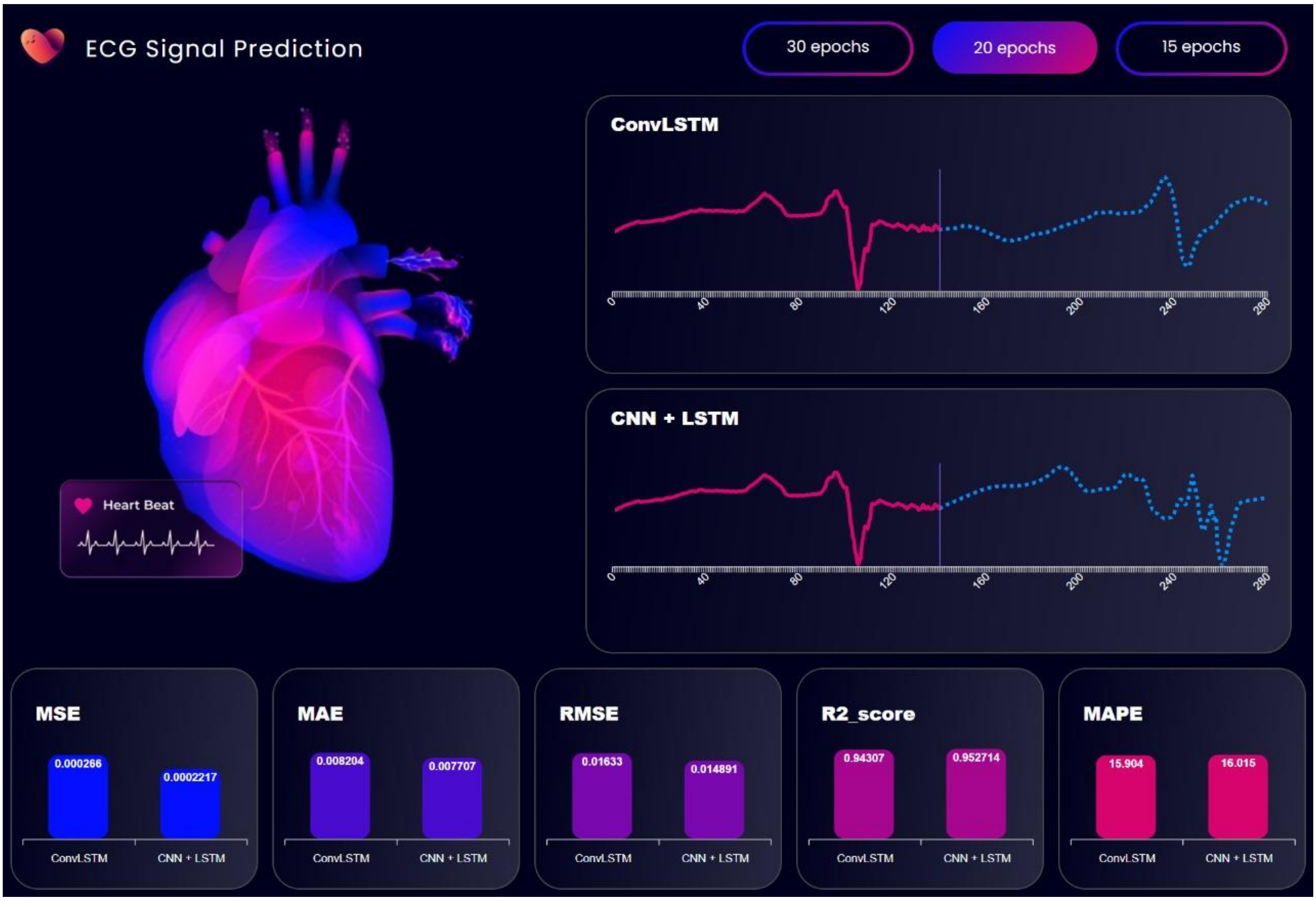
PROGRAMMING LANGUAGES:

- Html
- Css
- Javascript

GUI REPRESENTATION OF 15 EPOCHS RESULT:



GUI REPRESENTATION OF 20 EPOCHS RESULT:



GUI REPRESENTATION OF 30 EPOCHS RESULT:

7. CONCLUSION:

This project explored the use of ConvLSTM and CNN-LSTM architectures to predict future ECG signal segments and classify them as normal or anomalous. By training the models with various hyperparameters on a large ECG dataset and selecting the best performer based on various metrics, the project demonstrates the potential of deep learning for ECG anomaly detection.

