VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELGAUM, KARNATAKA- 590014

A PROJECT REPORT ON

DEVELOP AN ETHICAL AND SECURE MACHINE LEARNING FRAMEWORK TO UNCOVER CUSTOMER TRENDS WITHOUT COMPROMISING USER PRIVACY

Submitted in partial fulfilment for the award of Degree of,

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

By

NISHANT KUMAR	4AL21IS034
BHARATH J	4AL21IS011
SRIKANTH RAJU S	4AL21IS056
SHRAVITHA	4AL21IS051

Under the guidance of

Mr. Mounesh A

Associate Professor

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

ALVA'S Education Foundation

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K -574225

2023-24

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

ALVA'S
Education Foundation

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"Develop an ethical and secure machine learning framework to uncover customer trends without compromising user privacy"** has been successfully completed by

NISHANT KUMAR	4AL21IS034
BHARATH J	4AL21IS011
SRIKANTH RAJU S	4AL21IS056
SHRAVITHA	4AL21IS051

the bonafide students OF **DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING, Alva's Institute of Engineering and Technology**, Moodbidri affiliated to **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the academic year 2023–24. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed in partial fulfillment of awarding Bachelor of Engineering degree.

Mr. Mounesh A **Project Guide**	**Mr. Mounesh** **Project Coordinator**	**Dr. Sudheer Shetty** **HOD ISE**

ABSTRACT

This framework addresses the critical need for balancing the extraction of valuable customer insights with stringent privacy protections. By leveraging advanced anonymization techniques, differential privacy, and federated learning, businesses can analyze aggregated data without accessing individual-level information. These methods ensure that customer data remains secure and private, while still enabling the identification of key trends and patterns. The framework also includes comprehensive data governance policies to comply with international regulations and build customer trust. This approach not only mitigates privacy risks but also enhances the credibility and ethical standing of businesses in the eyes of consumers.