INFORMATION SECURITY PROJECT

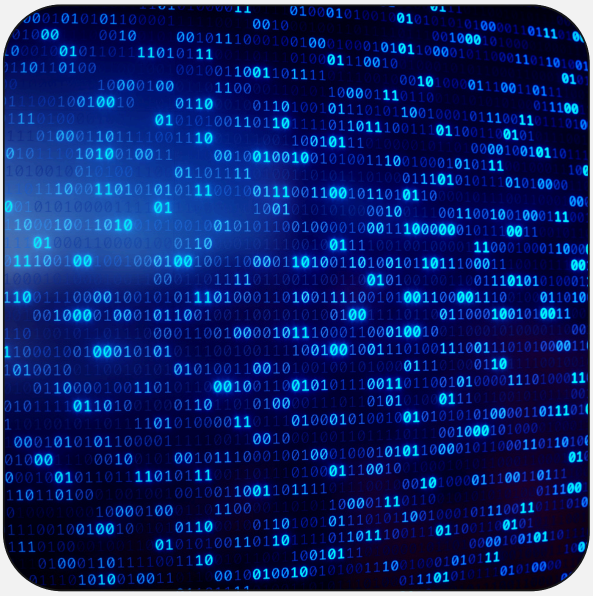
Prepared By : Saleh Ahmad, Aman Shah, Ahmad Raza Toor

TABLE OF CONTENTS

INTRODUCTION TO DATASET

In the field of medicine, the smooth combination of healthcare with technology has boosted our knowledge of various health conditions that have led to more accurate diagnostics and treatments. On the one hand, this digital revolution is bringing the issue of patient privacy and the integrity of electronic medical records. To tackle these issues, we offer a systematically designed dataset, which is suitable for learning and is tailored for conceptual information security projects.

This dataset covers numerous heath indicators derived from the blood analysis obtained through pandemics and is meticulously generated to mimic a real-world situation to be completely confidential and anonymous. Taken together, each feature herein represents significant health measurements that can range from cholesterol levels to blood pressure indices, which are extensively calibrated between 0 and 1 considering the need for a uniform range of analysis.



(CONTINUED)

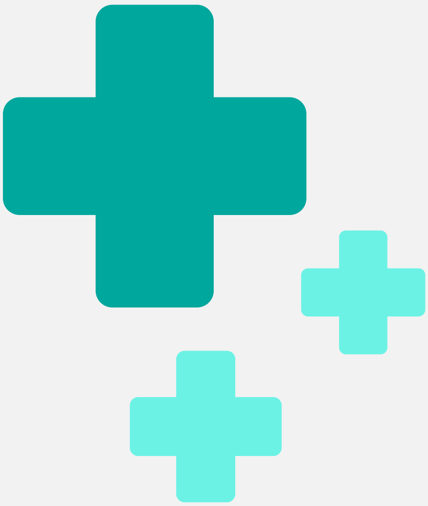
Key parameters include:

- Cholesterol: Showing the level of lipid profile and cardiovascular health.
- Hemoglobin: Demonstrating oxygen capacity carrying feature and blood oxygenation capacity.
- Platelets, White Blood Cells (WBC), and Red Blood Cells (RBC): Providing forensics insights into hematological health and immune function.
- Hematocrit, Mean Corpuscular Volume (MCV), Mean Corpuscular Hemoglobin (MCH), and Mean Corpuscular Hemoglobin Concentration (MCHC): Factors important in analysis of red blood cell shape and function.
- Insulin and BMI (Body Mass Index): Capturing metabolic information and weight status.
- Systolic and Diastolic Blood Pressure: Vital parameters of cardiovascular health and the state of blood vessels.
- Triglycerides, HbA1c (Glycated Hemoglobin), LDL (Low-Density Lipoprotein) Cholesterol, and HDL (High-Density Lipoprotein) Cholesterol: To understand lipid metabolic pathways and glucose control methods.
- ALT (Alanine Aminotransferase) and AST (Aspartate Aminotransferase): Liver enzymatic markers.
- Heart Rate, Creatinine, Troponin, and C-reactive Protein (CRP): Identifying the cardiac and renal situation as well as the inflammatory status through a comprehensive assessment.

