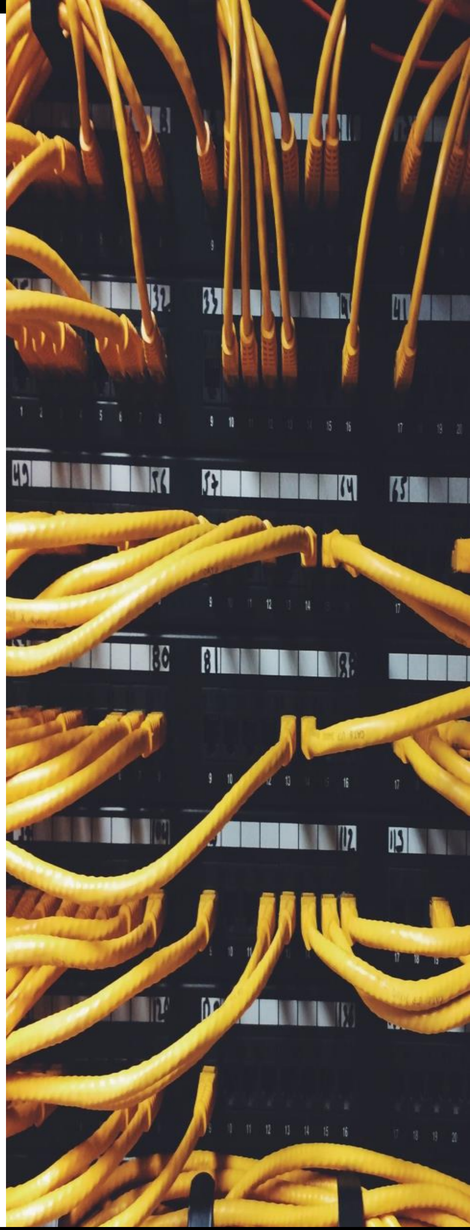
LEVERAGING MACHINE LEARNING FOR MALWARE DETECTION

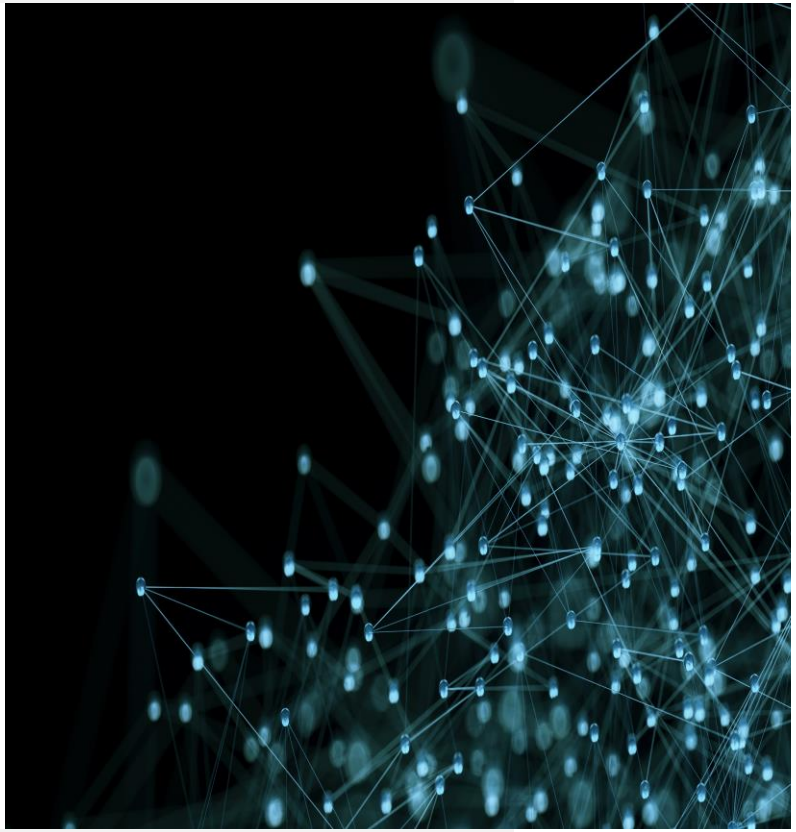


Name: Ekwunife Blessing Ifunanya

Supervisor: Dr. Kabiru Mohammed

INTRODUCTION

- IoT devices are increasingly targeted by malware due to their proliferation and often weak security
- Traditional signature-based approaches are inadequate for detecting evolving threats and zero-day attacks
- ML and deep learning offer promising approaches for identifying malicious network traffic through pattern recognition
- Effective malware detection systems can significantly improve IoT ecosystem security and prevent widespread compromise



