

AI-based Pneumonia Diagnosis System with Zero Trust Security



Session: 2022 – 2026

Submitted by:

Abu Bakar Sajid	2022-CS-125
Mohammad Abdullah	2022-CS-155

Submitted to:

Mr. Waqas Ali

Department of Computer Science
University of Engineering and Technology
Lahore Pakistan

Table of Contents

1. Abstract.....3

2. Introduction3

3. Problem Statement.....3

4. Objective.....4

5. Scope4

6. Existing Systems.....5

7. Literature Review5

8. Key Functionality6

9. Methodology.....7

8. System Architecture7

9. Tech Stack8

10. Operational Workflow8

11. Security Threats and Zero Trust Solutions9

12. Implementation 10

13. Test Results and Evaluation 14

14. Recommendations for Future Deployment..... 15

15. Future Work and Conclusion..... 15

References 15

1. Abstract

This report presents the design and implementation of the pneumonia diagnosis system developed using the zero trust security principles. The system allows the patient to upload the data and then the doctor can look at the image and audio of the patient. The doctor can ask for assistance from the AI model and submit its diagnosis. The system is built with zero trust security principles by multi-factor authentication of the user, role-based access control, least privilege access, protection from file tampering, end-to-end encryption and continuous monitoring. The frontend of the system is built using React.JS, backend is developed in C# ASP.NET Core. MongoDB is used as database and clouinary is used for file storage. Model server is built using TensorFlow and Flask in Python. The evaluation from test results shows good results. This report writes the scope, objectives, methodology, implementation and results from the development of the system to improve the healthcare by securing AI systems in healthcare.

2. Introduction

The project is focused on building a platform for patients to connect with the doctor and gain medical diagnosis from the doctors. The platform will assist the doctors by the provision of automated medical diagnosis using Computer Vision AI. Additionally, platform will be built according to the Zero Trust principles to ensure the safety of medical data from potential cyber-attacks.

Patients will register in the system and then choose the type of diagnosis they want from the doctor and then they will upload their images. The AI model will analyze these images and give its predictions on the diagnosis. These predictions will be provided to the doctor who will review these predictions and the images, who then will generate a final report which will be forwarded to the patient and he/she will be notified through mail. Zero Trust will ensure that most of the attacks will be dealt with to maintain confidentiality, integrity and availability of the system.

The Zero Trust Security strategy will be implemented in the project to safeguard the AI model from different kinds of attacks like adversarial attacks. It is based on the principles of continuous verification and monitoring, LPA (Least Privilege Access) and end-to-end encryption of data. This approach will help in securing the AI model from adversarial attacks.

We will outline the objective, key features, scope of the system, literature review and implementation of zero trust principles in the system in this proposal.

3. Problem Statement

Pneumonia is a common and a fatal disease, especially for children and elders, which requires early detection for effective treatment of the disease. It could lead to prolonged illness and even death. The quick and accurate detection of pneumonia and other diseases could be significant in a timely treatment and minimizing the chances of severe complications and

saving lives of patients through early diagnosis. The early diagnosis of pneumonia should be accessible to everyone but due to the lack of healthcare skilled professionals in the remote areas, patients have limited access to it. Also, the traditional healthcare systems in remote areas lack the skilled diagnostic tools and decision support systems which result in delays and misdiagnosis, which could have been avoided. This creates an urge to develop an accurate and reliable system for quick pneumonia diagnosis. There will be security challenges for the storage and transmission of the patient's data. The patient's data is sensitive and must be protected during storage and transmission.

The platform offers a solution to these problems where the patients can upload their images and audio for diagnosis. A healthcare professional can analyze the data of the patient and can ask for assistance from the machine learning model and then give its final diagnosis and treatment remarks for the patient. The solution will assist the professional by the AI model which will tell him its diagnosis and its confidence in its prediction. The platform will ensure security and data privacy of the patient by integrating zero trust security principles in the system. Security challenges such as data transmission and storage can be mitigated by implementing zero trust principles. AI-driven diagnostics, healthcare professional oversight and zero trust security combine to ensure faster and quality healthcare.

4. Objective

The main objective of the system is to design and develop a secure platform focusing on the detection of pneumonia using chest X-ray images with machine learning models. The system will streamline the process of pneumonia diagnosis between patients and the doctor while also ensuring model and data security using Zero Trust principles. The objectives of the project are listed below.

