AI/ML-POWERED FRAMEWORK FOR ENHANCED NETWORK INTRUSION DETECTION USING NON-IOC METHODS.

A PROJECT REPORT

Submitted by,

Mr. S VARUN KUMAR - 20211CCS0006
Mr. DEEPAK R - 20211CCS0008
Mr. CHINMAYA GP - 20211CCS0046
Mr. DARSHAN U - 20211CCS0094

Under the guidance of,

Dr. SHANTHI S

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

At

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

PRESIDENCY UNIVERSITY

BENGALURU

MAY 2025

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Project report **"AI/ML-POWERED FRAMEWORK FOR ENHANCED NETWORK INTRUSION DETECTION USING NON-IOC METHODS"** being submitted by "S VARUN KUMAR, DEEPAK R, CHINMAYA GP, DARSHAN U," bearing roll number(s) "20211CCS0006, 20211CCS0008, 20211CCS0046, 20211CCS0094" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security) is a bonafide work carried out under my supervision.

Dr. Shanthi S
Associate Professor
PSCS
Presidency University

Dr. S P Anandaraj
Professor & HoD
PSCS
Presidency University

Dr. MYDHILI NAIR
Associate Dean
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor-Engineering
Dean -PSCS/PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **AI/ML-POWERED FRAMEWORK FOR ENHANCED NETWORK INTRUSION DETECTION USING NON-IOC METHODS** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried under the guidance of **Dr. SHANTHI S, ASSISTANT PROFFESOR, School of Computer Science Engineering & Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

CHINMAYA G P- 20211CCS0046

DARSHAN U – 20211CCS0094

S VARUN KUMAR – 20211CCS0006

DEEPAK R – 20211CCS0008

ABSTRACT

The cybersecurity landscape is undergoing a transformation as attackers develop increasingly sophisticated methods to bypass traditional defences. Conventional intrusion detection systems that depend on predefined Indicators of Compromise (IoCs) face significant limitations they can only recognize threats they've seen before, leaving networks exposed to novel attack vectors. This research presents an innovative machine learning-based approach that shifts the paradigm from signature-dependent detection to behavioural anomaly identification, offering robust protection even against previously unknown threats.

At the heart of our system lies a comparative analysis of five machine learning algorithms Random Forest, K-Nearest Neighbours, Naive Bayes, Logistic Regression, and XGBoost each evaluated for their ability to distinguish between normal and malicious network activity. Through extensive testing on diverse datasets, we discovered that Logistic Regression, often overlooked in favour of more complex models, demonstrated superior performance in real-world scenarios. Its strengths included consistent accuracy, resistance to overfitting, and critically interpretability, a vital feature for security professionals who need to understand and trust their detection systems.Practical implementation was a key design consideration. The solution integrates seamlessly with existing network infrastructure, including routers, firewalls, and endpoint protection systems, requiring minimal configuration while significantly enhancing threat detection capabilities. By reducing false positives a common pain point in anomaly detection our system delivers actionable alerts that security teams can prioritize with confidence.

Perhaps most importantly, this research demonstrates that effective cybersecurity doesn't require sacrificing simplicity for sophistication. As threat actors continue to evolve, our approach provides a scalable, adaptive framework for defense one that doesn't wait for the next attack to be documented before offering protection. In an era where a single breach can cost millions, such proactive, intelligent systems represent not just an advancement, but a necessity for any organization serious about safeguarding its digital assets.

ACKNOWLEDGEMENT

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC, School of Engineering and Dean, School of Computer Science Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate dean **Dr. Mydhili Nair,** School of Computer Science Engineering & Information Science, Presidency University, and **Dr. S P Anandaraj**, Head of the Department, School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Shanthi S, Associate Professor** and Reviewer **Dr. Nihar Ranjan Nayak**, School of Computer Science Engineering & Information Science, Presidency University for their inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the **CSE7301** Capstone Project Coordinators **Dr. Sampath A K, Dr. Abdul Khadar A and Mr. Md Zia Ur Rahman,** department Project Coordinators **Dr. Sharmasth Vali** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

S Varun Kumar

Deepak R

Chinmaya GP

Darshan U