RESEARCH OBJECTIVES

Objectives

1

Analyze network traffic patterns associated with IoT malware infections

2

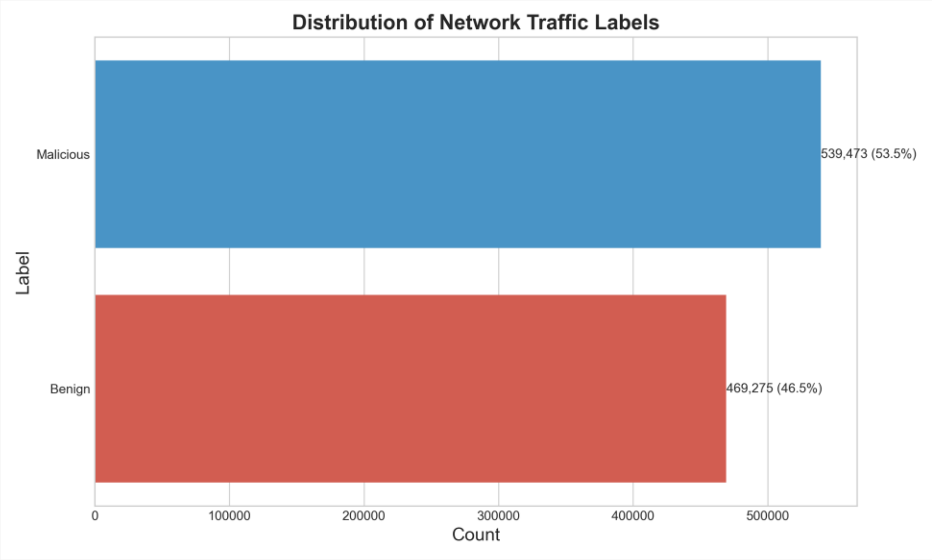
Identify distinctive features that differentiate benign from malicious traffic

3

3. Develop and evaluate machine learning models for automated malware detection using supervised model and neural network approaches

Coventry University

DATASET



- CTU-IoT-Malware dataset from the Czech Technical University. These labels were painstakingly created at the Stratosphere labs using malware capture analysis.
- The dataset was collected using network monitoring equipment that recorded alltraffic flows between the monitored devices and external networks
- Over 1 million labeled network connections from IoT devices. But we are using a variant of it due to computational resources
- 12 datasets was downloaded from the Kaggle version to use for the analysis Malware Detection in Network Traffic Data
- 53.5% malicious, 46.5% benign traffic
- 23 original network flow features like

  - Connection metadata (timestamps, protocols)

  - Traffic volume metrics (bytes, packets)