- Development of a secure system facilitating diagnostic process between patients and doctor.
- Building an AI model to assist in diagnosis of pneumonia.
- Ensuring protection of AI-based system using Zero Trust Security principles.

5. Scope

The proposed system will provide the diagnosis of pneumonia and secure communication between patients and the doctor. The doctor will generate a report with his comments and diagnosis. The system will initially support diagnosis of pneumonia with X-ray images. Patients will be able to self-register into the system and ask for diagnosis. The system will guide the patients about the images to upload. Zero Trust Security principles will authenticate user access, enforcing continuous verification and monitoring, least privilege access, and MFA (Multi-Factor Authentication) for sensitive operations. Zero Trust will also protect the AI model from various attacks like model poisoning, adversarial attacks, etc. The admin can edit the doctor profile. Admin can also monitor the login attempts and API calls. Rate limiting will be applied to prevent the abuse of APIs and RBAC (Role-based Access Control) will be

implemented for implementing LPA. Handling of multiple diagnosis and multiple doctors is currently kept out of scope of the system.

6. Existing Systems

GE Healthcare is an international company that offers diagnostic, treatment and monitoring solutions for healthcare providers. **Thoracic Care Suite** is one of the products of GE Healthcare. It uses AI to help doctors diagnose pneumonia from the x-ray images of patients. The Thoracic Care Suite has its clinical benefits but there are security limitations in it. Lack of Zero Trust implementation, access control measures and end-to-end encryption in the product indicates security vulnerabilities. There is no such mention of zero trust and end-to-end encryption for transmission and storage of the patient's data in the public documentation of GE Healthcare Thoracic Care Suite.

Qure.ai is a health-tech company that specializes in providing medical imaging solutions using AI. **qXR** is a product of Qure.ai which provides chest X-ray analysis for detection of abnormalities including pneumonia in lungs, heart, etc. It lacks implementation of zero trust principles and measures like end-to-end encryption, role-based access control or continuous monitoring. It suggests security potential security vulnerabilities such as adversarial attacks, data privacy breaches in the system.

Although, these products are a great assistance to the doctors and to the patients as well, but the absence of zero trust and security features could result in a dangerous situation. Addition of zero trust principles in the development of AI solutions can create a huge impact in the development of software solutions in medical industry.

7. Literature Review

Pneumonia is an infection of one or both lungs caused by bacteria, viruses or fungi. It could lead to life-long disease if not treated timely. With the rise of artificial intelligence and computer vision, research has been conducted for detection of pneumonia using computer vision and machine learning. We will review key research papers and explore the methodologies used and limitations of each research paper.

Rai et al. [1] presents a comprehensive survey on comparative analysis of machine learning algorithms for pneumonia detection. The aim of the study was to identify optimal machine learning models for pneumonia detection using X-ray of chest images.

Abdullah et al. [2] proposes a CNN model for diagnosis of pneumonia using chest X-ray images. The model achieved accuracy of 90.22% and an AUC score of 0.96. SMOTE technique is used in this study for oversampling to deal with class imbalance. Data augmentation techniques were employed to generalize the model's capability. The model is limited as it misclassified normal cases which can be improved.

This study [3] highlights the economic impact of artificial intelligence in healthcare. It presents an AI-based economic model for diagnosis and treatment. It used a PRISMA paradigm to select relevant AI studies for diagnosis and therapy. The study presents economic models to evaluate the cost-effectiveness of AI in healthcare. It demonstrated that AI lowers healthcare costs when compared to traditional methods.

Najjar et al. [4] reviews the integration of artificial intelligence in radiology and highlight its impact on medical imaging. It discussed the security challenges that are faced in integration of AI applications. It reported that security concerns are yet to be addressed for the nature of AI models. Challenges, limitations and future directions are given in this research paper for medical imaging.

Rajpurkar et al. [5] proposes a 121-layer dense convolutional neural network for detection of pneumonia from chest X-ray images. The model is trained on large scale ChestX-ray14 dataset, which includes over 100,000 frontal-view X-ray images covering 14 different diseases. The model has a f1-score of 0.435. The comparison of CheXNet's performance was limited to only frontal radiographs, which may underestimate the model's effectiveness.

Stokes et al. [6] reviews the existing systems for pneumonia diagnosis with a focus on evaluating their performance and best practices. It reported that several studies did not follow best practices for model development even though high performance was reported. This study is limited to application of machine learning in the recent years.

Yang et al. [7] reviews the role of artificial intelligence in medical imaging for diagnosis of pneumonia. It focuses on application of primary imaging techniques such as chest X-ray. The paper emphasized on collaboration between healthcare professional and AI researchers to improve AI applications.