The two-stage approach, where the chosen model predicts anomaly scores for segments and a separate model classifies the entire signal, offers a promising solution for ECG analysis. Future work can focus on expanding data size, exploring advanced architectures, and validating the approach in real-world settings to further improve its effectiveness in healthcare.

8. *REFERENCES:*

1. *Izhar Ahmed Khan, Nour Moustafa, Imran Razzak, M. Tanveer, Dechang Pi, Yue Pan, Bakht Sher Ali,XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks, Future Generation Computer Systems, Volume 127,2022, ISSN 0167-739X.*
2. *M. Woźniak, J. Siłka, M. Wieczorek and M. Alrashoud, "Recurrent Neural Network Model for IoT and Networking Malware Threat Detection," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5583-5594, Aug. 2021, doi: 10.1109/TII.2020.3021689.*
3. *J. Fan, X. Wang, Y. Guo, X. Hu and B. Hu, "Federated Learning Driven Secure Internet of Medical Things," in IEEE Wireless Communications, vol. 29, no. 2, pp. 68-75, April 2022, doi: 10.1109/MWC.008.00475.*
4. *M. Woźniak, A. Zielonka, A. Sikora, M. J. Piran and A. Alamri, "6G-Enabled IoT Home Environment Control Using Fuzzy Rules," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5442-5452, 1 April1, 2021, doi: 10.1109/JIOT.2020.3044940.*
5. *M. Ali, F. Naeem, M. Tariq and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 778-789, Feb. 2023, doi: 10.1109/JBHI.2022.3181823.*
6. *E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724-4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.*
7. *I. A. Khan, N. Moustafa, D. Pi, K. M. Sallam, A. Y. Zomaya and B. Li, "A New Explainable Deep Learning Framework for Cyber Threat Discovery in Industrial IoT Networks," in IEEE Internet of Things Journal, vol. 9, no. 13, pp. 11604-11613, 1 July1, 2022, doi: 10.1109/JIOT.2021.3130156.*
8. *Ali, R., Kim, B., Kim, S. W., Shahin, N., Bajracharya, R., Butt, R. A., ... & Gungor, V. C. (2020). Reinforcement learning-based channel access mechanism for LTE-LAA and Wi-Fi coexistence. Computer Communications, 150, 498-505.*
9. *Y. Xu, Z. Liu, Y. Li, H. Hou, Y. Cao, Y. Zhao, W. Guo, L. Cui, Feature data processing: Making medical data fit deep neural networks, Future Gener. Comput. Syst. 109 (2020) 149–157.*
10. *B. Li, Y. Wu, J. Song, R. Lu, T. Li, L. Zhao, DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems, IEEE Trans. Ind. Inform. 17 (8) (2020) 5615–5624.*
11. *M.N. Hossen, V. Panneerselvam, D. Koundal, K. Ahmed, F.M. Bui, S.M. Ibrahim, Federated machine learning for detection of skin diseases and enhancement of internet of medical things (IoMT) security, IEEE J. Biomed. Health Inform. (2022).*
12. *Y. Chen, X. Qin, J. Wang, C. Yu, W. Gao, Fedhealth: A federated transfer learning framework for wearable healthcare, IEEE Intell. Syst. 35 (4) (2020) 83–93.*

13. *R. Ali, Y. B. Zikria, S. Garg, A. K. Bashir, M. S. Obaidat and H. S. Kim, "A Federated Reinforcement Learning Framework for Incumbent Technologies in Beyond 5G Networks," in IEEE Network, vol. 35, no. 4, pp. 152-159, July/August 2021, doi: 10.1109/MNET.011.2000611.*

