Cloud-Based Intrusion Detection System for Advanced Threat Detection and Prevention using Machine Learning Technique

T. Senthil Kumar, Nikunj Kunduru, Abhinav Ravella, Shanthan Reddy, Sai Koushik, Kartik Srinivasan, Anjali Tibrewal, Sulakshan Vajipayajula

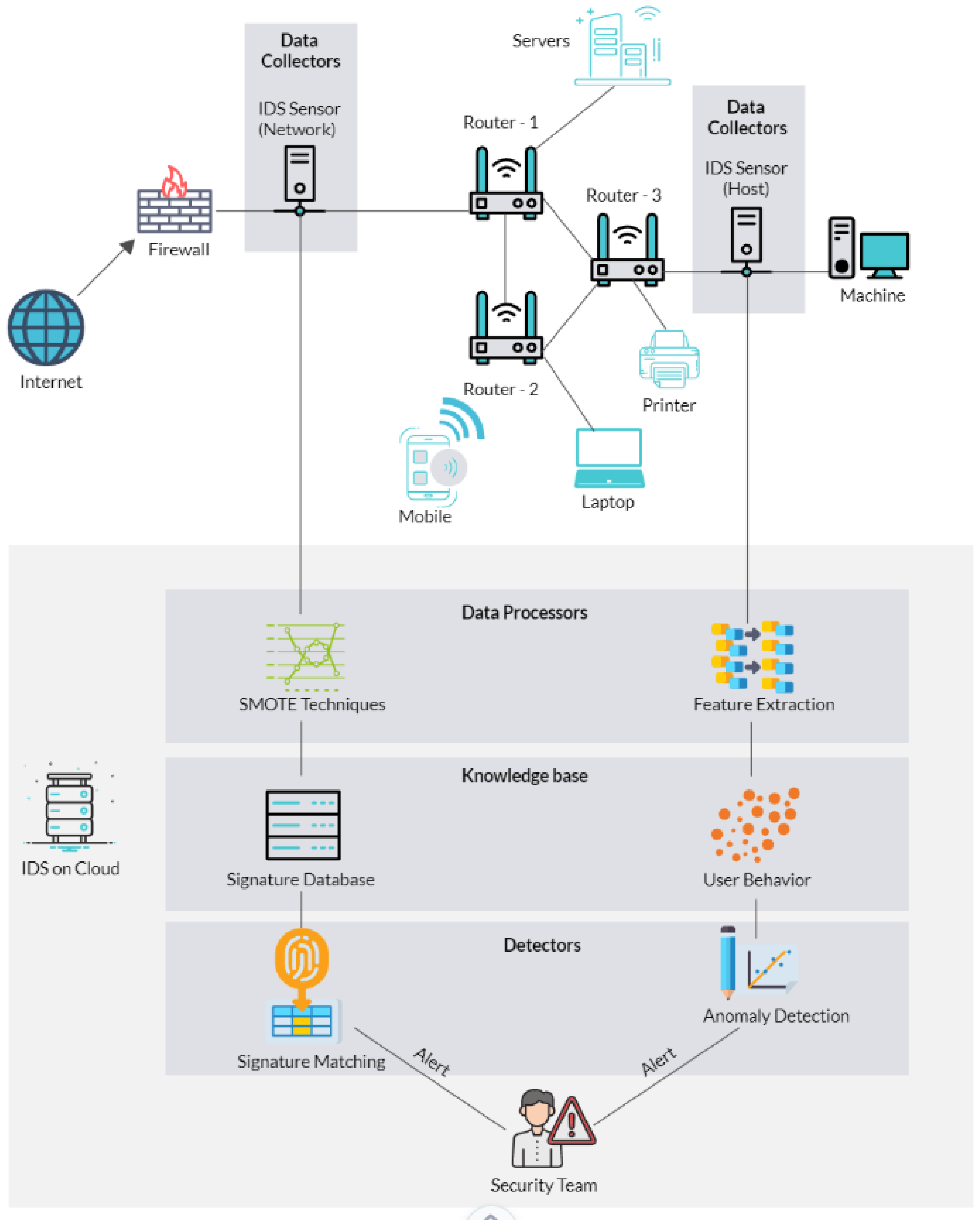
(A) CONTRIBUTIONS & GOALS

In this research, we propose a hybrid intrusion detection system that combines Feed Forward Neural Network for signature-based detection, Isolation Forest for anomaly-based detection in a stacked model, and Linear Regression for final attack prediction, achieving accurate identification of attacks.

