HACK THE FUTURE

TEAM OF ABSOLUTES

Cryptography

Objective

Objective:
To develop an AI/ML-based solution that automatically analyzes cryptographic algorithms, identifies vulnerabilities, and suggests enhancements for stronger cybersecurity protocols.

Approach:
We created synthetic datasets using Python scripts, generating ciphered text from plaintext and encryption keys. We then trained different machine learning models to classify the encryption algorithm used, based solely on the ciphered text.

Overview:

- Use AI/ML algorithms to detect and classify cryptographic algorithms in datasets.
- Identify potential security weaknesses through pattern recognition and anomaly detection.
- Provide real-time vulnerability assessment to enhance encryption methods.

Key Features

Dataset Generation:
We generated synthetic cipher text using multiple encryption algorithms, ensuring:

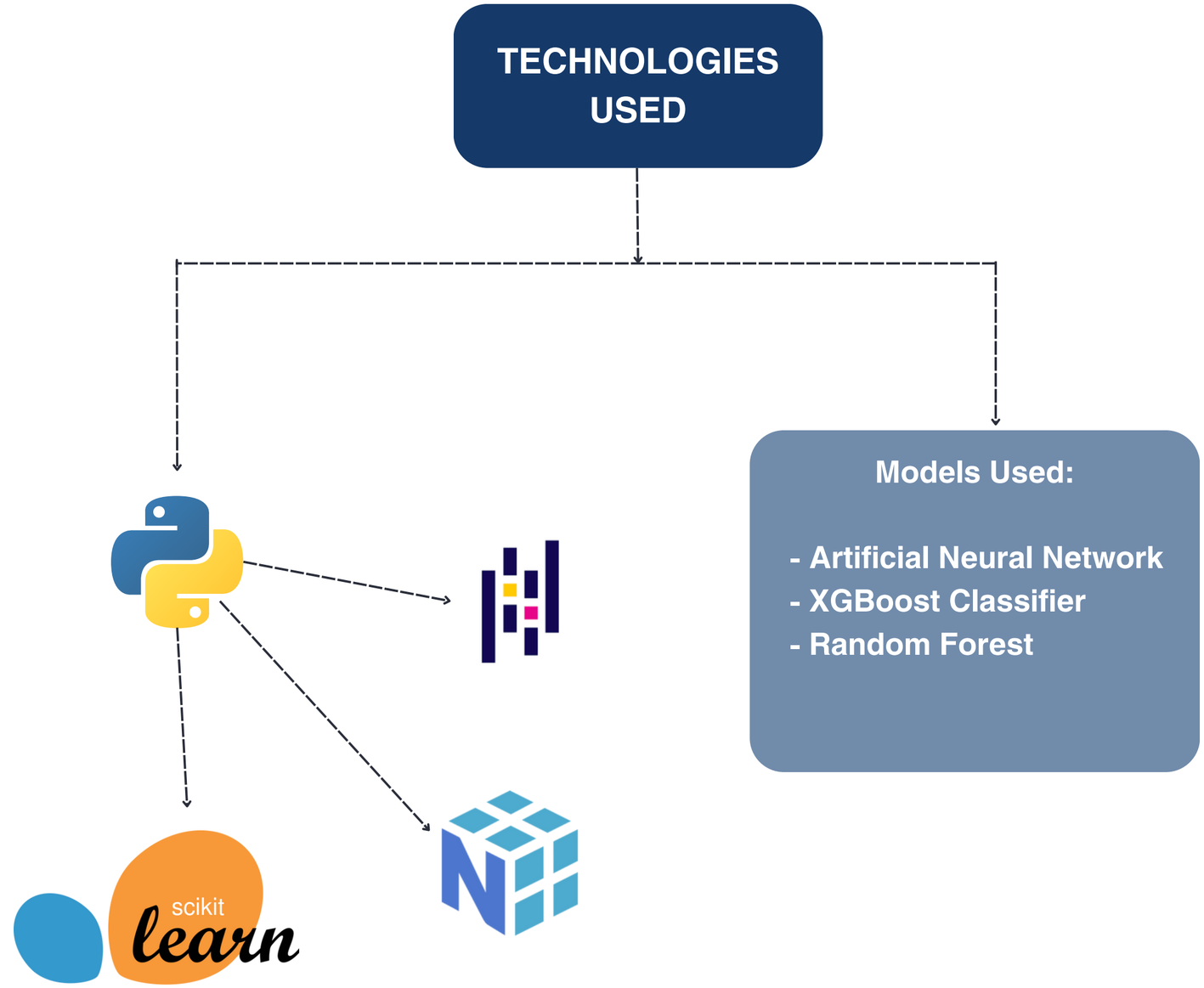
- Different key sizes and encryption methods.
- Various levels of randomness and complexity.
- Enough samples for effective model training and testing.

Automated Cryptographic Algorithm Detection:
Automatically identifies and classifies cryptographic algorithms used in datasets without manual intervention.

Vulnerability Identification & Classification:
Uses machine learning models to detect patterns indicative of security weaknesses in cryptographic implementations.