14. *J. Ahmed, T. N. Nguyen, B. Ali, M. A. Javed and J. Mirza, "On the Physical Layer Security of Federated Learning Based IoMT Networks," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 691-697, Feb. 2023, doi: 10.1109/JBHI.2022.3173947.*

15. *Md. Milon Islam, Sheikh Nooruddin, Fakhri Karray, Ghulam Muhammad, Multi-level feature fusion for multimodal human activity recognition in Internet of Healthcare Things, Information Fusion, Volume 94, 2023, Pages 17-31, ISSN 1566-2535,*

16. *X. Yuan, J. Chen, K. Zhang, Y. Wu and T. Yang, "A Stable AI-Based Binary and Multiple Class Heart Disease Prediction Model for IoMT," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3,pp. 2032-2040, March 2022, doi: 10.1109/TII.2021.3098306.*

17. *Huang, Fuying, et al. "An ECG signal prediction method based on ARIMA model and DWT." 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, 2019.*

18. *Prakarsha, Kandukuri Ratna, and Gaurav Sharma. "Time series signal forecasting using artificial neural networks: An application on ECG signal." Biomedical Signal Processing and Control 76 (2022): 103705.*

19. *Chen, Jiaming, Ali Valehi, and Abolfazl Razi. "Smart heart monitoring: Early prediction of heart problems through predictive analysis of ECG signals." Ieee Access 7 (2019): 120831-120839.*

20. *Sun, Zhong-Gao, et al. "An ECG signal analysis and prediction method combined with VMD and neural network." 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC). IEEE, 2017.*

9. APPENDIX:

9.1. REVIEW 3 MODULES:

- ***EXPLORING MODEL PARAMETER MODIFICATIONS***

  Done by: Rithika A and Vignesh M

- ***ANOMALY DETECTION***

  Done By: Lithika B

- ***GUI IMPLEMENTATION***

  Done By: Sadhana S

9.2. GOOGLE DRIVE LINK:

- ***ISM BASE PAPER LINK:***

  https://drive.google.com/file/d/1bI8G7hAbyMBi9c5t7dc4TjFekYOez_r-/view?usp=sharing

- ***ISM REVIEW 1 DOC LINK:***

  https://drive.google.com/file/d/1wmkv7h81qpTBnSYZGVfeAj_5cdfzh6Qj/view?usp=sharing

- ***ISM REVIEW 2 DOC LINK:***

  https://drive.google.com/file/d/1Pkl03V-N_s_nHCQ0Tt2IDDiLzXsWc9sa/view?usp=sharing

- ***ISM PYTHON NOTEBOOK LINK:***

  https://drive.google.com/drive/folders/1Wmyw_BZtUDocVhFHvXT0lRK0wlBvSV_h?usp=sharing

- ***ISM EDITABLE IMAGE LINK:***

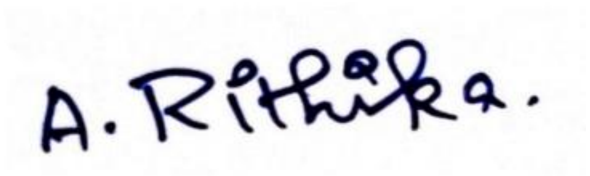
  https://drive.google.com/drive/folders/1qpw6AOkwma7cWS3P3VjOF1wzJ0eqVBrB?usp=sharing

- ***VIDEO DEMONSTRATION LINK:***

  https://youtu.be/ppIBEZ2fkDw

9.3. DIGITAL SIGNATURE & EMAIL ID OF TEAM MEMBERS:

1. ***RITHIKA A (rithika.a2020@vitstudent.ac.in)***



2. ***LITHIKAA B (lithikaa.b2020@vitstudent.ac.in)***

3. ***VIGNESH M (vignesh.m2020b@vitstudent.ac.in)***

4. ***SADHANA S (sadhana.2020b@vitstudent.ac.in)***