[1] Ritunsa Mishra*
[2] Rabinarayan Satpathy
[3] Bibudhendu Pati
[4] Rudra Prasanna Mishra

Enhancing Patient Outcome Predictions Through Differential Privacy with Optimized RNN Model Applied to Electronic Health Record

Abstract: - This study introduces a novel method for predicting patient admission and discharge events using Electronic Health Records (EHR) while prioritizing the protection of personal privacy. Our approach utilizes a Simple Recurrent Neural Network (RNN) model enhanced with a Differential Privacy mechanism to strike a balance between high-accuracy outcome predictions and the confidentiality of patient data. At the core of our methodology is the application of a Simple RNN to EHR data, which facilitates the prediction of whether a patient will be admitted to or discharged from a healthcare facility. To strengthen data confidentiality, we integrate Differential Privacy by injecting controlled noise into the dataset, ensuring that our model's predictions preserve the privacy of individual patient records.
We conducted experiments using six different classifiers to implement our privacy-preserving prediction strategy. Among these, the Random Forest classifier emerged as the most accurate, proving the effectiveness of our method in providing reliable predictions without compromising privacy. In contrast, the XG Boost classifier showed the least precision, indicating some limitations in its ability to balance privacy with predictive accuracy. This research significantly advances the field of healthcare informatics by presenting a sophisticated solution that combines cutting-edge predictive models with stringent privacy safeguards. Our findings highlight the critical need to maintain a delicate balance between achieving precise clinical predictions and upholding the moral responsibility to protect patient privacy in the modern landscape of digital health records.

Keywords: RNN, Electronic Health Record (EHR), Differential Privacy (DP), Patient Data Confidentiality, In & Out Prediction.

I. INTRODUCTION

The digitalization of healthcare records has brought about a revolution in the realms of medical research and patient care. Electronic Health Records (EHR) present an invaluable source of information, unlocking unprecedented opportunities for predicting patient outcomes and refining clinical decision-making. However, this transformative shift towards digitization has not come without its share of challenges, especially when it comes to safeguarding the privacy and confidentiality of sensitive health data. Graph Neural Networks (GNNs) prove instrumental in predicting clinical risks by capturing the relational dynamics within medical events and entities, handling extensive Electronic Health Record (EHR) datasets. Future research endeavors within this domain could tackle challenges such as the diverse nature of EHR data, incorporation of multiple modalities, and enhancing model interpretability. The overarching goal is to advance the development of comprehensive GNN models that offer heightened prediction accuracy, seamless integration into clinical settings, and, ultimately, contribute to the enhancement of patient care [1, 24].

In response to these challenges, our research is dedicated to addressing the dual imperative of ensuring accurate patient outcome predictions and safeguarding individual privacy within the domain of EHR. We employ Recurrent Neural Networks (RNNs), a subset of artificial neural networks tailored for handling sequential data, to propose an innovative approach for predicting patient admission and discharge statuses based on their EHR details. Additionally, in recognition of the inherent privacy risks associated with handling such sensitive information, we introduce a Differential Privacy optimization mechanism into our model. Patient representation learning involves acquiring a condensed mathematical representation of a patient, capturing significant information from Electronic Health Records (EHRs). This process typically employs sophisticated deep learning methods to accomplish the task [2].

The incorporation of Differential Privacy stands out as a pivotal element in our methodology, seeking to strike a delicate balance between harnessing the wealth of information contained within EHR and upholding patient confidentiality. By introducing controlled noise during the training process, we ensure that the predictions generated by our model do not compromise the privacy of individual health records. As an example, in the

[1,2,3,4] Faculty of Engineering & Technology, Sri Sri University, Cuttack, Odisha, India, 3Dept. of Computer Science, Rama Devi Women's University, Bhubaneswar, Odisha, India.
*Corresponding author: Ritunsa Mishra, Faculty of Engineering & Technology, Sri Sri University, Cuttack, Odisha, India, Email: mishraritunsa@gmail.com

research [3] its primary objective is to address the pressing security challenges in healthcare administration, particularly concerning the exposure of sensitive medical data. The proposed solution involves a hybrid system combining sensitive attribute access primitives, enhanced attribute-based encryption, and anonymity methods to safeguard electronic health records. The focus is on achieving improved performance, particularly in terms of completion time, encryption, and decryption processes, with a goal to provide a more secure and efficient healthcare technology solution in the face of evolving threats and technological advancements. The swift integration of electronic health records (EHRs) presents a significant opportunity for progressing medical knowledge through insights gained from practical experience. Nonetheless, the credibility of clinical research based on EHRs faces uncertainty, given the challenges of inadequate research reproducibility stemming from the intricate and diverse nature of healthcare institutions and EHR systems [4].

Time-based electronic health records (EHRs) encompass extensive information suitable for secondary purposes, including the prediction of clinical events and the management of chronic diseases. Nevertheless, there are inherent challenges associated with the representation of temporal data [5, 25]. This paper is dedicated to providing a comprehensive exploration and presentation of our RNN-based approach, delving into the methodology, experimentation, and outcomes. Through a meticulous analysis of six classifiers that implement our proposed technique, we aim to shed light on the effectiveness of our model in achieving both accurate outcome predictions and robust data privacy. This research seeks to contribute meaningfully to the broader discourse on healthcare informatics, offering a holistic solution that navigates the intricate intersection of predictive modelling and ethical considerations surrounding patient data privacy in electronic health environments. In particular, the technique of evidence-based decision-making demonstrates the capacity to employ multiple levels of non-linear feature transformation through representation learning, addressing challenges presented by extensive datasets [6].

This research paper delves into the formulation of a novel methodology geared towards forecasting patient outcomes using Electronic Health Records (EHR) data, all while prioritizing the privacy and confidentiality of sensitive patient information. The research commences by harnessing primary EHR data to predict patient in-and-out probabilities based on their blood reports. To safeguard patient privacy, the initial step involves de-identifying the primary data meticulously. Subsequently, the EHR data undergoes intensive model training employing an RNN model architecture to enable precise outcome predictions. Post the model training stage, the study integrates differential privacy mechanisms to introduce carefully controlled noise into the data, thereby bolstering the safeguarding of patient information from unauthorized access. Through this comprehensive approach, the paper endeavors to contribute to the advancement of outcome prediction in healthcare while concurrently addressing the paramount concern of data privacy in electronic health records.