8. Key Functionality

The system will provide the following functionalities.

1. Patient

- **User Registration & Authentication:** The patient will be able to register and login into the system. MFA will be implemented at login to ensure only verified users can access their accounts.
- **Choose Diagnostic Service:** The patient will choose the diagnostic service they need and upload required images into the system.
- **Receive Report:** Patient will be notified when the doctor completes its diagnosis and receive his/her report.

2. Doctor

- **User Authentication:** Doctor will be able to secure login into the system ensuring only real doctor has access to the system.

- **Doctor Dashboard:** A dashboard which displays the patients and pending cases.
- **Perform AI Diagnosis:** An AI model to assist the doctor in diagnosis.
- **Finalize Report:** The doctor can view patient images and then finalize the diagnostic report and send to the patient.

3. Admin

- **Update Doctor Profile:** Admin will have the rights to update the profile of the doctor.
- **Admin Dashboard:** A dashboard for the admin.
- **Login Request:** Admin can monitor the requests for login.
- **API Monitoring:** Admin can monitor the all the APIs. Each request will be monitored by the admin.

9. Methodology

The following methodology was followed for the development of the system and for the completion of the above-mentioned objectives.

1. **Requirement Gathering:** Analysis of the existing systems and scope of the system.
2. **System Design:** Designed a secure system with zero trust security principles according to the requirements of the system.
3. **Data Collection:** Collected the data from the Kaggle repository of pneumonia Chest X-ray images.
4. **Model Development:** The jupyter notebook of Xray-Vision for pneumonia diagnosis was used for the development of the model.
5. **Backend and Frontend Development:** The system backend and frontend components were developed accordingly to the system design.
6. **Zero Trust Implementation:** Zero Trust security was implemented across the system.
7. **Testing and Evaluation:** Evaluated the results from the system after conducting tests.

8. System Architecture

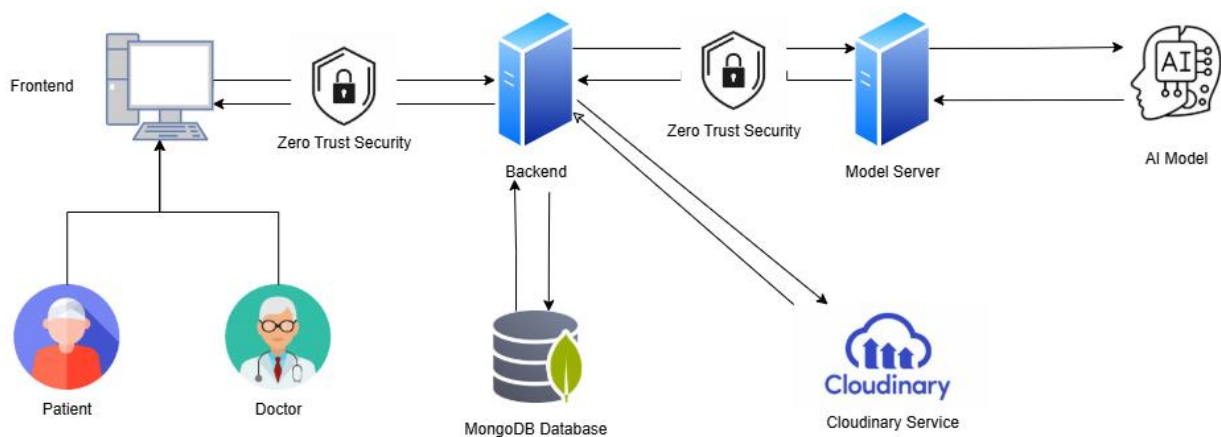
The system architecture of this application is designed to be secure by implementing zero trust security to ensure confidentiality, integrity and availability of the system. It comprises of the frontend, backend, model server, database and supporting service of cloudinary.

The frontend of the system is used for easier interaction with the backend service. The frontend communicates with the backend through APIs which will be secured using zero trust security. Each request will be verified and authenticated through the frontend to improve the overall security of the system. The frontend is built using React.JS.

The backend will be a central hub for the system. The backend is developed in the C# .NET framework. Each request from the frontend will go through the backend and it will be verified and authenticated. The backend will interact with the frontend for responding to the client's requests and interact with the MongoDB database to store and retrieve patient's data and diagnosis from the doctor. AI diagnosis request will be sent to the backend. Server after

authentication of the request will request the model server for AI diagnosis. The cloudinary service will be used for storing audio and video files of patient. Rate limiting will be applied to prevent the abuse of API usage and brute force attacks.

