A REAL-TIME RESEARCH PROJECT REPORT

ON

DETECTION OF ACCOUNT TAKEOVER USING MACHINE LEARNING MODELS

submitted in partial fulfillment of the requirements for the award of the degree

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

by

[Your Name] [Roll Number]

Under the Guidance of

[Guide Name]

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR TECHNICAL CAMPUS

ABSTRACT

This project focuses on detecting account takeovers using machine learning techniques...

TABLE OF CONTENTS

1. INTRODUCTION

Account takeovers pose a significant cybersecurity threat...

2. LITERATURE SURVEY

Existing research highlights various approaches to fraud detection...

3. ANALYSIS AND DESIGN

Dataset Description:

- Login Timestamp

- User ID

- IP Address

- Device Type

- Login Successful

- Is Attack IP

- Is Account Takeover

4. IMPLEMENTATION

Machine Learning Models Used:

- Logistic Regression

- Decision Tree

- Random Forest

- AdaBoost

- XGBoost

5. TESTING AND RESULTS

Model Performance Metrics:

| Model | Accuracy | AUC Score |

|------|------|------|

| Logistic Regression | 99.99% | 0.867 |

| Decision Tree | 99.99% | 0.625 |

| Random Forest | 99.99% | 0.857 |

| AdaBoost | 99.99% | 0.978 |

| XGBoost | 99.99% | 0.985 |

6. CONCLUSION

This study demonstrated the effectiveness of machine learning models in detecting fraudulent account takeovers...

7. REFERENCES

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

2. Hastie, T., Tibshirani, R., & Friedman, J. (2009). The Elements of Statistical Learning. Springer.

3. Scikit-learn Documentation. https://scikit-learn.org/stable/