



Kammavari Sangham (R) 1952, K.S.Group of Institutions

K. S INSTITUTE OF TECHNOLOGY

9 No.14, Raghuvanahalli, Kanakapura Road, Bengaluru - 560109

Affiliated to VTU, Belagavi & Approved by AICTE, New Delhi, Accredited by NBA , NAAC & IEI

Department of Computer Science and Engineering Project Phase – I (18CSP83)

Project Title: Machine Learning Based Intrusion Detection System

Group No.: A1

Batch No.: 2023_CSE_09

1. 1KS20CS056 – Moniesh S
2. 1KS20CS057 – Monika N
3. 1KS20CS073 – Pavithra R
4. 1KS20CS093 – Sindhura H

Guided By:
Mr.Somasekhar T
Associate Professor
Dept of CSE , KSIT

Contents

- Introduction
- Literature survey
- Problem identification
- Problem Statement
- Scope
- Goals and objectives
- Methodology
- Data flow
- Contribution to the society
- References

Introduction

- Intrusion is a form of attack where the attacker tries to gain sensitive information by posing as a reputable source.
- A victim opens a compromised link that poses as a credible network site. The victim is then asked to enter their credentials, but since it is a “fake” network site, the sensitive information is routed to the hacker and the victim gets hacked.
- Social engineering attack is a common security threat used to reveal private and confidential information by simply tricking the users without being detected.
- Intrusion attack may appear in many types of communication forms such as messaging, SMS and fraud mails.

Literature Survey

	Title	Author	Methodology	Outcomes
1	Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network-2019	Hong Yu Yang	The paper proposes an improved Convolutional Neural Network (CNN) for wireless network intrusion detection. The CNN is customized for the specific characteristics of wireless networks.	The improved CNN demonstrates enhanced accuracy in detecting intrusions in wireless networks compared to traditional methods.
2	Generalized Intrusion Detection Mechanism for Empowered Intruders in Wireless Sensor Networks-2020	Wenming Wang	The paper presents a generalized intrusion detection mechanism designed to identify empowered intruders in wireless sensor networks. The mechanism takes into account various types of intrusions that can occur in these networks.	The proposed mechanism shows effectiveness in detecting and mitigating intrusions by empowered attackers within wireless sensor networks.

Literature Survey

	Title	Author	Methodology	Outcomes
3	Method of Network Intrusion Discovery Based on Convolutional Long-Short Term Memory Network and Implementation in VSS-2021	Zhijie Fan	This paper introduces a network intrusion detection method based on a Convolutional Long-Short Term Memory (CLSTM) network. The method is implemented in a Virtual Security System (VSS) environment.	The CLSTM network demonstrates improved capabilities in capturing temporal dependencies, leading to enhanced detection accuracy in network intrusions when implemented in the VSS.
4	Effective algorithms to detect stepping-stone intrusion by removing outliers of packet RTTs-2022	Lixin Wang	The paper proposes algorithms to detect stepping-stone intrusions by analyzing packet Round-Trip Times (RTTs) and removing outliers. The focus is on identifying anomalous patterns indicative of stepping-stone attacks.	The proposed algorithms effectively identify and mitigate stepping-stone intrusions by filtering out outlier RTT values, improving the overall security of the network.

Problem identification

- With the escalating frequency and sophistication of cyber-attacks, traditional rule-based intrusion detection systems often struggle to keep pace with evolving threats.
- This project identifies the need for a more adaptive and efficient approach by leveraging machine learning techniques.
- The over arching problem involves the development of a robust intrusion detection system capable of autonomously learning and adapting to emerging threats, thereby enhancing the overall security posture of networks.

Problem Statement

The challenge lies in developing comprehensive and effective security measures to detect and prevent intrusion attacks, especially those leveraging social engineering techniques. Addressing this problem requires advanced threat detection technologies, and enhanced authentication methods to safeguard users against the evolving tactics employed by malicious activities.

Scope

- The scope of the project encompasses the design, development, and implementation of a comprehensive Intrusion Detection System (IDS) employing state-of-the-art machine learning techniques.
- The focus will be on creating a scalable and adaptive solution capable of real-time analysis of network traffic to identify and classify potential intrusions.
- The project will involve the exploration and integration of various machine learning algorithms, feature engineering, and model optimization to enhance the accuracy and efficiency of intrusion detection.