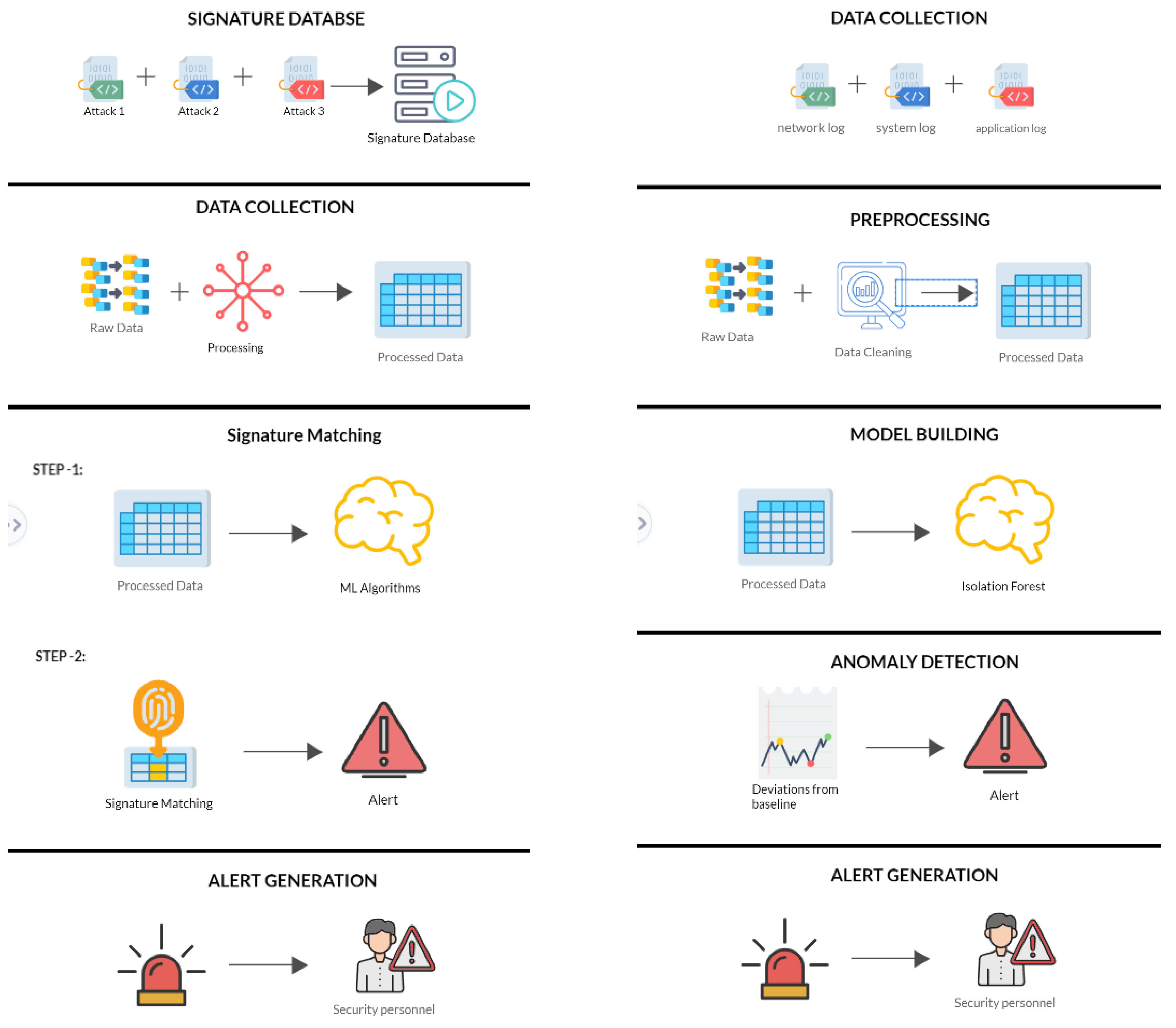
Our goals are as follows :

1. Developing a hybrid intrusion detection system that combines signature-based and anomaly-based approaches, utilizing machine learning algorithms, to improve attack detection and prediction accuracy.