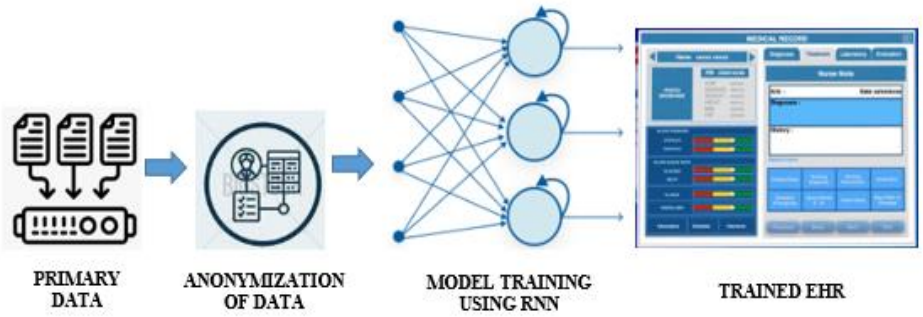


Fig 1: Training Electronic Health Record Data.

Referring to the Fig 1, the integration of differential privacy optimization is instrumental in enhancing privacy measures without compromising the predictive accuracy of the model. As a result, the culmination of the research yields EHR data enriched with privacy-preserving noise, accessible solely to authorized personnel, thus ensuring the safety and confidentiality of patient information. Through this holistic approach, the study endeavors to advance outcome prediction in healthcare while simultaneously addressing paramount concerns surrounding data privacy in electronic health environments [26].

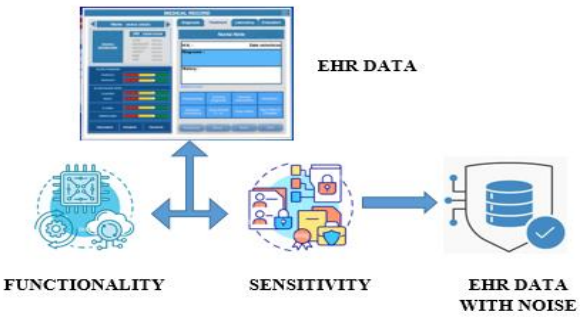


Fig 2: Add Noise to EHR Data to Secure the Information.

II. OBJECTIVE OF THIS WORK

In this study, our attention is directed towards three fundamental objectives outlined below.

- To conduct a thorough literature review to identify gaps in existing research methodologies within the field.
- To enhance privacy measures by integrating and optimizing the model with Differential Privacy mechanisms, aiming to fortify the confidentiality of individual patient records in the Electronic Health Records (EHR) dataset.
- To develop an innovative predictive model based on Recurrent Neural Networks (RNNs) to achieve accurate patient outcome predictions using EHR data.

III. MOTIVATION FOR THIS WORK

The motivation behind undertaking this research stems from the pressing need to bridge gaps in the current landscape of healthcare informatics. As we witness the transformative shift toward digitized Electronic Health Records (EHR), the potential for leveraging predictive modelling to enhance patient outcome predictions is substantial. However, this potential is accompanied by ethical considerations, particularly concerning the privacy and confidentiality of sensitive health data. Recognizing these challenges, our motivation is rooted in the desire to develop a nuanced solution that not only accurately predicts patient outcomes using Recurrent Neural Networks (RNNs) but also prioritizes the implementation of robust privacy measures through Differential Privacy optimization. By navigating the intersection of predictive modelling and privacy preservation, our work aspires to contribute a thoughtful and practical approach to healthcare analytics, fostering advancements that are not only technologically sound but also ethically responsible in the ever-evolving realm of electronic health records.

IV. REVIEW OF LITERATURE

The literature review section encompasses essential aspects such as examining predictive models employed in healthcare, the intersection of Electronic Health Records (EHR) and predictive models, and the role of Differential Privacy (DP) optimizers in healthcare informatics. This exploration aids in comprehending the broader landscape of predictive modelling in healthcare, specifically in the context of EHR, and the incorporation of privacy measures. Within this section, our objective is to thoroughly analyze existing research, identifying the current state of knowledge, pinpointing research gaps, and establishing the context for the significance of our proposed "RNN-Based Approach for Outcome Prediction with Differential Privacy Optimization.

This research aims [7] to compare the effectiveness of deep Elman Recurrent Neural Networks (RNNs) with deep gated RNNs for statistical parametric speech synthesis (SPSS). While deep neural networks (DNNs) are commonly used for SPSS, their inability to capture temporal structures in speech poses limitations. RNNs, particularly those with LSTM cells, offer better performance but are computationally complex. This study explores whether deep Elman RNNs, with simpler architecture, can perform competitively in SPSS. Using the Blizzard Challenge 2015 dataset across three Indian languages, the research demonstrates the potential of deep Elman RNNs for acoustic modelling, context representation learning, and outperforming DNN-based duration models through both subjective and objective evaluations.