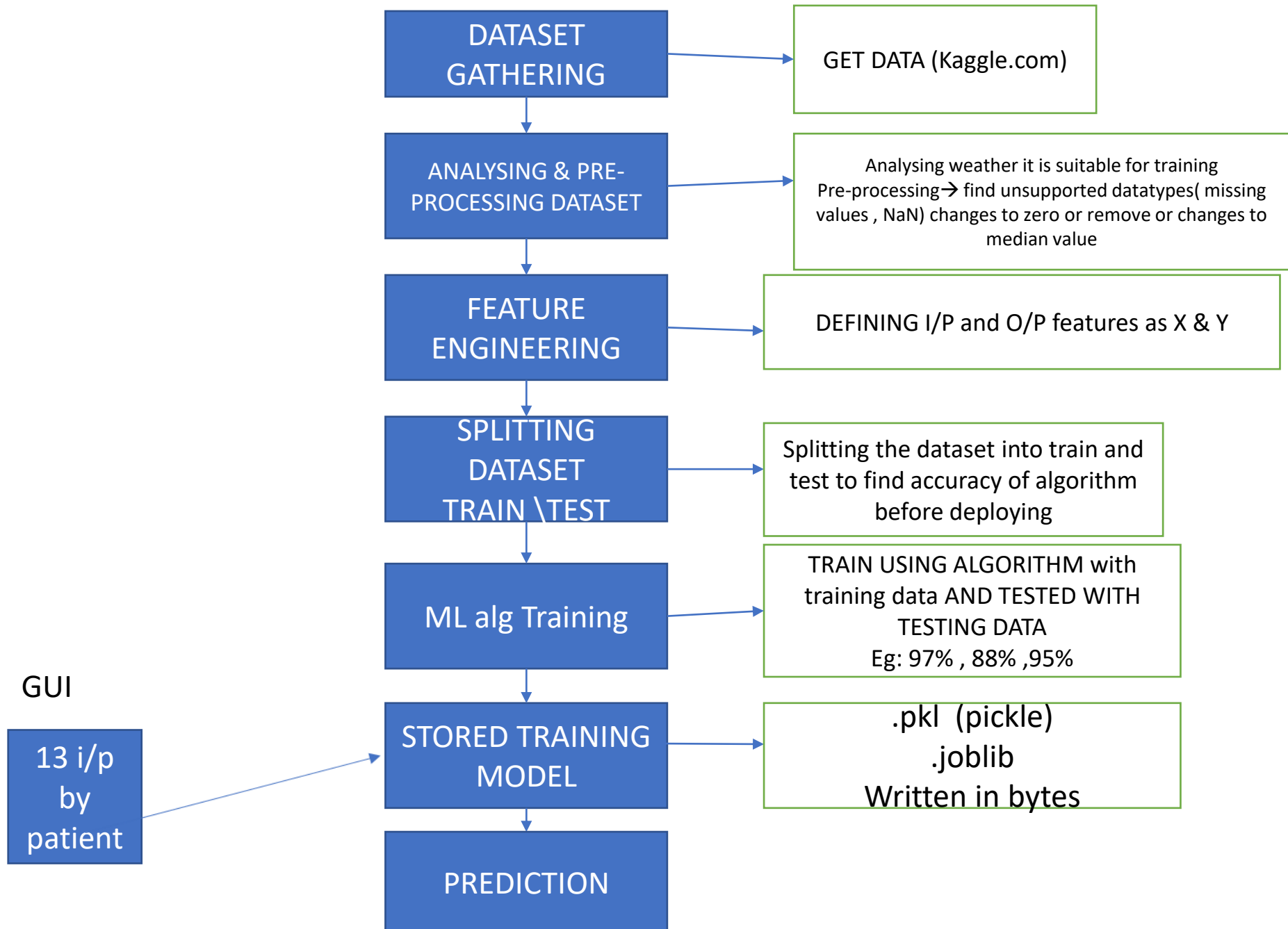
Goals and Objectives

GOALS:

- Develop an advanced Intrusion Detection System (IDS) using machine learning techniques. Enhance the adaptability, accuracy, efficiency and scalability of the IDS for real-time analysis environments.