  - Connection states and durations

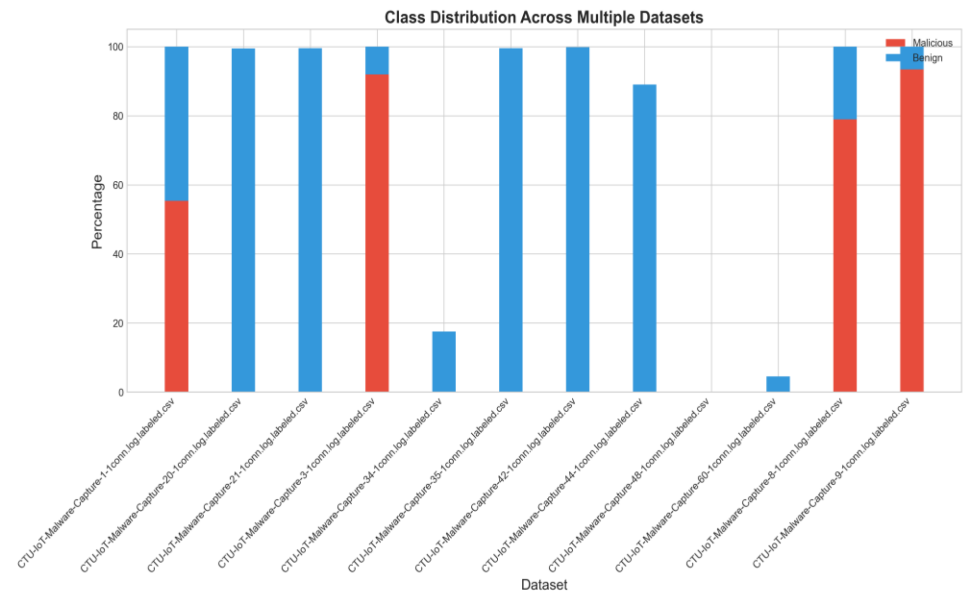
DATA PREPROCESSING

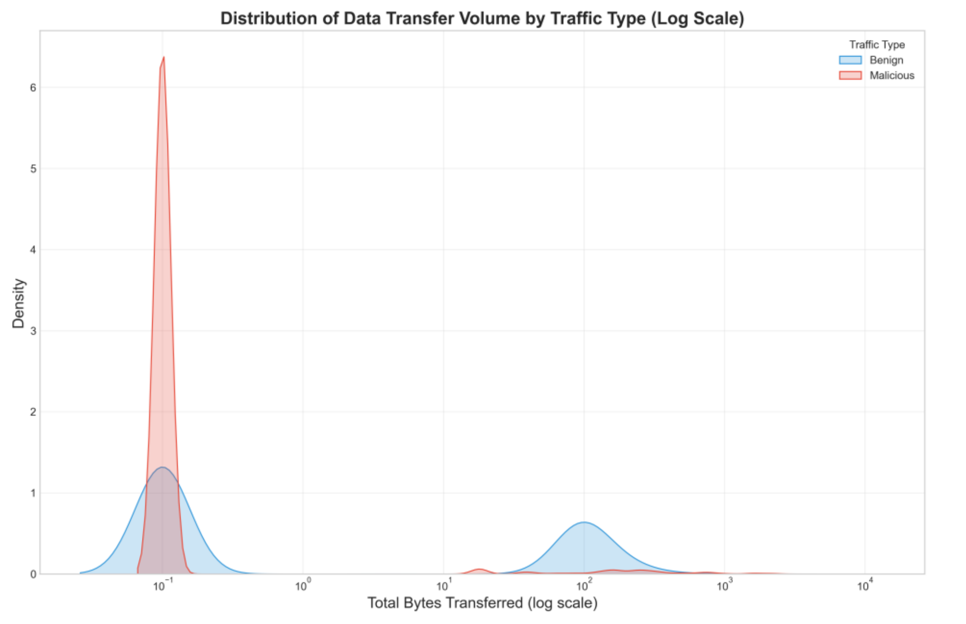
Missing Value Handling

- Duration: Conditional median imputation based on protocol and state
- Over 79% of records had missing values in certain columns, they were dropped
- Bytes/packets: Replaced with zeros (representing no data transfer)

Outlier Treatment

- Applied IQR method and log transformation for skewed distributions
- Standardized time stamps, categorical variables, and labels
- Applied SMOTE for addressing moderate class imbalance





FEATURE ENGINEERING

Temporal Features:

- Hour of day, day of week
- Connection density in time windows

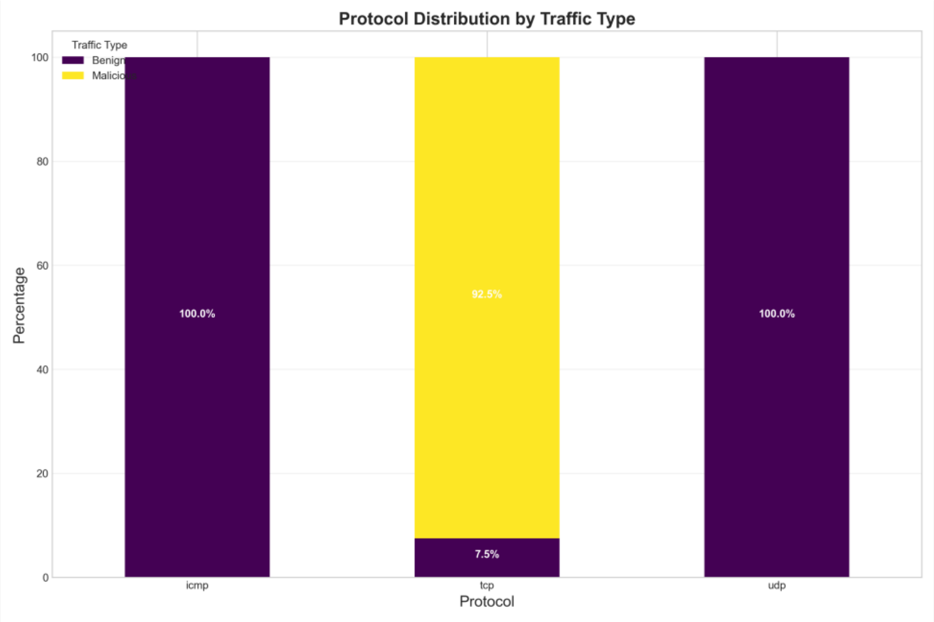
Traffic Volume Features:

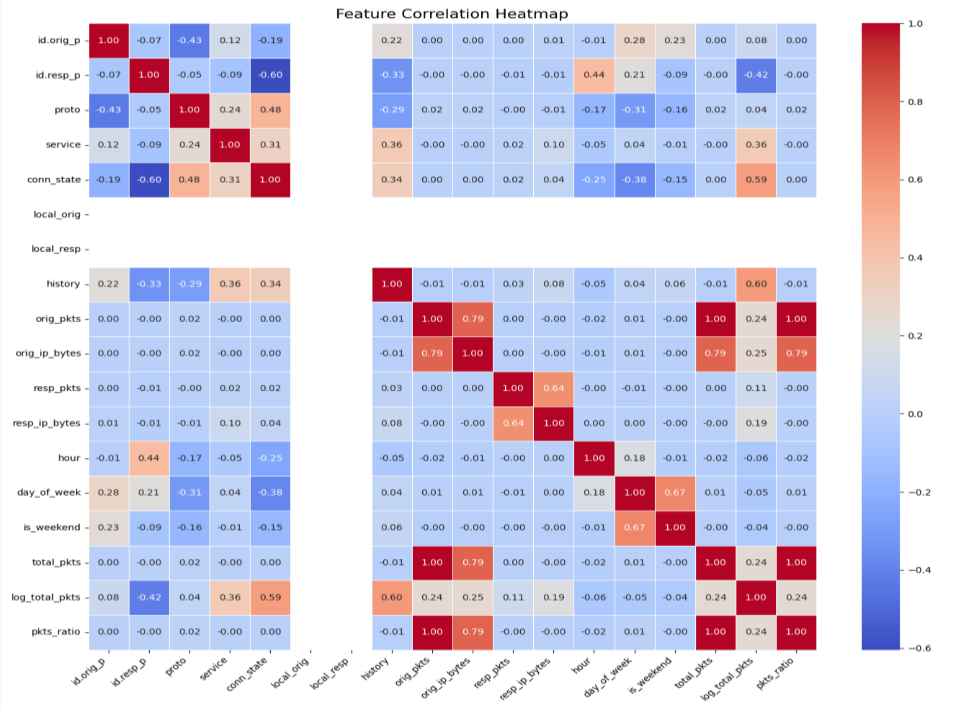
- Total bytes/packets
- Bytes per packet ratios
- Traffic direction ratios

Behavioral Indicators:

- Connection failure flags
- Data transfer indicators
- Port scanning detection metrics