Table 1: Related Research Work

Author / Year	Objective	Dataset used	Methods Used	Focused Disease	Performance Measure	Future Scope
Choi et al. [2015] [8]	Applied to EHRs with longitudinal time stamps.	262K individuals.	Simple RNN	Multiple Diseases	Recall: 80.5%	Applicability and Accuracy need to be

						considered
Wu et al. [2018] [9]	Paediatric asthma classification using root mean difference.	4013 patients from the Olmsted Country Birth Cohort and 4000 patients from Physionet.	Simple RNN	Asthma in case of Children's	Precision- 84.54% Recall- 85.65% F1 score- 85.08%	Relative Time for event sequence need to be extended
Shi et al. [2016] [10]	Clinical notes for the assessment of various diseases based on a standard model.	4298 patients from a Chinese hospital with an A grade were assessed.	The accuracy of the CNN and Framingham risk score	Cerebral infraction (CI), Pulmonary Infarction (PI), And Coronary Heart (CH)	Accuracy CI- 96.5% PI- 95.6% CH- 93.6%	Adaptability, Effectiveness and risk assessment model need to be enhanced
Farzi et al. [2017] [11]	A rapacious method of utilising DBN for ADHD diagnosis.	73 New York University neuroimaging samples totalling 263.	DBN's avaricious strategy	ADHD	NI: 69.83% NYU's accuracy was 63.68%.	Early detection and accuracy need to be considered
Hwang et al. [2017] [12]	Disease prediction from EHRs using stacked auto-encoders and Generative Adversarial Networks (GAN).	There are 569 cases of breast cancer with records accessible, 212 of which are malignant and 357 of which are benign.	AE and GAN stacked	Breast cancer	95.28% is the sensitivity. 98.05% accuracy 99.47% specificity	Sensitivity & specificity of two stage framework need to be improved
Jorge et al. [2019] [13]	Identify lupus patients from the EHR.	A dataset including 400 EHR records.	The codified algorithm for machine learning is rule-based.	Specify SLE & probable SLE	Sensitivity- 86% Specificity- 60% PPV- 46% for SLE Sensitivity- 84% Specificity- 69% PPV 65% for probable SLE	Performance metric optimization need to be enhanced
Sun & Zhang [2019] [14]	The EHR is utilised in conjunction with five machine learning algorithms to diagnose DR.	301 hospitals in China 5057 records were supplied.	Decision Tree	Diabetic Retinopathy	87.7% Accuracy	Disease diagnosis method need to be integrated with readily available EHR
Aidaroos et al. [2012]	Medical data classifications include LR,	15 databases from the UCI library provide	NN, LR, DT, and NB	Numerous Health issues, such	97.43%: Accuracy AUC: 99%	Focus on hybrid models to

[15]	NB, NN, and DT.	illustrations of various disorders.		as liver problems, hepatitis, and cancer		enhance the efficiency of medical data mining
Zhang et al. [2019] [12]	SVMs are being used in EHRs to classify cancer.	Used 400 pieces of data for training, and 100 pieces of health information for every cancer.	SVM-RBF	Cancer	Accuracy: 98.31%	Accuracy need to be focused to detect the broader range of Cancer

The paper [17] introduces a distributed intelligence framework for Cyber-Physical Systems (CPS) focusing on security, data privacy, and adaptability. Unlike conventional methods prioritizing performance, our framework addresses risks linked to centralized data processing by leveraging Federated Machine Learning techniques. By decentralizing CPS architecture, local data processing on individual nodes is enabled, mitigating data breach and privacy risks. Successful implementation in an industrial CPS application validates the framework's viability, offering privacy, security benefits, along with promising accuracy and precision results.

This study [18] aims to improve the interpretability of Deep Learning (DL) models in clinical ICU settings by introducing a new interpretable neural network model called double self-attention architecture (DSA). Using two attention-based mechanisms, self-attention and effective attention, the DSA model captures the significance of input variables and their temporal changes. Evaluation on real-world clinical datasets of 22,840 patients demonstrates the effectiveness of our model in predicting delirium onset 12 h and 48 h in advance. Comparative analysis with three post-hoc interpretable algorithms and clinical opinion shows that our model effectively incorporates variable and temporal dependencies, enhancing descriptive performance without sacrificing predictive accuracy.

The main objective of this review [19] is to examine the recent advancements in utilizing deep learning techniques for clinical tasks based on electronic health records (EHRs). The review encompasses various applications such as information extraction, representation learning, outcome prediction, phenotyping, and de-identification. By analyzing existing literature, the review aims to identify the current state of the field and highlight areas for future research, including challenges related to model interpretability, data heterogeneity, and the need for universal benchmarks.

In this research [20] the primary objective is to develop a smart city application using IoT and Wireless Sensor Network (WSN) technology, aiming for optimal network performance classification. The infrastructure includes WSN, VANET, MANET, RFID, and WBAN. The study predicts the efficiency of each network component, considering factors like energy consumption, data size, mobility, throughput, and delay. The output from each network is fed into an Optimized Recurrent Neural Network (ORNN) for predicting the overall effectiveness of the IoT network. Parameter tuning in the RNN is achieved using the Self Adaptive Honey Badger Algorithm (SA-HBA). The method aims to accurately forecast and enhance the performance of the simulated IoT system, achieving minimal energy consumption and improved prediction accuracy. In a recent study, [23] this was highlighted that, limited success of utilizing natural language processing and machine learning to detect suicide attempts in a small group of hospitalized adolescents within a psychiatric environment.

V. METHODOLOGY USED

Data Pre-processing: The initial step involves meticulously processing the collected Electronic Health Record (EHR) data to ensure its integrity and suitability for analysis [21]. This encompasses several tasks such as addressing missing values, standardizing numerical features, encoding categorical variables, and eliminating any irrelevant or redundant information [22].

Feature Extraction: Subsequently, relevant features are either chosen or extracted from the pre-processed EHR dataset. This process may entail employing domain knowledge and statistical methodologies to identify variables that exhibit high predictive potential for patient outcomes.

Model Architecture Design: The architecture of the Recurrent Neural Network (RNN) model is meticulously crafted to effectively handle the sequential nature of EHR data [27]. Key decisions involve determining the number of layers, selecting appropriate RNN cell types (e.g., LSTM or GRU), defining activation functions, and tuning other hyper parameters.

Model Training: Following the architectural design, the RNN model undergoes rigorous training using the pre-processed and privacy-protected EHR data [30]. This phase revolves around optimizing the model's parameters utilizing advanced training algorithms such as stochastic gradient descent or Adam optimization, all while adhering to stringent differential privacy constraints.

