VISVESVARAYA TECHNOLOGICAL UNIVERSITY

JNANA SANGAMA, BELAGAVI-590018

A Project Report

ON

"Cybersecurity for AI in Healthcare."

Submitted in partial fulfillment for the award of degree of Bachelor of Engineering in In Computer Science & Engineering (Data Science) during the year 2024-2025

Submitted by

Poorvika M S	**4MH22CD044**
Priyadarshini	**4MH22CD046**
Aishwarya A	**4MH22CD063**
Ravikumar P	**4MH23CD0405**

Under the guidance of
Prof. Deepthi
Asst. Professor
Dept. of CSE(Data Science)

2024-2025

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(DATA SCIENCE)

MAHARAJA INSTITUTE OF TECHNOLOGY MYSORE
BELAWADI, NAGUVANAHALLY POST, S.R. PATNA TALUK,
MANDYA DISTRICT-571477

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(DATA SCIENCE)
MAHARAJA INSTITUTE OF TECHNOLOGY MYSORE
MANDYA — 571477.

CERTIFICATE

Certified that the project work entitled "**Cybersecurity for AI in Healthcare**" has been successfully carried out by **Poorvika MS [4MH22CD044], Priyadarshini [4MH22CD046], Aishwarya A [4MH22CD063], Ravikumar P [4MH23CD0405],** bonafide students of **Maharaja Institute of Technology Mysore** in partial fulfilment of the requirements of PROJECT PHASE-1 [BCD685] in **Computer Science and Engineering (Data Science) of Visvesvaraya Technological University, Belagavi** during the academic year **2024-2025**. It is certified that all corrections/suggestions indicated for the Internal Assessment have been incorporated in the report deposited in the department library. The project phase-1 report has been approved as it satisfies the academic requirements with respect to the project work prescribed for Bachelor of Engineering Degree.

Signature of the Guide **Prof. Deepthi** Assistant Professor Dept. of CSE (Data Science) MIT MYSORE	Signature of the HOD **Dr. Pushpa D** Professor & Head Dept. of CSE (Data Science) MIT MYSORE	Signature of the Principal **Dr. Murali S** Principal MIT MYSORE

ABSTRACT

The rapid digitization of healthcare systems has led to a significant increase in cybersecurity threats, including data breaches, ransomware attacks, and unauthorized access to sensitive patient information. Traditional security mechanisms often fall short in providing comprehensive protection against such evolving threats. This project proposes the development of an AI-based anomaly detection system aimed at enhancing the security of hospital networks and protecting critical healthcare data. The system employs machine learning algorithms, particularly the Random Forest model, to detect and predict abnormal behaviors indicative of cyberattacks. To further strengthen data protection, the solution integrates blockchain technology for ensuring data integrity and immutability, as well as Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enforce access control and prevent data leakage. The Advanced Integrated Data Security (AIDS) framework is implemented to address the unique security challenges of cloud-based healthcare infrastructures. This multi-layered approach not only enables real-time monitoring and proactive threat mitigation but also enhances confidentiality, integrity, and availability of healthcare data. The outcome is a comprehensive, intelligent cybersecurity framework designed to safeguard digital healthcare environments against modern cyber threats.

TABLE OF CONTENT