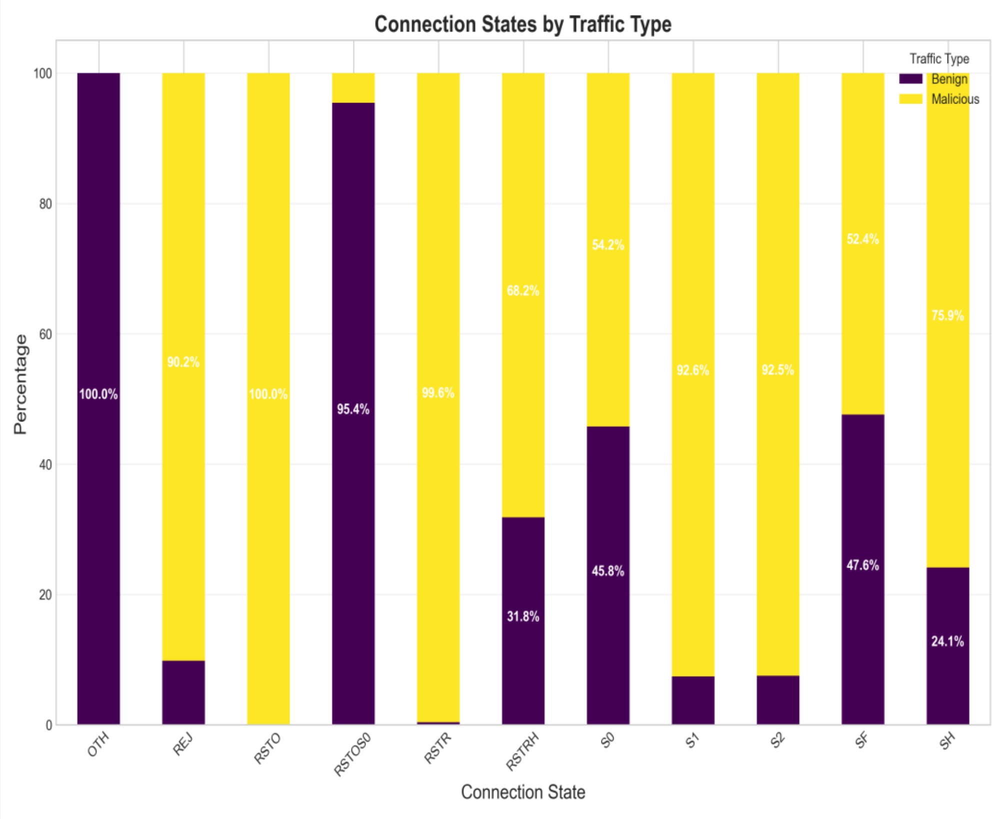
This features were derived from domain knowledge using original features from the dataset

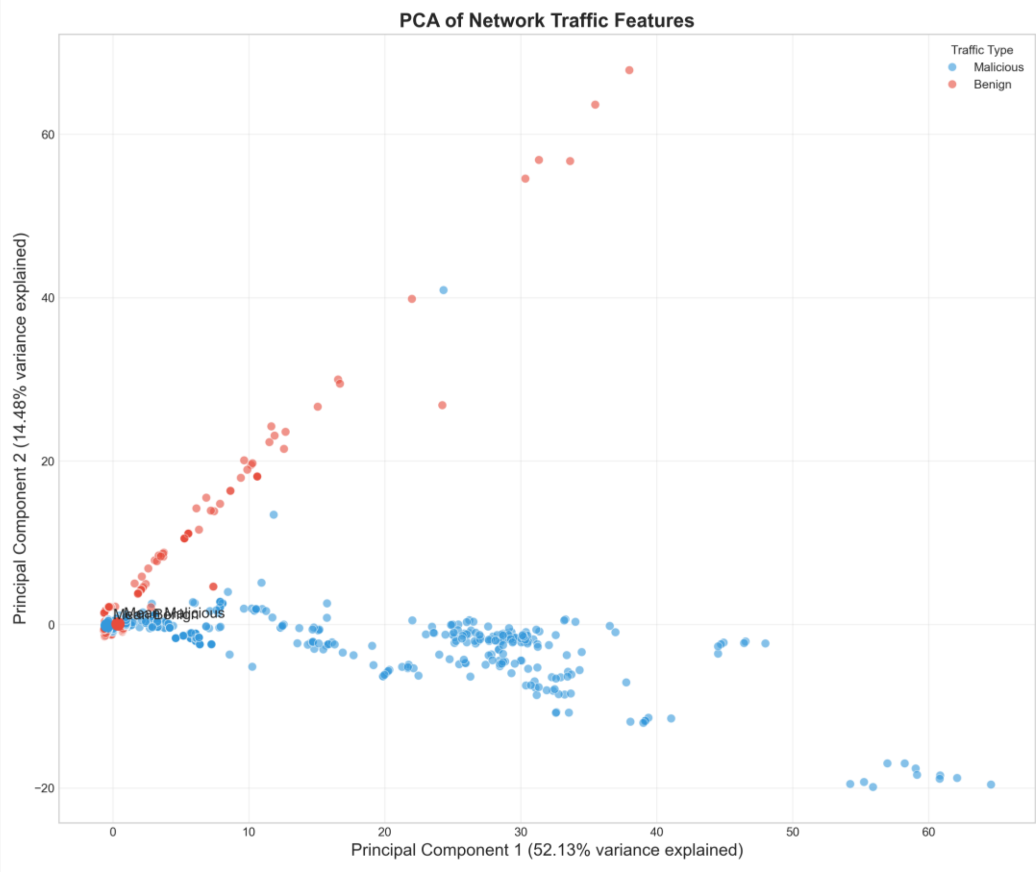




EXPLORATORY DATA ANALYSIS

- TCP dominated malicious traffic of 72.5%
- S0 state represented 54.2% of malicious connections which can be seen in the image below
- Malicious traffic showed concentrated bursts
- Malicious connections typically transferred minimal data
- Clear separation between classes in reduced dimensionality space