The model server is a server which will be used for employing AI model for diagnostic assistance purposes. It is developed in Flask in Python and the model is developed in TensorFlow. The model will be secured by encryption of the model file. The file will be decrypted when the server will start. The request for the model will verify the signature and integrity of the x-ray image and if verified will preprocess the image to prevent adversarial attacks and then compute the model results and send its response to the backend.



9. Tech Stack

The following tech stack is used for the development of the diagnostic system.

Frontend: React.JS, Tailwind CSS, Redux, JavaScript

Backend: ASP.NET, C#

Database: MongoDB Atlas, Cloudinary (File storage)

Model: Flask, TensorFlow

10. Operational Workflow

The system architecture is designed to support patient data privacy and decision support system for patients and doctor respectively. The system is composed of four main components namely frontend, backend, AI model, database and supporting service like cloudinary.

Patients and doctor will login or register into the system after two-factor authentication. The users will interact with the system thorough frontend with API calls which are secured and the sensitive data that the patient wants to send to the doctor will be end-to-end encrypted. The system will be developed using the zero trust security principles which will ensure that all the requests from doctor and patients will be verified and authorized.

Patient will register into the system using frontend. The password of the user will be stored in the database after encryption to protect it. The patient will be authenticated by verification through OTP sent to the user's email. The user will login into the system using the OTP that will be sent to the user's email each time its password is verified. The patient after registering or logging into the system, will complete its profile and input all the personal details. The patient will then input the symptoms, chest X-ray image and cough audio. The audio and the image will be encrypted to ensure data privacy and secure transmission of the sensitive data. This data will be sent to the backend server which will store them on cloudinary service and store the URLs of the image and audio in the MongoDB database on cloud.

The doctor will login into the system and can view the list of patients. The doctor can diagnose its patients by clicking on the diagnose button which will open a popup showing the image of the selected patient's X-ray, audio, symptoms and personal details of the patient. The doctor can ask for the AI analysis of the image. This image will be sent with a digital signature to ensure that no one has tampered with it in the process of transmission to the model server. The image with the signature will be sent to the backend which will verify and authorize the request and if authorized will send a request to the model server where signature will be verified and if correct then, the model will compute its result on the image and send the response back to the backend where it will be returned to the doctor who can now view the AI analysis. The doctor after receiving AI assistance can make a final decision on whether the patient is diagnosed with pneumonia or not or whether further tests are needed for diagnosis. The doctor will submit its diagnosis.

After the submission of diagnosis, an email notification will be sent to the email of the patient. The patient can login into the system and view the diagnostic report sent by the doctor.

11. Security Threats and Zero Trust Solutions

Security threats were identified during the lifecycle of the system. Following security threats were found in the system.

- **Unauthorized Access:** Attacker can try to access the system as a patient or doctor and can perform unethical actions.
- **Data Leaks:** Patient data such as chest x-ray images and cough audio files could be leaked during storage of these files. The attacker can get the access of these sensitive files. This leads to data privacy violations of GDPR.
- **File Tampering:** The attacker can access the file and tamper it to manipulate the decisions from the AI model.
- **DDoS Attack:** Attacker can send multiple requests to the server to disrupt the services.

Zero Trust Security principles will be implemented into the system in the following manner to mitigate the previously mentioned security risks.

- **Multi-Factor Authentication** will be implemented for secure user authentication for doctor and patients. All users will be verified by an OTP sent to their emails after a successful login.
- **Role-based Access Control (RBAC)** is implemented so the patients can only access their own dashboard, images and reports and not anything else and doctors can access their own dashboard and their services.
- **Least Privilege Access** is implemented so that patients can only access their own data and cannot view other patient's data and doctor cannot access the patient's personal data which is not needed for diagnosis.
- **End-to-end encryption** is applied to the image and audio files.
- **Continuous Monitoring** is conducted by logging all the user actions and taking automated actions by flagging IPs with suspicious behavior.
- **Rate Limiting** is applied to protect the abuse of APIs.
- **Digital Signatures** are used to verify the integrity of the image sent to the model.
- A tiny **Gaussian blur** and slight **Image Rotation** is applied to the image to protect the model from adversarial attacks.