OBJECTIVES:

- Design and implement a robust IDS architecture capable of handling large-scale network traffic.
- Explore and integrate state-of-the-art machine learning algorithms for anomaly detection and intrusion classification.
- Optimize model performance through feature engineering and continuous evaluation in various network scenarios.
- Validate the effectiveness of the developed IDS through rigorous testing and comparison with existing intrusion detection systems.



Methodology

➤ Dataset Collection:

- Gather a diverse and representative dataset containing labeled instances of normal network behavior and various types of intrusions. Utilize publicly available datasets and, if possible, collaborate with industry partners to ensure realism and relevance.

➤ Data Preprocessing:

- Clean and preprocess the collected dataset by handling missing values, normalizing features, and addressing any inconsistencies. This step is crucial for ensuring the quality and reliability of the data used for training and testing.

➤ Feature Engineering:

- Extract relevant features from the preprocessed data to characterize network traffic patterns effectively. Feature engineering may involve selecting key attributes, transforming variables, and creating new features to enhance the performance of machine learning models.

Methodology

➤ Model Selection:

- Evaluate and choose suitable machine learning algorithms for intrusion detection, considering factors such as accuracy, interpretability, and scalability. Common choices include decision trees, random forests, support vector machines, and deep learning models.

➤ Model Training:

- Train the selected machine learning models using the preprocessed and engineered dataset. Employ techniques such as cross-validation to optimize model hyperparameters and ensure robust generalization to unseen data.

➤ Model Evaluation:

- Assess the performance of the trained models using separate test datasets, employing metrics such as precision, recall, F1 score, and ROC-AUC. Iterate on the model training and evaluation process to fine-tune the system for optimal results.