Differential Privacy Optimization: Integral to the training process is the incorporation of differential privacy mechanisms to bolster the confidentiality of individual patient records. This entails introducing controlled perturbations into the training data or adapting learning algorithms to ensure that sensitive information remains safeguarded from potential inference.
Model Evaluation: Upon completion of training, the efficacy of the trained RNN model is assessed using a suite of evaluation metrics including accuracy, precision, recall, F1-score, and the area under the receiver operating characteristic curve (AUC-ROC). This comprehensive evaluation gauges the model's proficiency in predicting patient outcomes while upholding privacy preservation standards [31].
Cross-Validation: To ascertain the robustness and generalizability of the RNN-based approach, experimental validation is conducted using either a dedicated validation dataset or through cross-validation techniques. This validation procedure ensures that the model's performance remains consistent across diverse patient cohorts and healthcare environments.
Comparison and Interpretation: Finally, the performance of the RNN-based approach is meticulously benchmarked against baseline models or existing prediction methodologies to ascertain its superiority in terms of both predictive accuracy and privacy preservation. The study's findings are then meticulously interpreted and contextualized within the existing literature, elucidating the proposed approach's efficacy in outcome prediction and privacy optimization within the realm of electronic health records.

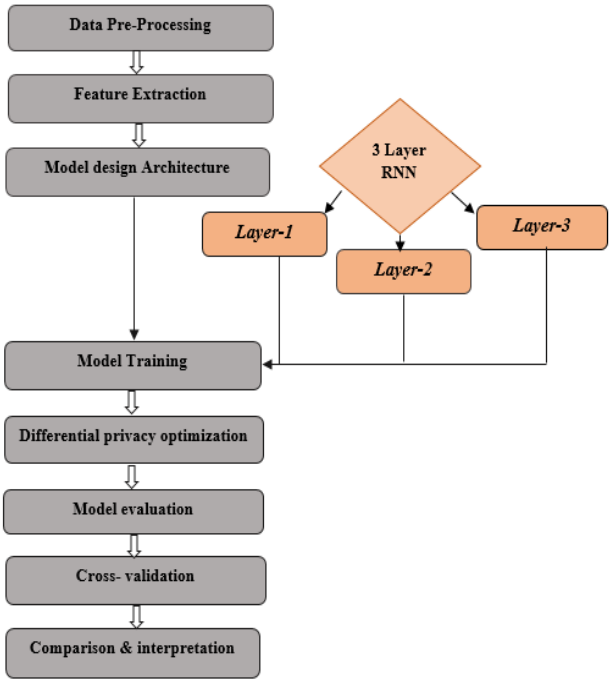
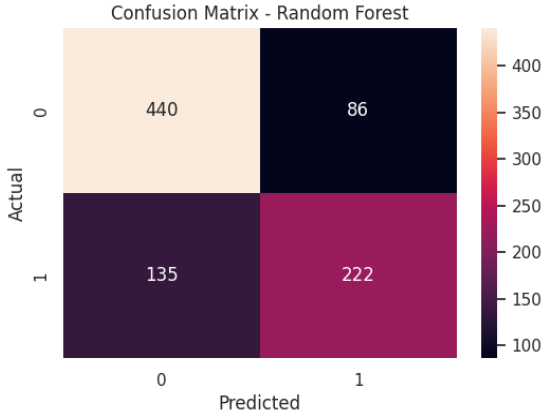


Fig 3: Model Architecture.

VI. MODELS AND MATERIALS

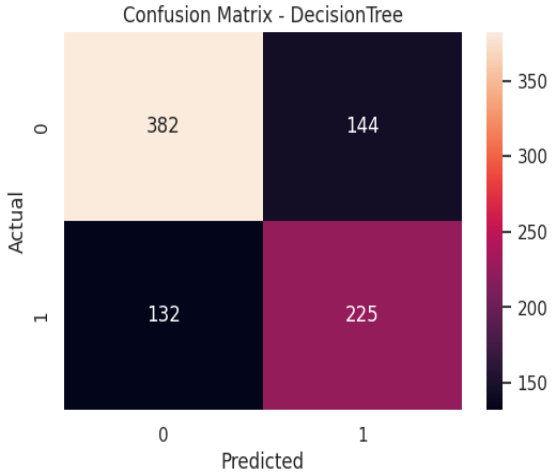
In this study, a comprehensive approach to machine learning model evaluation and comparison is presented for the classification of medical data [28]. Initially, the dataset is divided into features and the target variable 'Result', followed by a stratified train-test split to ensure representative data distribution. The dataset is inspected to ascertain its dimensions and the types of features present, distinguishing between numerical and categorical variables. Subsequently, the categorical feature 'SEX' is removed from both the training and testing datasets.
A variety of classification models are then employed, encompassing Random Forest, Decision Tree, K-Nearest Neighbors (KNN), Multilayer Perceptron (MLP), AdaBoost, and XGBoost classifiers. Each model is trained on the training data and evaluated on the testing data. Performance metrics including confusion matrices and classification reports are generated to assess the predictive capabilities of each model. Notably, the accuracy of each model is calculated and stored for subsequent comparison.



Classification Report:

	precision	recall	f1-score	support
0	0.77	0.84	0.80	526
1	0.72	0.62	0.67	357
accuracy			0.75	883
macro avg	0.74	0.73	0.73	883
weighted avg	0.75	0.75	0.75	883

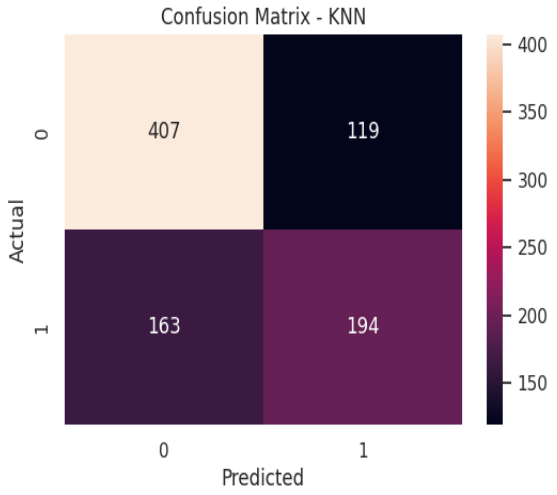
Plot 1: RF & it's Output



Classification Report:

	precision	recall	f1-score	support
0	0.74	0.73	0.73	526
1	0.61	0.63	0.62	357
accuracy			0.69	883
macro avg	0.68	0.68	0.68	883
weighted avg	0.69	0.69	0.69	883