12. Implementation

The system was developed using the tech stack mentioned previously in the report. The key features were implemented and are described. Role-based access control and least privilege access is implemented to ensure that no user is allowed to perform actions outside of their own allowed ones. Rate limiting is applied at the server at each API call.

A secure login and registration module was implemented for user authentication. JWT tokens were used to authenticate the user and for authorization of future user requests. The token is sent to the user after verification of the OTP sent to the email on successful login to ensure two-factor authentication.

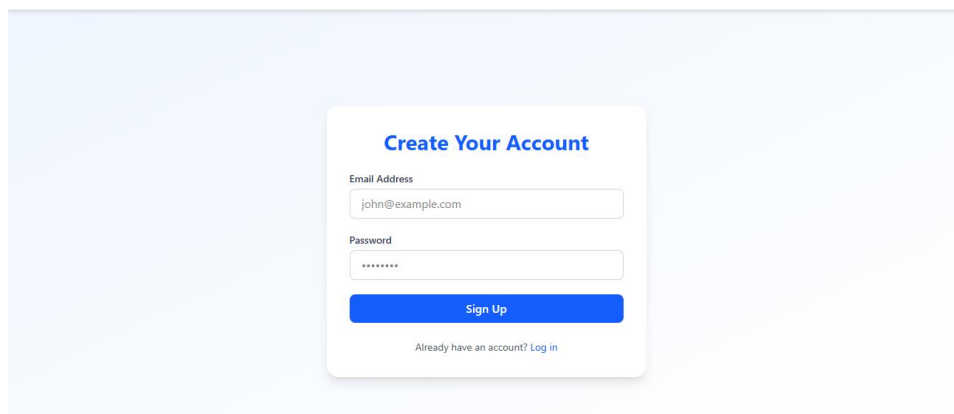


Figure 1. Signup Page

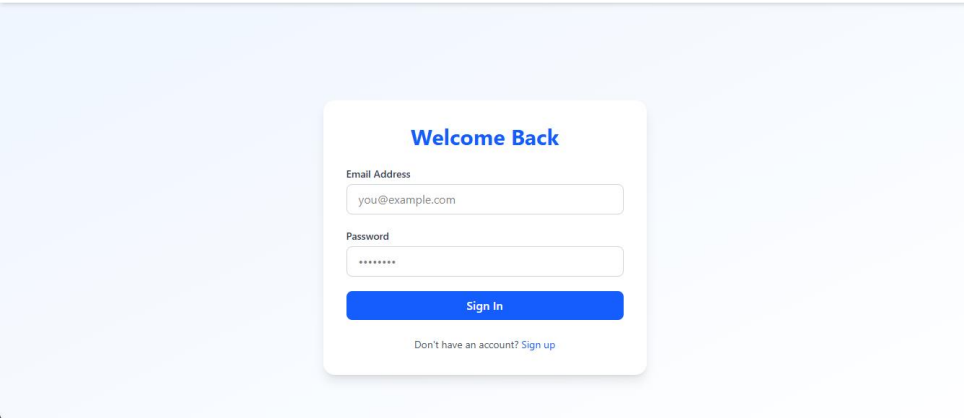


Figure 2. Login Page

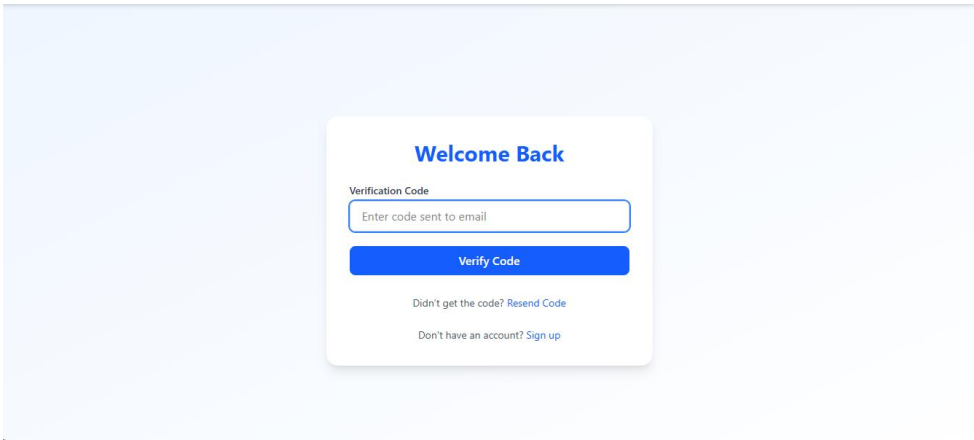


Figure 3. OTP Verification

A dashboard is built for the patient to edit its profile and request for a diagnosis from the medical professional and to view its diagnosis submitted by the doctor. Patient’s files will be encrypted with AES. The key for AES is generated and the key is also encrypted with RSA cryptography and then sent to the backend server which will store these files on cloudinary storage service and store these URLs and AES key on the database. After the submission of diagnosis from the doctor, patient will receive an email notification and then he can view its diagnosis results.