(B) Architecture Diagram

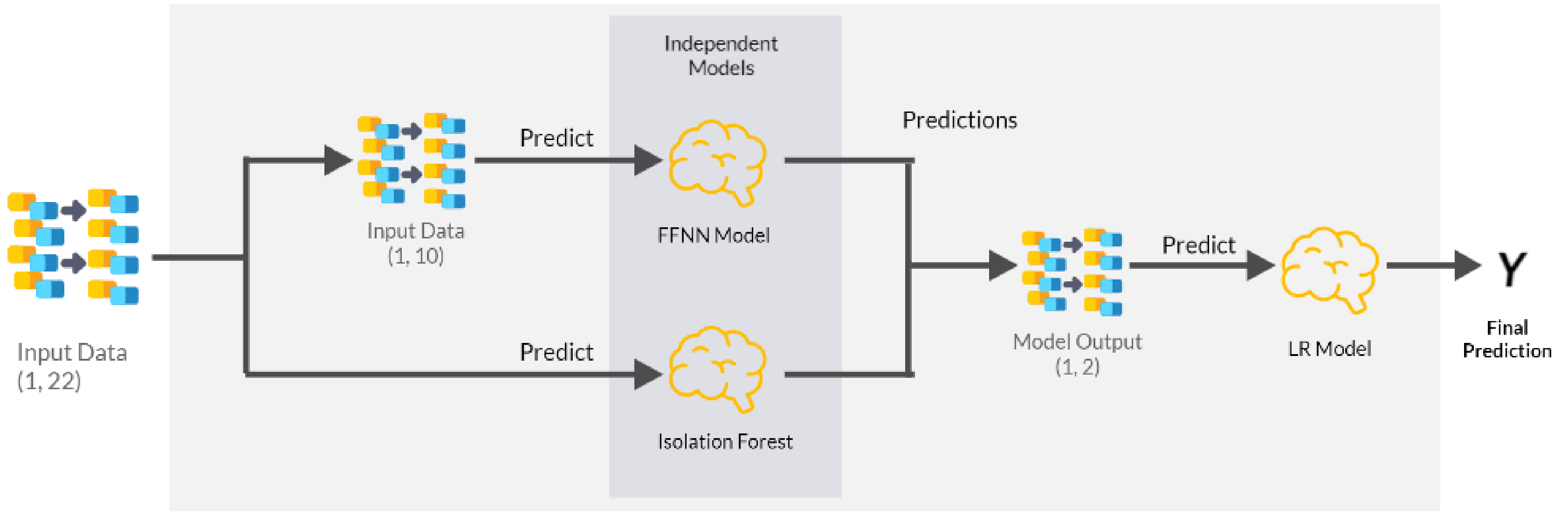


(C) Signature-based & Anomaly-based Detection



(D) Proposed Hybrid-model

Hybrid Intrusion Detection System



The hybrid model combines the strengths of the Feed Forward Neural Network (FFNN) algorithm for signature-based detection and the Isolation Forest (IF) algorithm for anomaly-based detection. By utilizing a stacked model, the FFNN and IF outputs are combined and fed into a Linear Regression (LR) algorithm for the final prediction, resulting in a more robust and accurate intrusion detection system.

(E) Results: Comparison of existing models with proposed model

Techniques	Normal	DDos	Bot	Brute force	Infiltration	Web
IF	62.6	78.9	-	-	-	-
AE	69.9	54.3	49.6	100	27.7	61
RF	88.4	78.9	99.9	91.8	58.9	98.6
FFNN	98.4	99.8	99.9	90.7	29.8	98.8
Hybrid	96.4	100	99.9	99.1	38.6	98.2

(F) Conclusion & Future Works

In conclusion, the proposed hybrid intrusion detection system demonstrates improved accuracy in attack detection and prediction. Future work includes optimizing the model and exploring additional machine learning techniques for enhanced performance.

Main Findings :

1. The integration of signature-based and anomaly-based approaches enhanced the system's ability to identify known attacks as well as detect previously unseen or novel attack patterns.
2. The proposed model showcases the effectiveness of combining multiple machine learning algorithms in creating a robust and comprehensive intrusion detection system for enhanced cybersecurity.
3. The need for a large and diverse dataset for training the hybrid model and ongoing challenge of keeping the signature database up-to-date with emerging threats.

Members

Left-to-Right : Dr. T. Senthil Kumar, Nikunj Kunduru, Abhinav Ravella, Shanthan Reddy, Sai Koushik, Kartik Srinivasan, Anjali Tibrewal, Sulakshan Vajipayajula

References

[1] G. J. Pandeeswari and S. Jeyanthi, "Analysis of Intrusion Detection Using Machine Learning Techniques," 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 2022, pp. 1-5, doi: 10.1109/ICATIECE56365.2022.10047057.

[2] P. Illavarason and B. Kamachi Sundaram, "A Study of Intrusion Detection System using Machine Learning Classification Algorithm based on different feature selection approach," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 295-299, doi: 10.1109/I-SMAC47947.2019.9032499.

[3] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 311-320, September 2023, doi: 10.26599/BDMA.2022.9020038.

[4] S. T. Slevi and P. Visalakshi, "A survey on Deep Learning based Intrusion Detection Systems on Internet of Things," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1488-1496, doi: 10.1109/I-SMAC52330.2021.9641050.

[5] S. Vijayalakshmi, T. D. Subha, M. L, E. S. Reddy, D. Yaswanth and S. Gopinath., "A Novel Approach for IoT Intrusion Detection System using Modified Optimizer and Convolutional Neural Network," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 180-186, doi: 10.1109/I-SMAC55078.2022.9987314.

[6] I. Idrissi, M. Azizi and O. Moussaoui, "A Stratified IoT Deep Learning based Intrusion Detection System," 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 2022, pp. 1-8, doi: 10.1109/IRASET52964.2022.9738045.

[7] F. Abbasi, M. Naderan and S. E. Alavi, "Anomaly detection in Internet of Things using feature selection and classification based on Logistic Regression and Artificial Neural Network on N-BaIoT dataset," 2021 5th International Conference on Internet of Things and Applications (IoT), Isfahan, Iran, 2021, pp. 1-7, doi: 10.1109/IoT52625.2021.9469605.