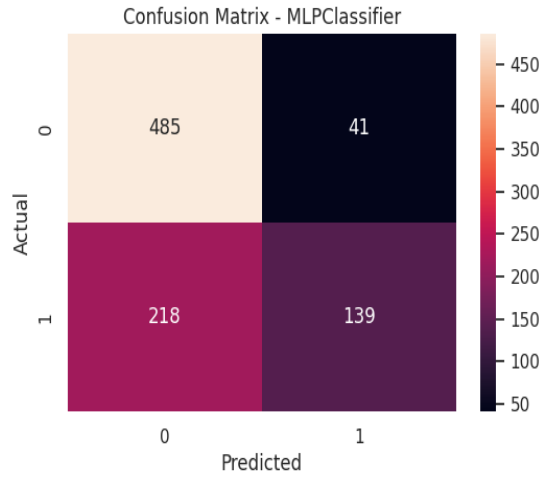
Plot 2: Decision Tree & it's Output



Classification Report:

	precision	recall	f1-score	support
0	0.71	0.77	0.74	526
1	0.62	0.54	0.58	357
accuracy			0.68	883
macro avg	0.67	0.66	0.66	883
weighted avg	0.68	0.68	0.68	883

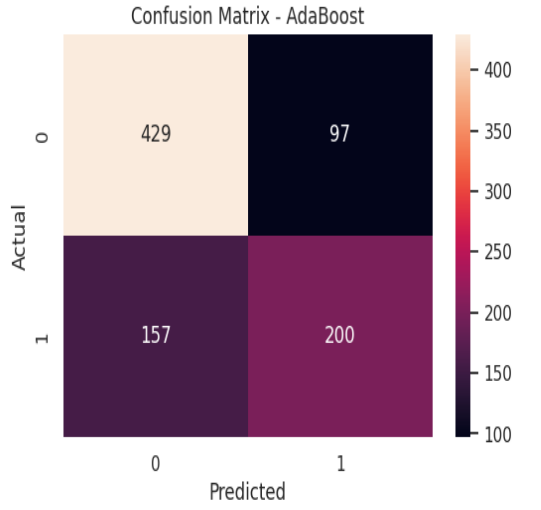
Plot 3: KNN & it's Output



Classification Report:

	precision	recall	f1-score	support
0	0.69	0.92	0.79	526
1	0.77	0.39	0.52	357
accuracy			0.71	883
macro avg	0.73	0.66	0.65	883
weighted avg	0.72	0.71	0.68	883

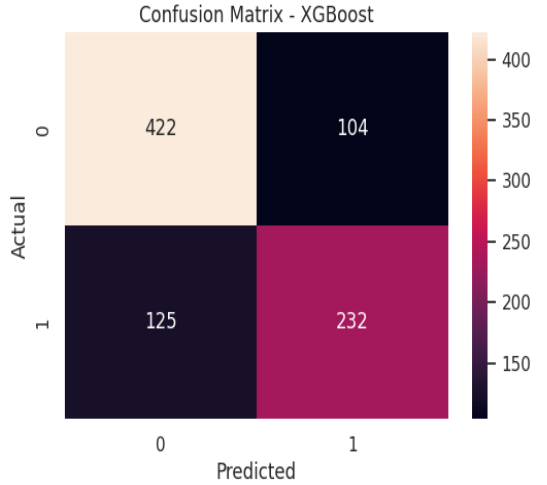
Plot 4: MLP & it's Output



Classification Report:

	precision	recall	f1-score	support
0	0.73	0.82	0.77	526
1	0.67	0.56	0.61	357
accuracy			0.71	883
macro avg	0.70	0.69	0.69	883
weighted avg	0.71	0.71	0.71	883

Plot 5: Ada-B & it's Output



Classification Report:

	precision	recall	f1-score	support
0	0.77	0.80	0.79	526
1	0.69	0.65	0.67	357
accuracy			0.74	883
macro avg	0.73	0.73	0.73	883
weighted avg	0.74	0.74	0.74	883

Plot 6: XGB & it's Output

Furthermore, the best-performing classifier is identified based on its achieved accuracy. The accuracies of all classifiers are visualized using a bar plot, facilitating a comparative analysis of their performance. The plot showcases the accuracy scores of each classifier, allowing for easy interpretation and comparison. The study concludes by highlighting the best-performing classifier and its corresponding accuracy, providing valuable insights into the effectiveness of different classification algorithms for the task of medical data classification

[29].

Table 2: Comparison table for all the Models

MODEL(S)	**ACCURACY**
RANDOM FOREST	0.7497168742921857 *[highest accuracy]*
DECISION TREE	0.6874292185730464
KNN	0.6806342015855039
MLP-CLASSIFIER	0.7066817667044167
ADA-BOOST	0.7123442808607021
XG-BOOST	0.7406568516421291

VII. DATASET DESCRIPTION

In this study, we conducted a comprehensive analysis of various machine learning classifiers to predict medical outcomes using a dataset obtained from clinics in New York City. The dataset, titled "Patient Treatment Classification," encompasses comprehensive patient details, spanning 11 columns from the patient's age and gender to their complete lipid profile. Comprising both numerical and categorical features, the dataset contains a total of 10 features, including demographic information such as age and gender, alongside clinical indicators. Structured as both a .csv file and a .docx file, the dataset provides flexibility in data exploration. While the .csv file contains tabular data, the .docx file likely offers additional contextual or descriptive information. With a size of approximately 77 kilobytes, the dataset facilitates efficient handling and analysis within the scope of this research. The dataset comprises 4412 rows and 11 columns, with 10 features utilized for analysis. Among these features, 9 are numerical, and 1 is categorical. To ensure balanced representation, the 'SEX' column, being categorical in nature, is removed before splitting the dataset into training and testing sets using a stratified approach.