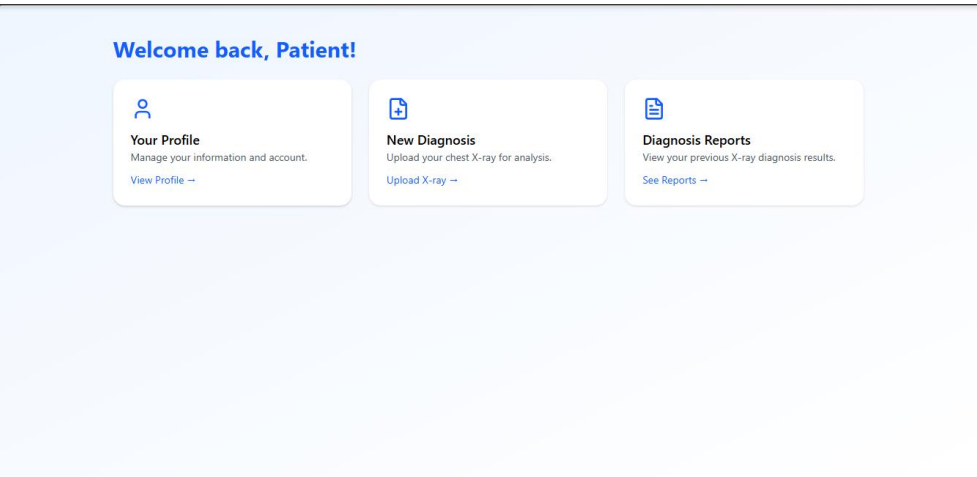


Figure 4. Patient Dashboard

← Back to Dashboard

Start a New Diagnosis

Upload Chest X-ray Image

Choose File pneumonia.jpg

Upload Cough Audio (MP3, 5-10 seconds)

Choose File censor-beep-10sec-8113.mp3

Please record and upload a short 5-10 second MP3 file of your cough.

Symptoms

Slight pain in chest.

Submit for Diagnosis

Figure 5. Patient X-ray and Cough Audio Submission

← Back to Dashboard

Your Diagnosis Reports

Diagnosis Result: No Pneumonia	28/04/2025
Doctor's Remarks: All Good	
Diagnosis Result: Confirmed Pneumonia	28/04/2025
Doctor's Remarks: hello	

Figure 6. Diagnosis Results

Doctor dashboard will allow the doctor to view the list of patients, review pending diagnosis and view the diagnostic reports previously submitted. The doctor can review the pending diagnosis. The files of the patient will be decrypted and then viewed by the doctor which ensures end-to-end encryption. The doctor can click on the diagnose action on the row of desired patient. A popup will appear which will show the decrypted files and the doctor can ask AI model for analysis and then give its remarks and diagnosis and then submit. The request to the AI model will send a digital signature to verify that the file has not been tampered by a man in the middle. This will verify the integrity of the file. The request will be authorized at the backend server and then the backend will request the model server which will verify signature and then respond to the backend which will return the response to the doctor.