Data Flow

- Level 0

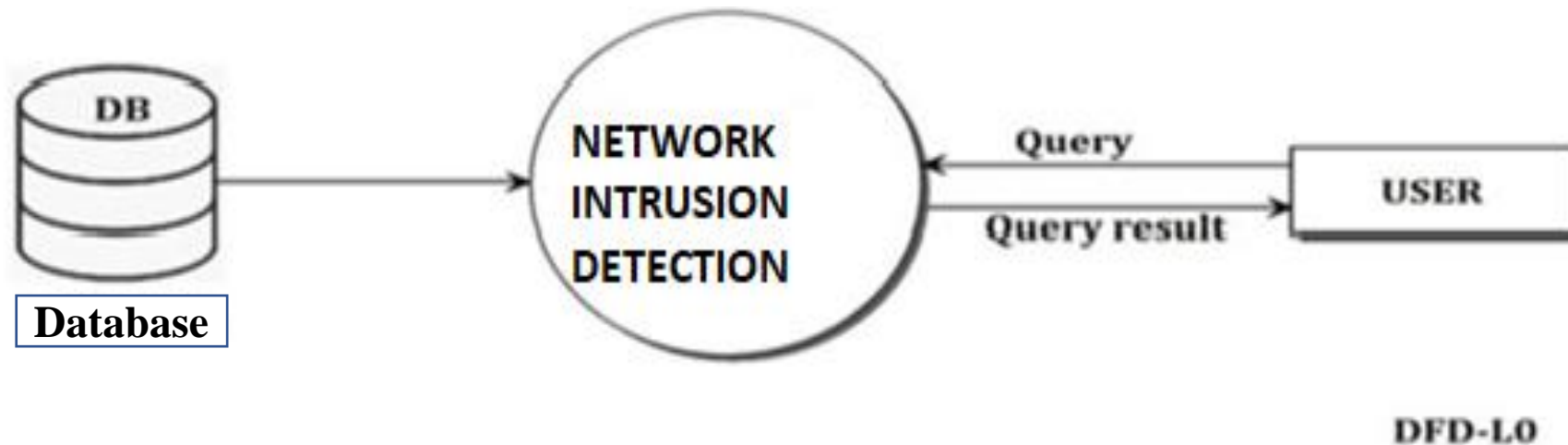


Figure : level 0 of dataflow diagram

Data Flow

- Level 1

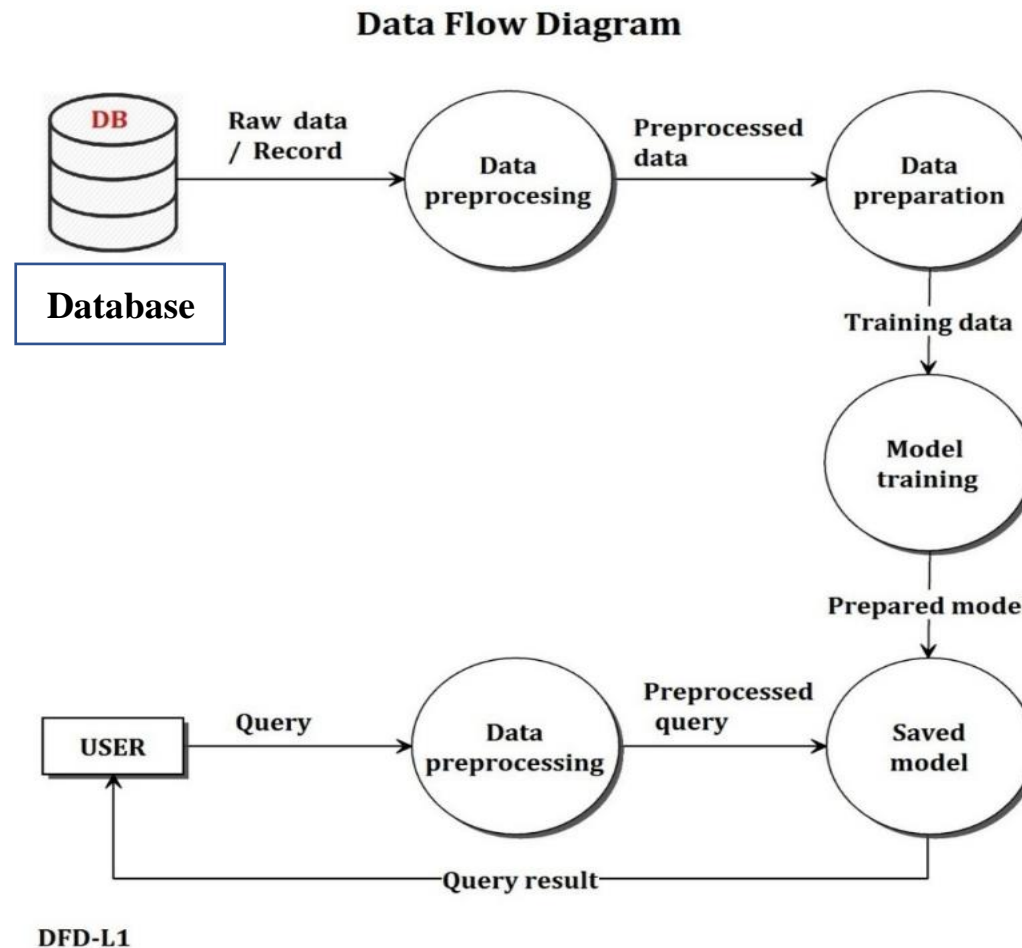


Figure : level 1 of dataflow diagram

Data Flow

- Level 2

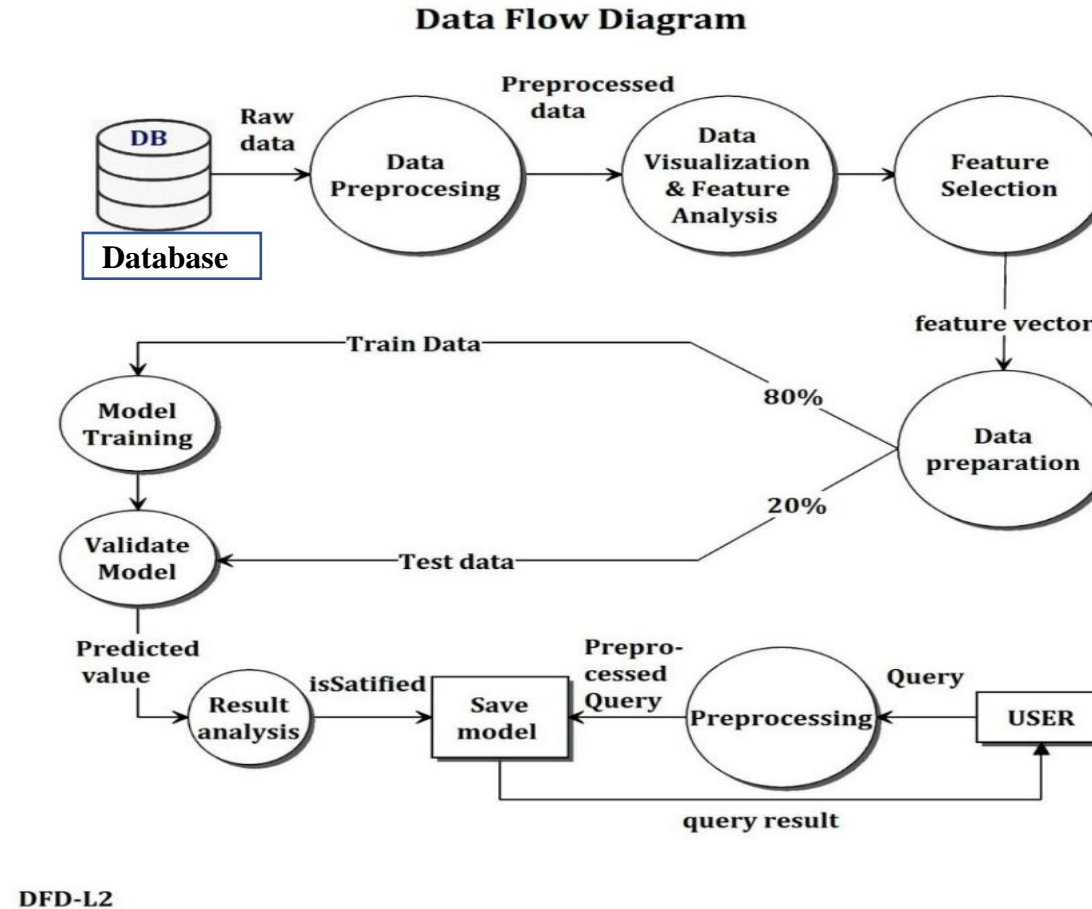


Figure : level 2 of dataflow diagram

Contribution to the society

- Machine learning techniques to detect and threat malicious activities in real-time, our solution contributes to securing critical infrastructure, confidential data, and sensitive information.
- In an era where cyber threats are increasingly sophisticated, the deployment of an intelligent defense mechanism aids in protecting individuals, businesses, and institutions from potential breaches.
- The proactive nature of our IDS not only enhances security but also helps digital environment, promoting trust and stability in the interconnected world.
- This initiative aligns with the broader goal of creating a safer digital space for individuals, businesses, and society at large.

Timeline

Task done	Task planned
September- Selecting Domain	January- Project implementation
October- Background work and defining problem statement	February- Result and discussion
November- Literature survey	March- Conclusion and future scope
December- Published survey paper	April- Publication and participation in project exhibition

References

1. P. Alaei and F. Noorbehbahani , “Incremental anomaly –based intrusion detection system using limited labeled data,” in Web Research (ICWR),2017 3th International Conference on, 2017, pp.178-184
2. M. Saber, S. Chadli, M. Emharraf, and I.El Farissi, ”Modeling and implementation approach to evaluate the intrusion detection system,” in International Conference on Networked systems, 2015, pp.513-517.
3. M. Tavallaee, N. Stakhanova, and A. A. Ghorbani ,”Toward credible evaluation of anomaly-based intrusion-detection methods”, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),vol. 40, no. 5, pp.516-524,2010.
4. A. S. Ashoor and S. Gore “Importance of intrusion detection system(IDS)”,International Journal of Scientific and Engineering Research,Vol.2,no. 1, pp. 1-4, 2011.