VIII. RESULT &DISCUSSION

The classifier exhibiting the highest performance in this study is the Random Forest, achieving an accuracy of 0.75. The graphical representation of classifier accuracies is presented, where a bar plot depicts the accuracy scores of different classifiers. It is crucial to note that a Future Warning is generated, indicating that the passing of palette without assigning hue is deprecated. The recommended approach involves assigning the x variable to hue and setting legend=False for equivalent functionality. This graphical visualization aids in the comparison of classifier performances, providing a clear illustration of the Random Forest's superiority in accuracy among the evaluated models.

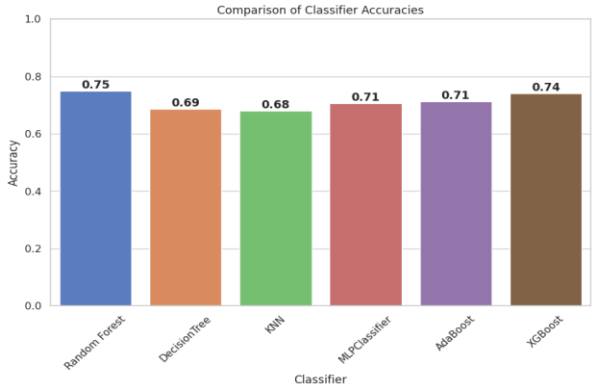


Fig 4: Comparative graph Plot to detect high accuracy.

The graph illustrates the effect of adding differential privacy noise to patient data in Electronic Medical Records (EMR) when using a Recurrent Neural Network (RNN) model. As shown:

Without Noise: The accuracy improves and stabilizes as the number of epochs increases, depicting typical learning behavior in neural network training.

With Noise: The introduction of noise simulating differential privacy mechanisms results in a general decrease in accuracy over the same number of epochs, reflecting the trade-off between privacy and performance.

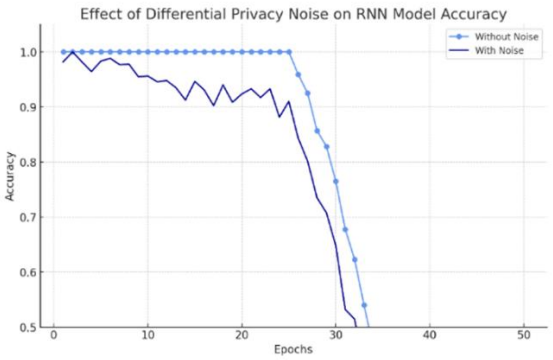


Fig 5: Representation of Data with and without Noise addition.

IX. ADDITION OF NOISE TO THE MODEL FOR DATA PRIVACY

To describe the process of enhancing EMR privacy using differential privacy and a Recurrent Neural Network (RNN) model mathematically, we can break down the steps into several key equations and definitions:

1. INPUT DATA REPRESENTATION

Let X represent the original patient data matrix, where each row corresponds to a patient's record and each column corresponds to a different attribute of the data.

2. DIFFERENTIAL PRIVACY MECHANISM

Differential privacy involves adding noise to the data to mask individual contributions while allowing statistical analysis of the dataset. Let M(X) be the mechanism that applies differential privacy:

$M(X) = X + \text{Laplace}(\Delta f/\epsilon)$

Where:

- Laplace $(\Delta f/\epsilon)$ represents the noise added to each entry of X, drawn from a Laplace distribution centred at zero with scale $\Delta f/\epsilon$.
- Δf is the sensitivity of the function f being computed, which measures the maximum change in f that any single individual's data can have.
- ϵ is the privacy budget, a parameter that controls the trade-off between privacy and accuracy.

3. RECURRENT NEURAL NETWORK (RNN) MODEL

The RNN takes the noise-added data M(X) and processes it over time to model temporal dependencies and produce an output Y.

The RNN function can be represented as:

$Y\,t = \sigma\,(W \cdot h\,t-1 + U \cdot xt + b)$

where:

- xt is the input at time step t (a row from M(X)).
- ht−1 is the hidden state from the previous time step.
- W and U are weight matrices for the hidden state and input, respectively.
- b is a bias vector
- σ is a non-linear activation function, commonly the sigmoid or tan function.

4. Output Data

The final output Y represents the processed, privacy-enhanced EMR data that can be used for further analysis or decision-making.

- Final Expression

Combining these steps, the complete process can be succinctly described by the transformation from X to Y through the differential privacy mechanism and the RNN model:

$Y = \text{RNN}(M(X))$

In this study, a recurrent neural network (RNN) architecture, specifically utilizing the Simple-RNN layer, is employed for the classification of medical data, focusing on the prediction of a binary outcome denoted as 'Result.' The dataset, sourced from New York City clinics, is pre-processed by extracting relevant features and partitioned into training and testing sets. The input data is reshaped to meet the RNN input format, with the model architecture comprising a Simple-RNN layer with 64 units, followed by two densely connected hidden layers with 32 units each, all employing the rectified linear unit (ReLU) activation function. The final layer employs the sigmoid activation function to output binary predictions. The model is compiled using stochastic gradient descent (SGD) as the optimizer, binary cross entropy as the loss function, and accuracy as the evaluation metric. The training process involves 320 epochs with a batch size of 32, and the model's performance is evaluated on the test set. The achieved accuracy and loss metrics, along with the model summary, contribute to a comprehensive understanding of the RNN-based classification approach for medical data.

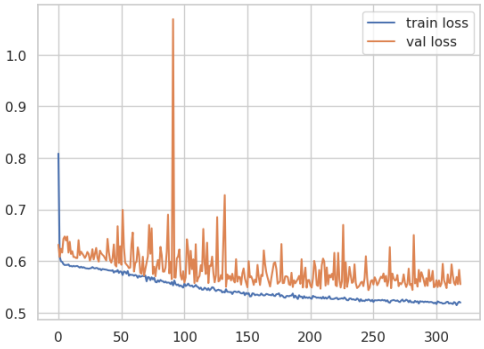


Fig 6: Addition of Noise in EHR using input to hidden layer of RNN.