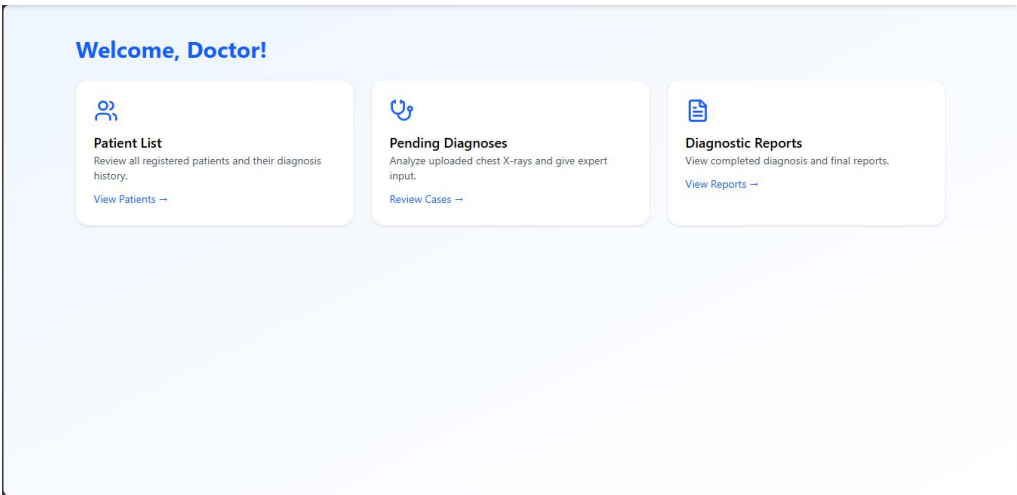


Figure 7. Doctor Dashboard



Figure 8. Pending Diagnosis Requests

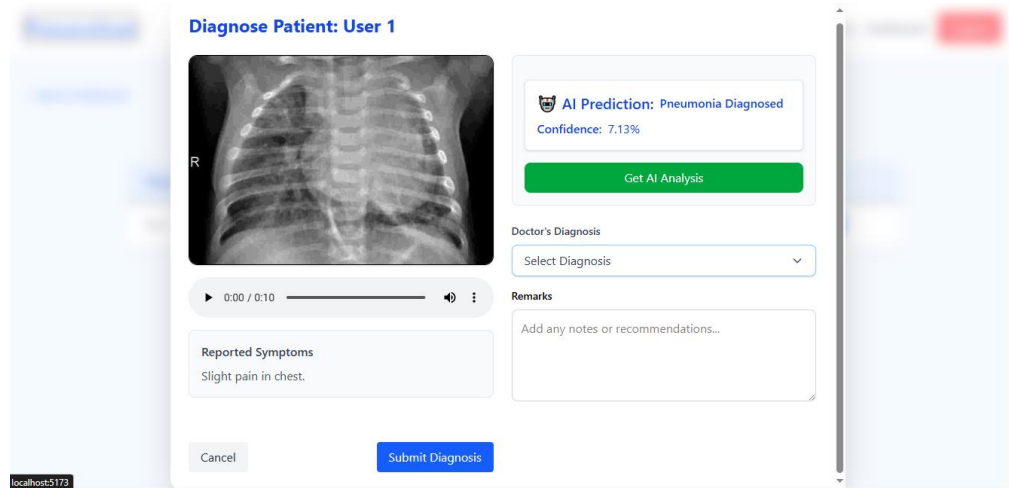


Figure 9. Patient Diagnosis Popup

Admin dashboard is developed for the admin to update the user profile in case of a doctor change. It will allow the admin to monitor the login attempts and the APIs usage. The login attempts will be automatically monitored at the backend server. It will flag those IPs trying to request huge login requests in short time period and then not allow them to login.