Published Survey Paper



International Journal for Research in Applied Science & Engineering Technology (IJRASET)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538

Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

Safeguarding Connections: Machine Learning Powered Intrusion Detection

Somasekhar T¹, Moniesh S², Monika N³, Pavithra R⁴, Sindhura H⁵

¹Associate Professor, Dept. of Computer Science, K S Institute of Technology, Bangalore, Karnataka

^{2, 3, 4, 5}Dept. of Computer Science, K S Institute of Technology, Bangalore, Karnataka

Abstract: *It's crucial to have reliable intrusion detection systems. a cutting-edge method of machine learning-based intrusion detection. Our solution uses cutting-edge algorithms to detect and eliminate any threats instantly, acting as a preventative measure against a wide range of cyberattacks. Since the model has been trained on a large number of datasets, it can eventually strengthen network security by evolving and adapting to new threats. Naive Bayes (NB) classifiers and correlation-based feature selection (CFS) methods are used to reduce the amount of data. For attack classification, the Intrusion Detection System recommends using an Instance-Based Learning algorithm (IBK) in combination with a Multilayer Perceptron (MLP).*

Keywords: *Support Vector Machine (SVM), Multilayer Perceptron (MLP), Correlation Based Feature (CFS), Classifier subset evaluation, Intrusion Detection System (IDS), and Instance-Based Learning algorithm (IBK).*

Certificates



IJRASET
International Journal for Research in Applied
Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISSN No. : 2321-9653

Certificate

It is here by certified that the paper ID : IJRASET56689, entitled
Safeguarding Connections: Machine Learning Powered Intrusion Detection
by
Somasekhar T

after review is found suitable and has been published in
Volume 11, Issue XI, November 2023
in

*International Journal for Research in Applied Science &
Engineering Technology*
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors

By 
Editor in Chief, IJRASET

ISRA Journal Impact
Factor: 7.429

45.98
INDEX COPERNICUS

THOMSON REUTERS
Researcher ID: N-9663-2016

doi
crossref
10.22214/IJRASET

TOGETHER WE REACH THE GOAL
SJIF 7.429

Certificates



IJRASET
International Journal for Research in Applied
Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISSN No. : 2321-9653

ISRA Journal Impact
Factor: 7.429

45.98
INDEX COPERNICUS

THOMSON REUTERS
Researcher ID: N-9581-2016

doi
crossref
10.22214/IJRASET

TOGETHER WE REACH THE GOAL
SJIF 7.429

Certificate

It is here by certified that the paper ID : IJRASET56689, entitled
Safeguarding Connections: Machine Learning Powered Intrusion Detection
by
Moniesh S

after review is found suitable and has been published in
Volume 11, Issue XI, November 2023
in

International Journal for Research in Applied Science &
Engineering Technology
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors

By 
Editor in Chief, IJRASET

Certificates



iJRASET
International Journal for Research in Applied
Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISSN No. : 2321-9653

Certificate

It is here by certified that the paper ID : IJRASET56689, entitled
Safeguarding Connections: Machine Learning Powered Intrusion Detection
by
Monika N

after review is found suitable and has been published in
Volume 11, Issue XI, November 2023
in
International Journal for Research in Applied Science &
Engineering Technology
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors

By 
Editor in Chief, IJRASET

ISRA Journal Impact
Factor: 7.429

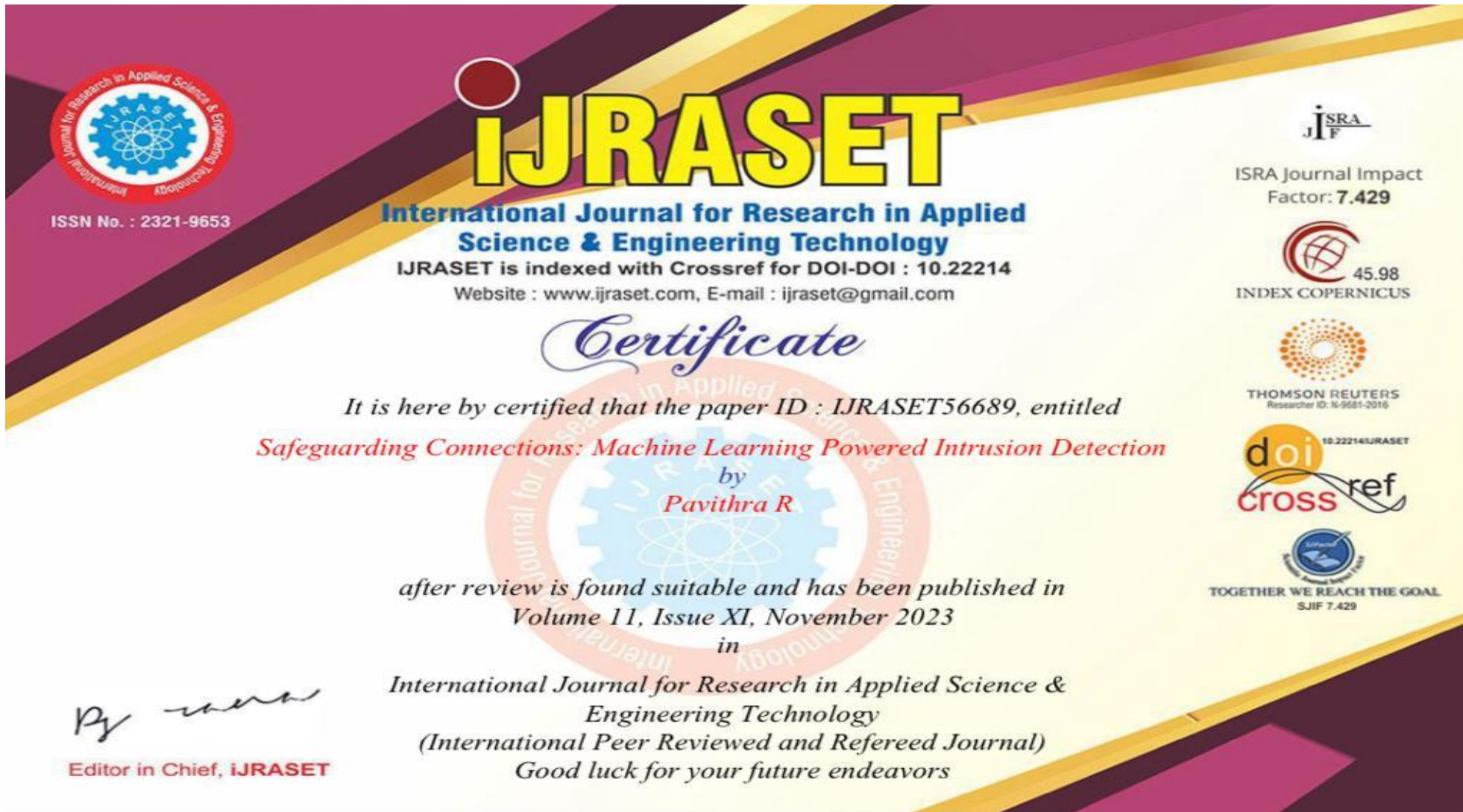
45.98
INDEX COPERNICUS

THOMSON REUTERS
Researcher ID: N-9581-2016

10.22214/IJRASET
doi
crossref

TOGETHER WE REACH THE GOAL
SJIF 7.429

Certificates



iJRASET
International Journal for Research in Applied
Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISSN No. : 2321-9653