This work in Fig. 6 represents, a sequential neural network architecture is implemented for medical data classification, as evidenced by the model summary presented below. The architecture consists of a Simple-RNN layer with 64 units, followed by two densely connected hidden layers, each comprising 32 units. The output layer, utilizing a sigmoid activation function, produces binary predictions. The model's parameters, totalling 7393 (28.88 KB), are non-trainable, and the entire model is trainable. The training process involves 320 epochs, during which the model is iteratively refined using stochastic gradient descent. The observed test accuracy at the conclusion of training is reported as 0.7157418. This comprehensive model summary and performance evaluation contribute essential insights into the effectiveness of the proposed neural network architecture for medical data classification.

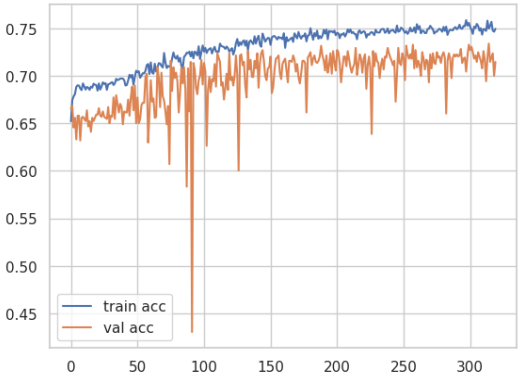


Fig 7: Addition of Noise in EHR using hidden to output layer of RNN.

In the above graph plot Fig. 7, the training and validation accuracies of the implemented model are visualized for comprehensive analysis and interpretation. The plot depicts the evolution of accuracy metrics over the training epochs, with the training accuracy represented by the 'train acc' curve and the validation accuracy denoted by the 'val acc' curve. The legend provides clarity regarding the identification of each curve. This graphical representation serves as a valuable tool for assessing the model's performance throughout the training process, aiding in the evaluation of its learning dynamics and potential over fitting or under fitting tendencies. Such visualizations contribute to a holistic understanding of the model's behavior and efficacy in the context of the medical data classification task undertaken in this research.

X. CONCLUSION

Our study has developed a Recurrent Neural Network (RNN)-based methodology for predicting patient outcomes, significantly enhancing data privacy using Differential Privacy on Electronic Health Records (EHR). This approach has provided profound insights into the convergence of predictive modelling and privacy management in healthcare. Our exploration into sophisticated privacy techniques, including but not limited to Differential Privacy, underscores the essential need to bolster data protection concurrently with maintaining accuracy in predictions. The advancements in RNN optimization highlight the critical role of refining these models to handle the vast scales of EHR data efficiently. Moreover, enhancing model explainability remains pivotal, as it ensures that healthcare providers can understand and trust the predictive outputs, which is vital for informed decision-making.

The inclusion of longitudinal analysis in our studies introduces a crucial temporal aspect to predicting patient outcomes, accommodating the variable nature of patient health over time. The adaptive features of our privacy techniques offer resilience against the changing dynamics of healthcare data environments. Furthermore, our research paves the way for applying these methods across various healthcare contexts, promising a robust,

adaptable, and ethically responsible predictive modelling framework.

XI FUTURE RESEARCH DIRECTIONS

Building on our findings, future research should explore several promising paths. Expanding privacy protections beyond the scope of Differential Privacy to include advanced cryptographic methods such as homomorphism encryption or federated learning could offer stronger safeguards without compromising the accuracy of predictions. There is also a pressing need to focus on the optimization of RNNs, particularly in improving the algorithms used for training these networks to ensure they are both efficient and scalable when applied to extensive EHR datasets.

Prioritizing the explainability of these models is essential for clinician acceptance and trust, necessitating the development of new methods that can provide clear, understandable explanations of model decisions. Furthermore, extending this research to include longitudinal predictions will enhance the models' ability to capture and utilize the temporal dynamics inherent in patient data effectively. Investigating the adaptability of our RNN-based approach and privacy frameworks to diverse healthcare situations and broader applications remains a vital future task. This will ensure that our predictive models are versatile and ethically sound, suitable for a wide array of healthcare environments.

REFERENCES

[1] Boll, H. O., Amirahmadi, A., Ghazani, M. M., de Morais, W. O., de Freitas, E. P., Soliman, A., & Recamonde-Mendoza, M. (2024). Graph neural networks for clinical risk prediction based on electronic health records: A survey. Journal of Biomedical Informatics, 104616.

[2] Si, Y., Du, J., Li, Z., Jiang, X., Miller, T., Wang, F., & Roberts, K. (2021). Deep representation learning of patient data from Electronic Health Records (EHR): A systematic review. Journal of biomedical informatics, 115, 103671.

[3] Zala, K., Thakkar, H. K., Dholakia, N., Shukla, M., & Thumar, D. (2024). Designing an Attribute-Based Encryption Scheme with an Enhanced Anonymity Model for Privacy Protection in E-Health. SN Computer Science, 5(2), 203.

[4] Fu, S., Leung, L. Y., Raulli, A. O., Kallmes, D. F., Kinsman, K. A., Nelson, K. B., & Liu, H. (2020). Assessment of the impact of EHR heterogeneity for clinical research through a case study of silent brain infarction. BMC medical informatics and decision making, 20, 1-12.

[5] Xie, F., Yuan, H., Ning, Y., Ong, M. E. H., Feng, M., Hsu, W., & Liu, N. (2022). Deep learning for temporal data representation in electronic health records: A systematic review of challenges and methodologies. Journal of biomedical informatics, 126, 103980.

[6] Ahmed, S. F., Alam, M. S. B., Hassan, M., Rozbu, M. R., Ishtiak, T., Rafa, N., & Gandomi, A. H. (2023). Deep learning modelling techniques: current progress, applications, advantages, and challenges. Artificial Intelligence Review, 56(11), 13521-13617.

[7] Achanta, S., & Gangashetty, S. V. (2017). Deep Elman recurrent neural networks for statistical parametric speech synthesis. Speech Communication, 93, 31-42.

