VISVESVARAYA TECHNOLOGICAL UNIVERSITY,

BELAGAVI-590018

Mini Project Report On

"Mitigating False Positives: Enhancing Cybersecurity Accuracy"

A report submitted in partial fulfillment of the requirements for

MINI PROJECT

In

Computer Science and Engineering (IOT , Cyber Security including Blockchain Technology)

Submitted by

GAUTAM P KINI	4AL22IC011
DARSHAN K REVANKAR	4AL22IC010
JISHNU RAJ V K	4AL22IC014
MOHAMMAD TAMJEED IBRAHIM	4AL22IC017

Under the Guidance of

Prof. Vasudev S Shahapur

ALVA'S
Education Foundation®

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (IOT , CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOODBIDRI-574225, KARNATAKA

2023 – 2024

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI, D.K. - 574225

ALVA'S
Education Foundation®

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (IOT , CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

CERTIFICATE

This is to certify that the Project entitled "**Mitigating False Positives: Enhancing Cybersecurity Accuracy**" has been successfully completed by

GAUTAM P KINI 4AL22IC011 DARSHAN K REVANKAR 4AL22IC010
JISHNU RAJ V K 4AL22IC014 MOHAMMAD TAMJEED IBRAHIM
4AL22IC017

the bonafide students of Department of Computer Science & Engineering (IOT , Cyber Security including Blockchain Technology), Alva's Institute of Engineering and Technology in **DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING (IOT , CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)** of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the year 2023–2024. 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 for the Bachelor of Engineering Degree.

Prof. Vasudev S Shahapur
Project Guide

Dr. Pradeep V
HOD CSE(ISE/ICB)

H.O.D.
Dept. Of Information Science & Engineering
Alva's Institute
Mijar, MOODBIDRI

ABSTRACT

Cybersecurity threats have become a critical challenge in today's digital landscape, leading to an increasing need for effective solutions to mitigate false positives in security systems. This project explores strategies to enhance the accuracy of cybersecurity measures by reducing false positive rates, which can lead to unnecessary alerts and a misallocation of resources. False positives not only diminish the efficiency of security operations but also hinder response times and overall system effectiveness.

The project focuses on refining detection algorithms and leveraging advanced machine learning techniques to better differentiate between legitimate threats and benign activities. By analyzing vast datasets and applying sophisticated anomaly detection methods, the project aims to improve the precision of threat identification. It includes the development of models trained to recognize patterns indicative of true security breaches while filtering out non-threatening events.

Through a series of rigorous tests and performance evaluations, the project demonstrates how fine-tuning existing models and implementing hybrid approaches can significantly reduce false positives without compromising the detection of actual attacks. Additionally, the integration of contextual and behavioral data helps improve decision-making accuracy, further minimizing the risk of false alerts.

Key innovations in the project include the integration of contextual information, such as user behavior and environmental factors, to provide a more nuanced understanding of potential threats. By incorporating these additional layers of data, the detection system becomes better equipped to discern between anomalous activity that indicates a genuine security breach and that which may be a false positive.

In conclusion, this project provides an in-depth analysis of mitigating false positives in cybersecurity, offering practical solutions for improving the reliability and efficiency of threat detection systems. The results contribute to advancing cybersecurity measures in various sectors, enhancing the protection of critical infrastructure and sensitive data.