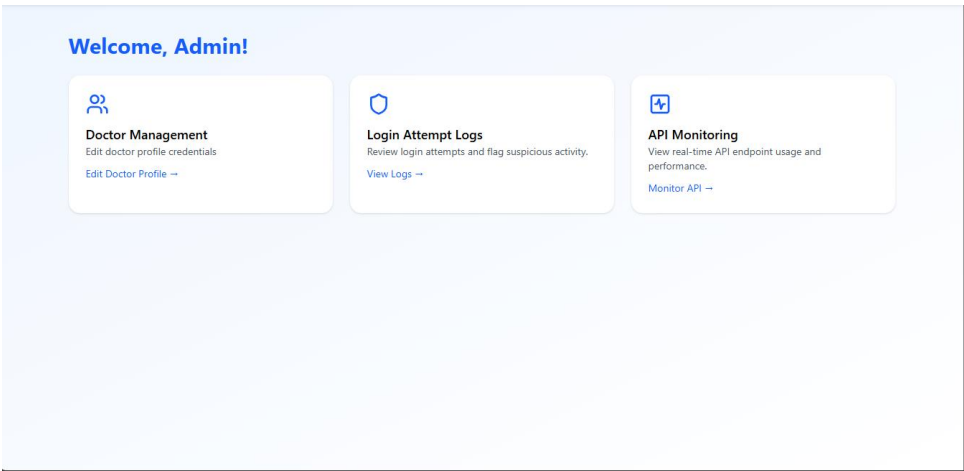


Figure 10. Admin Dashboard

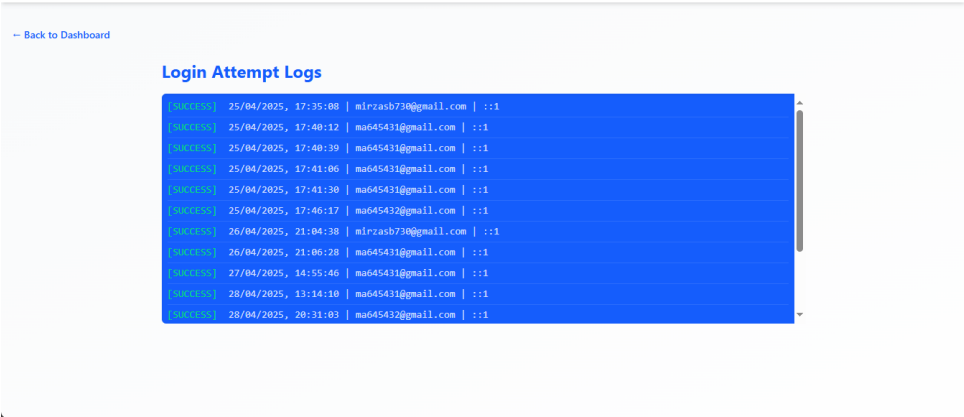


Figure 11. Login Attempts



Figure 12. API Monitoring

13. Test Results and Evaluation

A pre-built model by XRayVision-PneumoniaDetect have been used for this system. The model has shown an accuracy of 0.92 and precision of 0.91 and 0.92 for pneumonia and normal classes respectively. The recall metric for model performance is 0.85 and 0.95 while f1-score is 0.88 and 0.93 for normal and pneumonia respectively. So, the model shows satisfactory performance.

The access control and rate limiting measures have been tested thoroughly and have secured the system. 401 Unauthorized error was returned for trying to access an API for different role from an unauthorized role. Moreover, multiple requests were sent in short time period to the server. The server initially put the requests in the queue and sent response with a delay. These results show that the system have been secured with the zero trust measures.

14. Recommendations for Real-World Deployment

Real world deployment of the system would require the files which are currently stored on the clouinary service, should be stored on the server with better protection. Moreover, the data privacy regulations should be met and implemented into the system.

15. Conclusion and Future Work

The system offers a secure solution to the pneumonia diagnostic systems by implementing zero trust principles into the system to ensure the confidentiality of the patient's data, integrity of the model's input and the availability of the system. The solution has shown a great potential for the future diagnostic and medical platforms. The system can be upgraded to accommodate multiple doctors and multiple diagnosis such as diarrhea, and other diagnostic diseases in the future. This system demonstrates how zero trust can be applied to improve the security and user appraisal.

References

- [1] H. V. M. A. S. S. Devesh Rai, "COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS IN PNEUMONIA DETECTION," 2024.
- [2] S. S. Abdullah Al Foysal, "AI-Driven Pneumonia Diagnosis Using Deep Learning: A Comparative Analysis of CNN Models on Chest X-Ray Images," in *Open Access Library Journal*, 2025.
- [3] N. Khanna, M. Maindarkar, V. Viswanathan, J. Fernandes, S. Paul, M. Bhagawati, P. Ahluwalia, Z. Ruzsa, A. Sharma and Kolluri, "Economics of Artificial Intelligence in Healthcare: Diagnosis vs Treatment," p. 38, 2022.
- [4] R. Najjar, "Redefining Radiology: A Review of Artificial Intelligence Integration in Medical Imaging," in *Diagnostics*, 2023.
- [5] P. I. J. Z. K. Y. B. M. H. D. T. D. D. B. A. L. C. S. K. a. L. M. Rajpurkar, "Rajpurkar, P., Irvin, J., Zhu, K., Yang, B., Mehta, H., Duan, T., Ding, D., Bagul, A., Langlotz, C., Shpanskaya, K. and CheXnet: Radiologist-level pneumonia detection on chest x-rays with deep learning.," in *arXiv*, 2017.
- [6] K. R. C. C. F. S. P. A. M. F. C. G. F. M. S. M. F. a. L. P. Stokes, "The use of artificial intelligence systems in diagnosis of pneumonia via signs and symptoms: a systematic review," in *Biomedical Signal Processing and Control*, 2022.
- [7] W. X. Y. L. Y. L. D. T. Y. S. D. H. Yanping Yang, "Medical Imaging-based Artificial Intelligence in Pneumonia: A Review".