Security Enhancements:
Beyond identifying cryptographic methods, we introduced:

- Obfuscation Layer: Post-encryption obfuscation to reduce ML model accuracy and enhance security.
- XOR Masking: Adding a lightweight XOR-based security layer to alter the cipher text.
- Byte Shuffling: Rearranging bytes to prevent direct pattern recognition.



SOLUTIONS IMPLEMENTED

Dataset Preparation

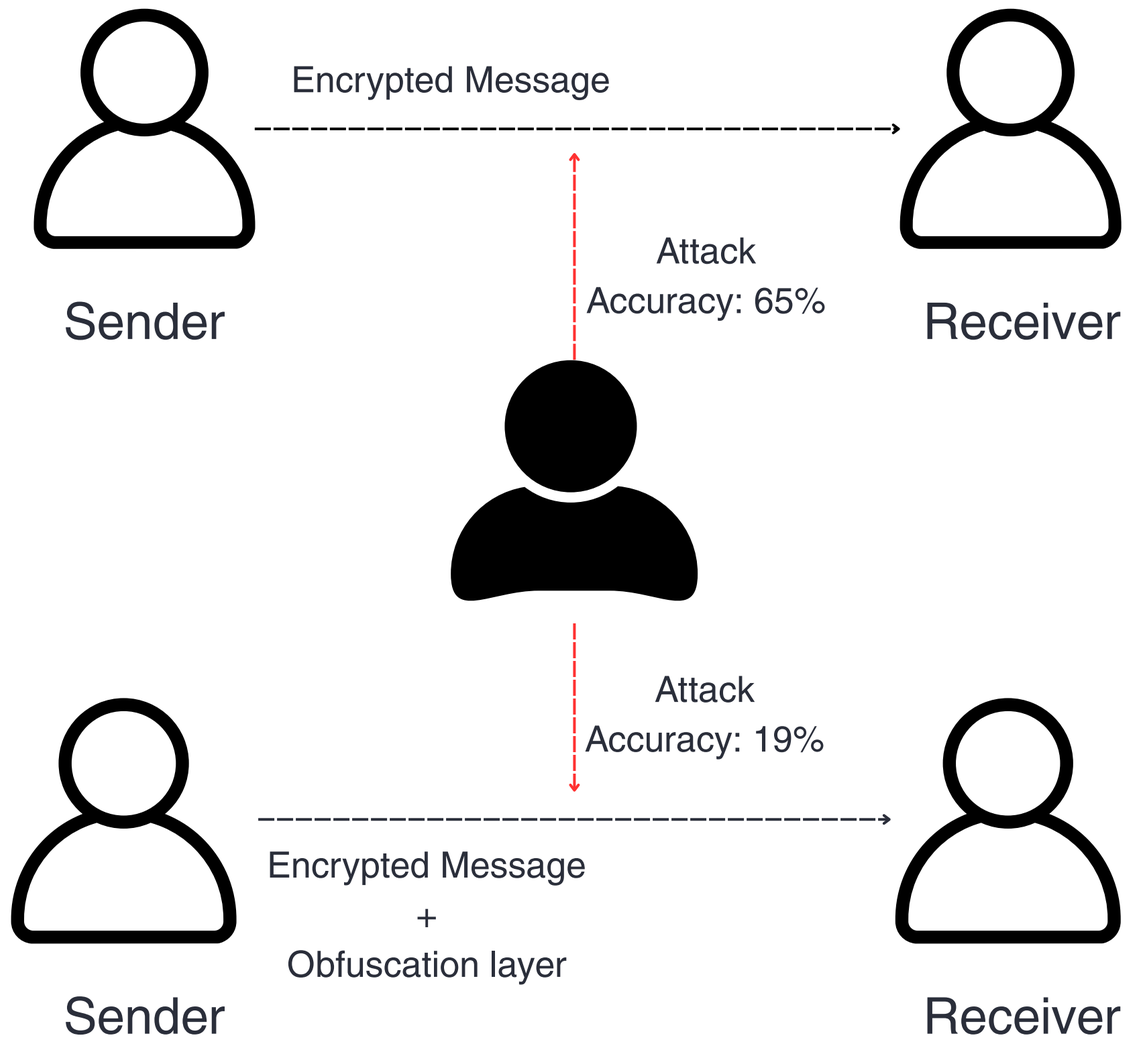
- Collected encrypted data samples
- Applied preprocessing techniques: normalization, feature extraction

Model Training:

- Trained supervised models for classification
- Used unsupervised learning for anomaly detection

Vulnerability Assessment:

- Developed real-time monitoring algorithms
- Integrated AI/ML models with cybersecurity dashboards for continuous analysis



Challenges Faced

Data-Related Challenges:

- Limited availability of diverse cryptographic datasets
- Difficulty in feature selection for complex encryption schemes

Model Performance Issues:

- High false positive rates in initial models
- Overfitting due to insufficient training data

Real-Time Assessment Limitations:

- Latency issues in processing large datasets
- Difficulty in integrating with existing cybersecurity infrastructures