(CONTINUED)

Our dataset is complemented by a binary characteristic, 'Disease', which is used to identify the presence of an ailment or a clean bill of health of an individual. This structured data allows data scientists to perform exploratory analysis, predictive modeling, and creating resilient algorithms for disease mitigation and prognosis.

The collection of such data is extremely important for the development of secure protocols, especially in the healthcare domain where data confidentiality and integrity plays a key role. We, therefore, intend to explore the technical side of health informatics and cybersecurity with a focus on developing the strategies and instruments that are necessary for the preservation of sensitive medical data as well as predictive analytics and disease management.



RELATED WORK

This particular dataset is proving to be a robust subject of research in the data science field, as it features on Kaggle's website with more than 1.5k downloads. Diverse scholars and experts have worked with this dataset and using its numerous intriguing features to accomplish various healthcare analytics and predictive medical tasks.

An elaborate survey of similar works reveals a varied set of mechanisms that exist for predictive modeling with classes that either are trained from scratch or use sophisticated pretrained neural networks. These strategies can bring very good results, having reported accuracies varying from 25% to 55%, which are not a surprise because prediction related to diseases is a very complex task and there are a number of aspects to it like feature extraction and model optimization.

Researchers have traversed this niche and made an effort to stretch the limits of existing approaches while exploring uncharted algorithmic paradigms and resourceful design methods. Solutions to this issue include ensemble learning, feature selection, and data augmentation as ways to strengthen the model robustness and generalizability which, in turn, allow for refinement by offering avenues for further improvement in predictive performance.

(CONTINUED)

On top of that, using transfer learning and Domain adaptation techniques is the effective methodology in that the knowledge acquired from related tasks or domains are needed to assist in model training on the given dataset. Hereby, researchers have exploited transfer learning and fine-tuning of the pretrained models on health dataset so that they can take the advantage of the wealth information contained in the diverse data sources, which in turn result in enhancement of the discriminative power and accuracy of the models.

Further, the integration of interpretability and explainability principles in disease prediction platforms is in great demand and it assists in clarifying the decision making process and selects the feature importance. Techniques like those of SHAP (SHapley Additive exPlanations) values, LIME (Local Interpretable Model-agnostic Explanations), and attention mechanisms, have been utilized to unpack the secret codes and relationships within the data, which Goals and Objectives:

Integrating all of the related work gives us a complete picture about a remarkable research community of an area related to health informatics and predictive analytics. We expect more work to be done in the future with the focus remaining on how data science and health care can work together in a synergy as a powerful tool to solving medical problems like disease diagnosis and treatment.

SECURITY ALGORHITHM

Security in this project depends on the use of RSA Encryption, a novel cryptographic method aimed at carrying out computations on encrypted data without decryption. This system is therefore designed to protect the privacy of the model parameters while making it possible to carry out distributed model training across various entities.

Client-side Training: First of all, individual client models are trained on their individual datasets in a decentralized way which helps in data privacy and data sovereignty. Every client providing local data is used to update the model parameters, protecting the privacy of sensitive health information by doing so.

Encryption of Model Parameters: Hence, the trained model parameters are encrypted with RSA Encryption and transmitted to the central server. Throughout this process of encryption, the model weights will be made unintelligible to any unauthorized parties, which protects the data from disclosure and security assault.

Secure Aggregation on Server: Upon getting the encrypted model parameters from the clients, the central server applies the secure aggregation operations through the RSA Encryption technique. This allows the server to compute aggregate statistics or model updates without the need for the decryption of the components of individual contributions, preserving the confidentiality and privacy of the users.

Transmission of Averaged Model Parameters: After the aggregation process is completed the averaged model parameters are encrypted and transmitted back to the corresponding clients. Homomorphic encryption encryption ensures that the transmitted aggregate model is protected so that the risk of interception or tampering by malicious actors in the transmission process is eliminated.

Decryption and Update on Client-side: Since the clients receive the averaged model parameters, they decrypt the encrypted data using their respective decryption keys. This way, they will be able to update their local models with the averaged models parameters which will help them become part of the collaborative knowledge exchange while they do not compromise on data privacy and security.

(CONTINUED)

Decryption and Update on Client-side: Since the clients receive the averaged model parameters, they decrypt the encrypted data using their respective decryption keys. This way, they will be able to update their local models with the averaged models parameters which will help them become part of the collaborative knowledge exchange while they do not compromise on data privacy and security.