[8] Choi, E., Bahadori, M. T., Schuetz, A., Stewart, W. F., & Sun, J. (2016, December). Doctor ai: Predicting clinical events via recurrent neural networks. In Machine learning for healthcare conference (pp. 301-318). PMLR.

[9] Wu, S., Liu, S., Sohn, S., Moon, S., Wi, C. I., Juhn, Y., & Liu, H. (2018). Modeling asynchronous event sequences with RNNs. Journal of biomedical informatics, 83, 167-177.

[10] Shi, X., Hu, Y., Zhang, Y., Li, W., Hao, Y., Alelaiwi, A., & Hossain, M. S. (2016). Multiple disease risk assessment with uniform model based on medical clinical notes. Ieee Access, 4, 7074-7083.

[11] Farzi, S., Kianian, S., & Rastkhadive, I. (2017, August). Diagnosis of attention deficit hyperactivity disorder using deep belief network based on greedy approach. In 2017 5th International symposium on computational and business intelligence (ISCBI) (pp. 96-99). IEEE.

[12] Hwang, U., Choi, S., Lee, H. B., & Yoon, S. (2017). Adversarial training for disease prediction from electronic health records with missing data. arXiv preprint arXiv:1711.04126.

[13] Jorge, A., Castro, V. M., Barnado, A., Gainer, V., Hong, C., Cai, T., ... & Feldman, C. H. (2019, August). Identifying lupus patients in electronic health records: development and validation of machine learning algorithms and application of rule-based algorithms. In Seminars in arthritis and rheumatism (Vol. 49, No. 1, pp. 84-90). WB Saunders.

[14] Sun, Y., & Zhang, D. (2019). Diagnosis and analysis of diabetic retinopathy based on electronic health records. Ieee Access, 7, 86115-86120.

[15] Al-Aidaroos, K., Bakar, A. A., & Othman, Z. (2012). Medical data classification with Naive Bayes approach. Information Technology Journal, 11(9), 1166-1174.

[16] Zhang, X., Xiao, J., & Gu, F. (2019, April). Applying support vector machine to electronic health records for cancer classification. In 2019 Spring Simulation Conference (SpringSim) (pp. 1-9). IEEE.

[17] Azeri, N., Hioual, O., & Hioual, O. (2024). A distributed intelligence framework for enhancing resilience and data privacy in dynamic cyber-physical systems. Cluster Computing, 1-16.

[18] Sheikhalishahi, S., Bhattacharyya, A., Celi, L. A., & Osmani, V. (2023). An interpretable deep learning model for time-series electronic health records: Case study of delirium prediction in critical care. Artificial Intelligence in Medicine, 144, 102659.

[19] Shickel, B., Tighe, P. J., Bihorac, A., & Rashidi, P. (2017). Deep EHR: a survey of recent advances in deep learning techniques for electronic health record (EHR) analysis. IEEE journal of biomedical and health informatics, 22(5), 1589-1604.

[20] Asha, A., Arunachalam, R., Poonguzhali, I., Urooj, S., & Alelyani, S. (2023). Optimized RNN-based performance

prediction of IoT and WSN-oriented smart city application using improved honey badger algorithm. Measurement, 210, 112505.
[21] Si, Y., Du, J., Li, Z., Jiang, X., Miller, T., Wang, F., & Roberts, K. (2021). Deep representation learning of patient data from Electronic Health Records (EHR): A systematic review. Journal of biomedical informatics, 115, 103671.
[22] Wells, B. J., Chagin, K. M., Nowacki, A. S., & Kattan, M. W. (2013). Strategies for handling missing data in electronic health record derived data. Egems, 1(3).
[23] Carson, N. J., Mullin, B., Sanchez, M. J., Lu, F., Yang, K., Menezes, M., & Cook, B. L. (2019). Identification of suicidal behavior among psychiatrically hospitalized adolescents using natural language processing and machine learning of electronic health records. PloS one, 14(2), e0211116.
[24] Ying, Z., Bourgeois, D., You, J., Zitnik, M., & Leskovec, J. (2019). Gnnexplainer: Generating explanations for graph neural networks. Advances in neural information processing systems, 32.
[25] Zhao, Q., Li, J., Zhao, L., & Zhu, Z. (2022). Knowledge guided feature aggregation for the prediction of chronic obstructive pulmonary disease with Chinese EMRs. IEEE/ACM Transactions on Computational Biology and Bioinformatics.
[26] Jayasekera, S. P., & Kalansooriya, L. P. (2024). A Comprehensive Review of Methods Used for Health Prediction and Monitoring Utilizing an Electronic Medical Records (EMR) System. EDITORIAL COMMITTEE, 50.
[27] Alkureishi, M. A., Lee, W. W., Webb, S., & Arora, V. (2018). Integrating patient-centered electronic health record communication training into resident onboarding: curriculum development and post-implementation survey among housestaff. JMIR Medical Education, 4(1), e8976.
[28] Yu, C. S., Lin, Y. J., Lin, C. H., Lin, S. Y., Wu, J. L., & Chang, S. S. (2020). Development of an online health care assessment for preventive medicine: a machine learning approach. Journal of medical Internet research, 22(6), e18585.
[29] Jamaluddin, M., & Wibawa, A. D. (2021, September). Patient diagnosis classification based on electronic medical record using text mining and support vector machine. In 2021 International Seminar on Application for Technology of Information and Communication (iSemantic) (pp. 243-248). IEEE.
[30] Nigo, M., Tran, H. T. N., Xie, Z., Feng, H., Mao, B., Rasmy, L., & Zhi, D. (2022). PK-RNN-V E: A deep learning model approach to vancomycin therapeutic drug monitoring using electronic health record data. Journal of Biomedical Informatics, 133, 104166.
[31] Priyanga, P., Pattankar, V. V., & Sridevi, S. (2021). A hybrid recurrent neural network-logistic chaos-based whale optimization framework for heart disease prediction with electronic health records. Computational Intelligence, 37(1), 315-343.