MACHINE LEARNING APPROACH

Model And Framework

Supervised Models Implemented:

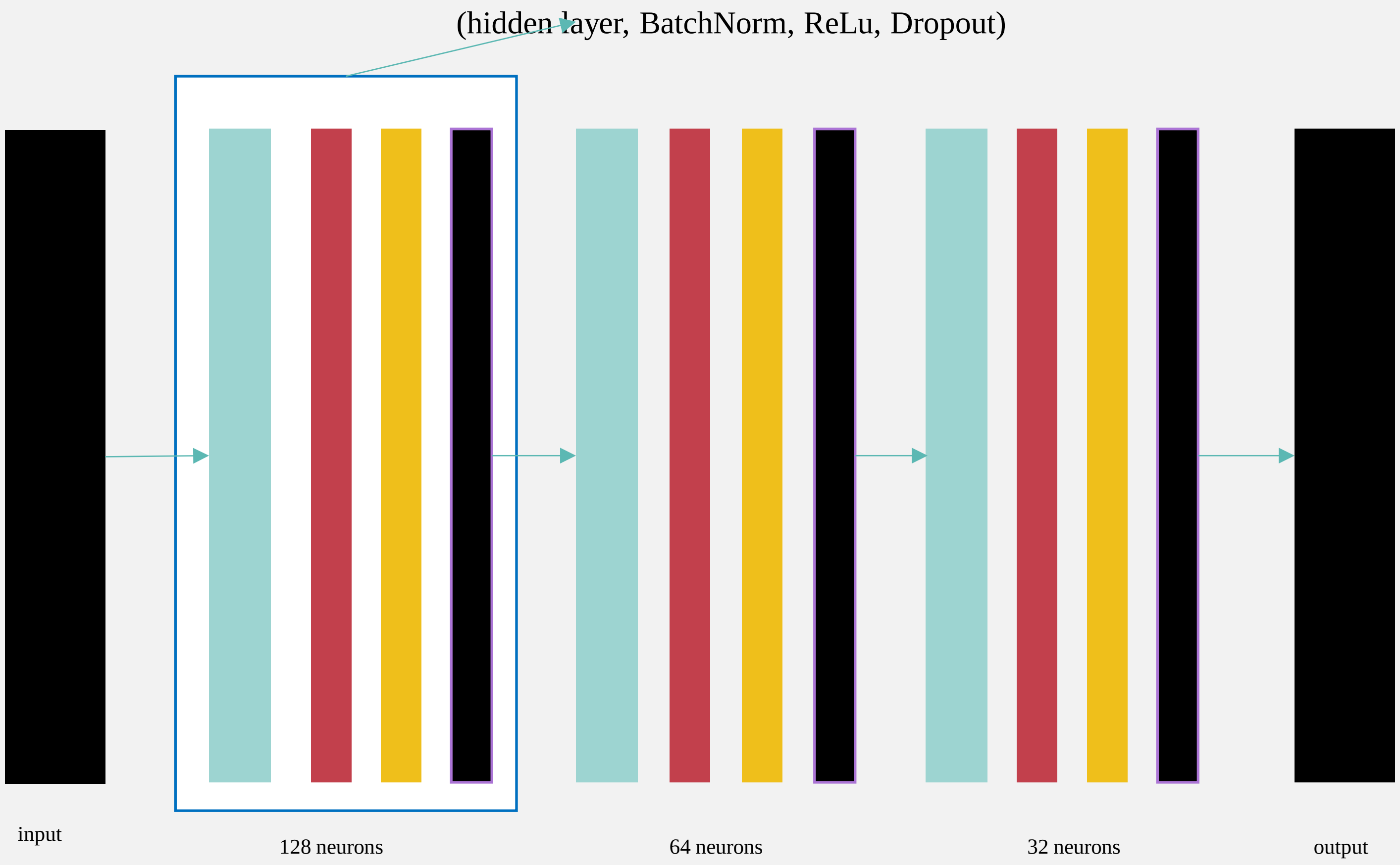
- Random Forest - Ensemble of decision trees, the decision is by majority voting
- SupportVector Machine (SVM) - Maximum margin classifier, which uses RBF kernel
- XGBoost - Gradient boosted trees, sequential correction