The security algorithm that is proposed utilizes RSA Encryption to achieve secure aggregation and collaboration between distributed entities in a seamless manner, and it also helps in protecting the data privacy and confidentiality of participants. This novel architecture not only enables secure, joint model training in healthcare situations but, in so doing, places cryptography in the spotlight as an effective way of addressing the challenges posed by data sharing in the data-driven domains.

ML / DL ALGORHITHM

The finished deep learning model for this project was a specific type of feedforward neural network which is also called vanilla feedforward architecture. While the feedforward networks in standard fashion are distinguished by a fixed architecture; the architecture of the model proposed is flexible and is dynamically equipped with a number of layers and neurons. As a result, however, it makes the developer's projects more dynamic, which in turn allows them to experiment with data complexity and different network models without jeopardizing the project's functionality.

Feedforward Structure: We use a feedforward model as the network's architecture because the input flows sequentially from the input layers to the output layers of the network. This architecture does the job of feature extraction and decision-making without the requirement of feedback loops and recurrent connections which cut out the need of feedback loops and recurrent connections.

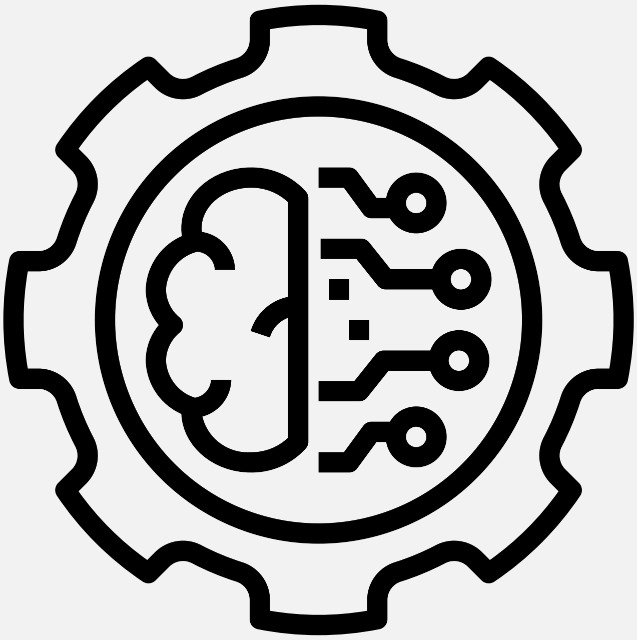
Dynamic Architecture: The distinguishing feature of the model is its adaptable architecture that implies the number of layers as well as the number of neurons to be changed dynamically without any performance degradation. This flexibility helps researchers and practitioners to identify the specific part of the network which can be changed so that it suits the feature of the dataset and hence is able to deliver optimal performance.

Activation Layers: The attributable features include a set of activation layers that introduce non-linearity into the neural network and enable it to learn the complex nature of characters and the features of the input data. Neuron transfer functions are commonly assumed to fall into one of three categories: ReLU (Rectified Linear Unit), sigmoid or tanh functions which are applied to inputs to create non-linearities and subsequently facilitate feature transformation and extraction.

(CONTINUED)

Softmax Layer: At the output of the network we usually apply a softmax layer that normalizes the outputs across multiple classes so that we obtain a probability distribution with respective to all the available classes. This guarantees that the model's predicted probability values sum up to 1, thus the result is easy to read and also can be used for classification.

Ultimately, this complexified feedforward network, with its layers of adjustable neurons, activation functions, and softmax layer, provides a strong asset to many deep learning and machine learning tasks. Such adaptability and scalability makes it versatile weapon, which can be applied to classification and regression, natural language processing or computer vision. Also, the architecture the dynamics which goes firmly and harmoniously with the shifting condition of data science and deep learning research, makes it more innovative and exciting for the area.



MODEL PERFORMANCE

We compared the results by executing multiple clients in parallel and evaluating the before and after aggregation i.e. the server aggregates and averages the weights of all the client models and returns the same state to each of the clients performance of the individual models

# Client	Accuracy (%)		Precision (%)		Recall (%)		F1 (%)	
Aggregation	Before	After	Before	After	Before	After	Before	After
Client 1	21	61	25	51	30	52	29	53
Client 2	20	59	29	55	35	59	31	50
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