ISRA Journal Impact
Factor: 7.429

45.98
INDEX COPERNICUS

THOMSON REUTERS
Researcher ID: N-9661-2016

doi 10.22214/IJRASET
CROSSref

TOGETHER WE REACH THE GOAL
SJIF 7.429

Certificate

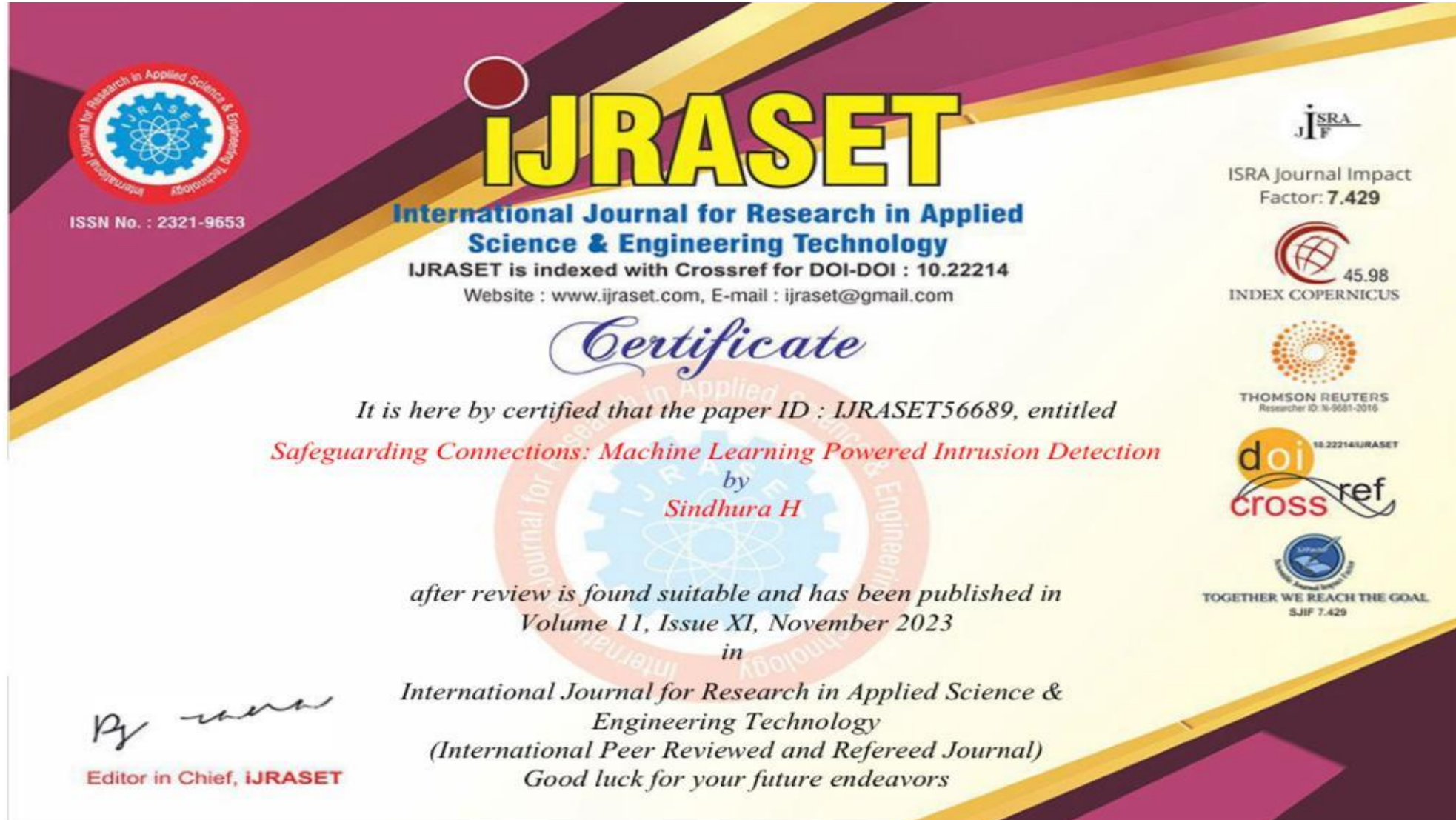
It is here by certified that the paper ID : IJRASET56689, entitled
Safeguarding Connections: Machine Learning Powered Intrusion Detection
by
Pavithra R

after review is found suitable and has been published in
Volume 11, Issue XI, November 2023
in

*International Journal for Research in Applied Science &
Engineering Technology*
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors

By
Editor in Chief, iJRASET

Certificates




iJRASET
International Journal for Research in Applied
Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com

Certificate

It is here by certified that the paper ID : IJRASET56689, entitled
Safeguarding Connections: Machine Learning Powered Intrusion Detection
by
Sindhura H

after review is found suitable and has been published in
Volume 11, Issue XI, November 2023
in

International Journal for Research in Applied Science &
Engineering Technology
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors

By 
Editor in Chief, IJRASET

ISSN No. : 2321-9653

ISRA Journal Impact
Factor: 7.429

45.98
INDEX COPERNICUS

THOMSON REUTERS
Researcher ID: N-9681-2016

doi 10.22214/IJRASET
crossref

TOGETHER WE REACH THE GOAL
SJIF 7.429