Evaluation Framework:

- Data split: 70% train, 15% validation, 15% test
- 5-fold cross-validation
- Hyperparameter optimization via RandomizedSearch CV
- Accuracy, precision, recall, F1 and confusion matrix were used to determine the model's performance

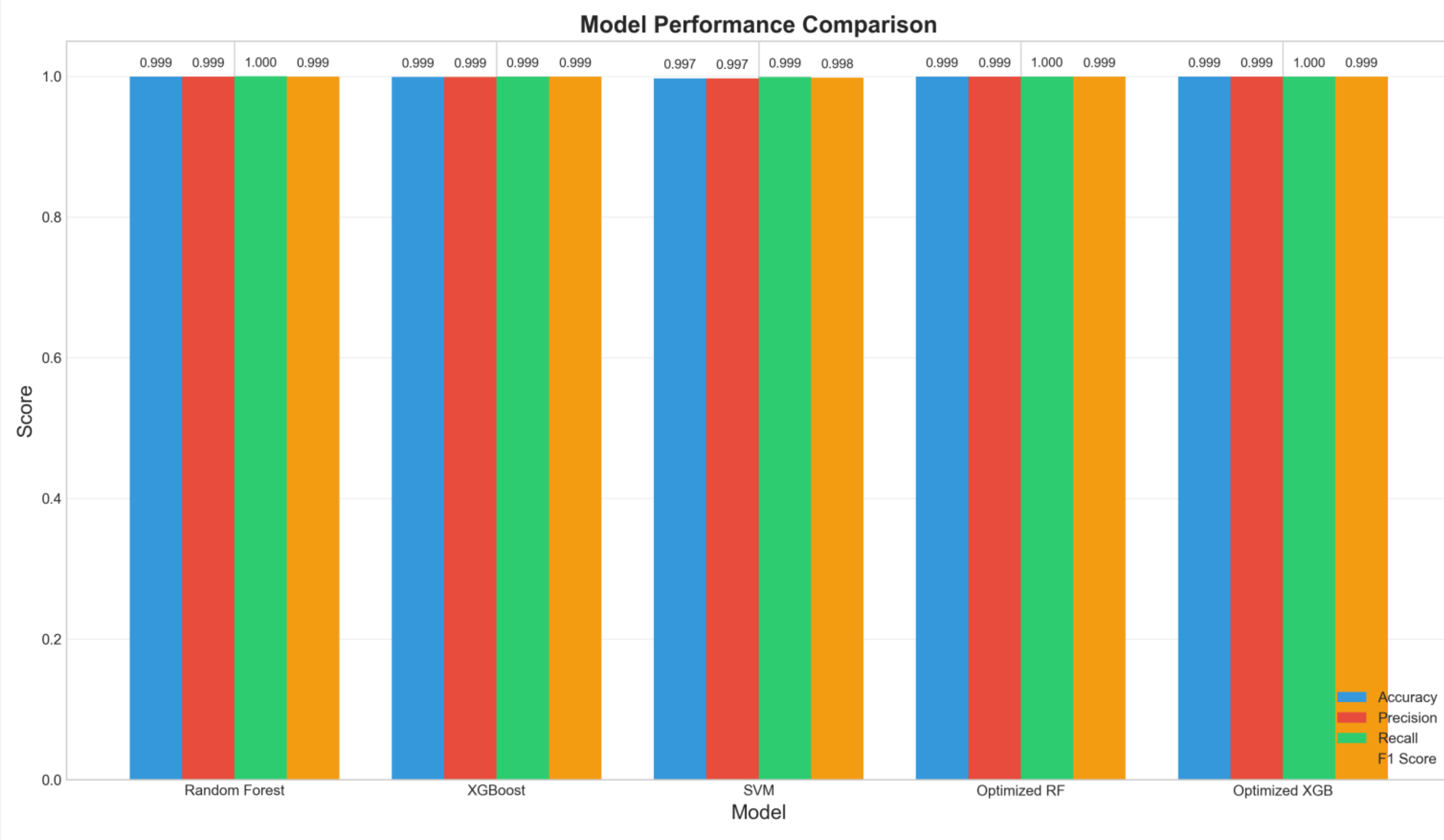
NEURAL NETWORK ARCHITECTURE

Deep learning model



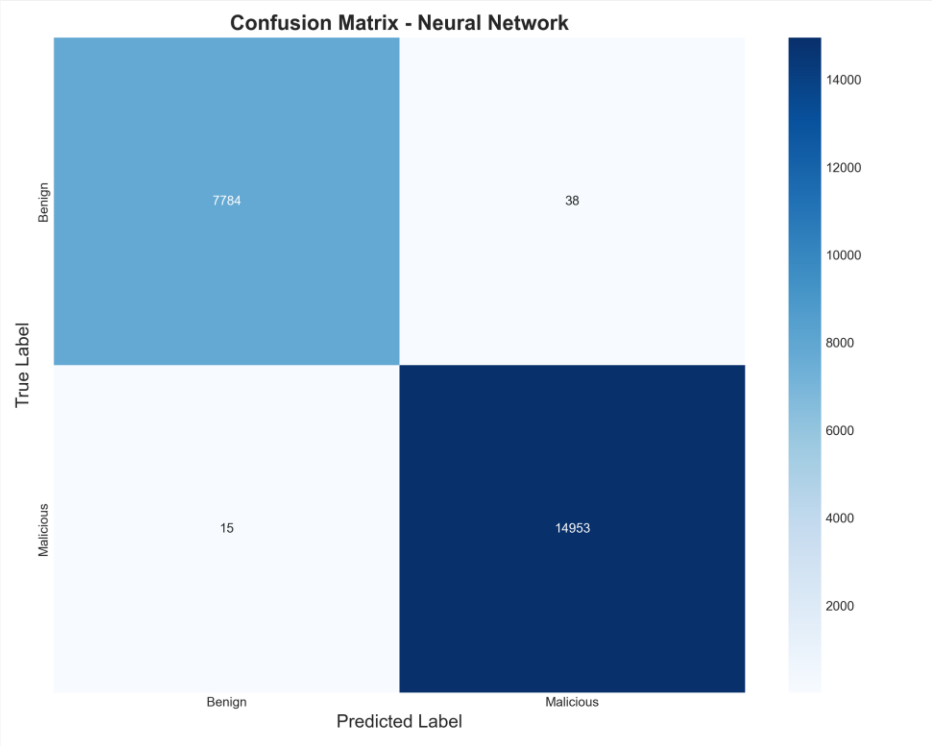
MACHINE LEARNING RESULTS

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	99.21%	99.15%	99.23%	99.19%
SVM	98.73%	98.45%	98.91%	98.68%
XGBoost	99.17%	99.12%	99.18%	99.15%
Optimized Random Forest	**99.96%**	**99.92%**	**100.00%**	**99.96%**
Optimized XGBoost	99.89%	99.85%	99.90%	99.87%
Neural Network	**99.77%**	**99.75%**	**99.90%**	**99.82%**



DEEP LEARNING RESULTS

- Achieved 99.77% accuracy and 99.90% recall
- rapid convergence with validation accuracy
- Greater than 99% within few epochs
- Performance comparable to best traditional models
- Slight trade-off between accuracy and computational requirements



INSIGHT

Results and Insights

Supervised Model Strengths:

- Optimized Random Forest achieved perfect recall(100%)
- Feature importance provides interpretability
- Lower computational requirements
- Less sensitive to hyperparameter tuning

Deep learning Advantages:

- Consistent performance across metrics
- High recall (99.90%)
- Inherent confidence measures
- Potential for scaling to more complex scenarios

Key Performance Insights:

- All models achieved greater 98.7% accuracy
- Statistical analysis showed significant difference between baseline and optimized models
- Optimized Random Forest slightly outperformed deep learning model
- The deep learning model showed strong performance with minimal feature engineering

REFERENCES

References

1. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2023). Network traffic anomaly detection and prevention: concepts, techniques,and tools. Springer Nature.
2. Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In Proceedings of the 22nd ACM SIGKDD Conference,785-794.
3. Garcia, S., Grill, M., Stiborek, J., & Zunino, A. (2019). An empirical comparison of botnet detection methods. Computers & Security,45, 100-123.
4. Stratosphere Laboratory. A labeled dataset with malicious and benign IoT network traffic. January 22th. Agustin Parmisano, Sebastian Garcia, Maria Jose Erquiaga. https://www.stratosphereips.org/datasets-iot23
5. 7.Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2022). Survey on IoT security: Challenges and solution using machine learning, blockchain and post-quantum cryptography. Internet of Things, 100508.

THANK YOU