TEKATHON-3.0- 2024

- **Problem Statement ID – 1681**
- **Problem Statement Title - Identification of algorithm from the given dataset using AI/ML Techniques.**
- **Theme - Blockchain & Cybersecurity**
- **PS Category- Software**
- **Team Name (Registered on portal) - whichCrypt**

SMART INDIA HACKATHON 2024

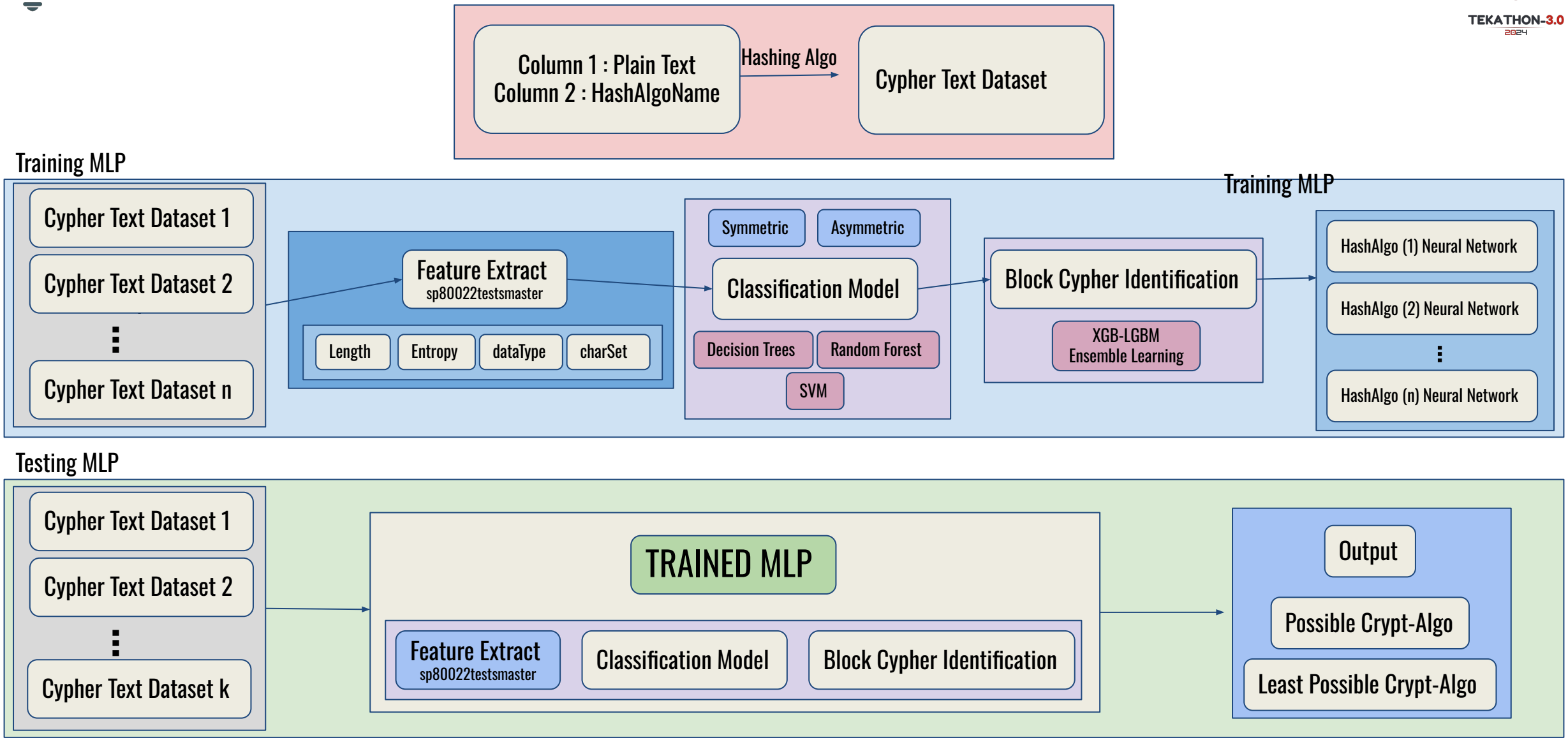
Neural Hash Predictor

TEKATHON-3.0 2024

AI/ML Model to predict crypto-algorithms

- **whichCrypt** is an AI/ML-Powered tool which is based on Classification models (such as Decision Trees and Random Forest) and is trained on a large labeled dataset of hashes.
- Our tool can accurately identify cryptographic algorithms by leveraging advanced machine learning models like Ensemble Learning (XGB-LGBM) and cryptography info to analyze ciphertext and infer the underlying algorithm.
- The solution employs various AI/ML models, such as supervised learning classifiers, deep learning networks, and feature extraction techniques, to analyze the datasets properly & provide accurate output. These models are trained on labeled datasets where the cryptographic algorithm is known, allowing them to learn the distinguishing features of each algorithm. Once deployed, these models can effectively identify the algorithms used in new, unseen datasets with certainty upto 97%.
- Our solution significantly increases the efficiency by classifying the value in the input data/dataset as symmetric and asymmetric in the initial stages of classification.
- It significantly increases the efficiency by determining symmetric and asymmetric values and furthermore increases the efficiency even more by identifying the block cipher. .

OUR APPROACH



SMART INDIA HACKATHON 2024

FEASIBILITY AND VIABILITY

TEKATHON-3.0 2024

- The application of AI/ML to cryptographic algorithm identification through dataset analysis or hexadecimal hashing is technologically possible. However, data-related challenges must be addressed to ensure its practical viability.
- To handle confidential data of ministries, all the datasets, model and connections should be generated locally on a single machine.
- Potential challenges include privacy risks associated with datasets, the computational resources needed for training models on large datasets, the potential for inaccuracies when applied to new, unseen data, and the risk of adversaries manipulating training data to compromise model performance.
- To make the model more robust and resistant to adversaries, it is necessary to train it with false data for the machine to recognize fake hashes.

SMART INDIA HACKATHON 2024

IMPACT AND BENEFITS

TEKATHON-3.0 2024

• IMPACTS

1. Potential Data Breaches & Cyber Attacks can be detected in real time scenarios such as Financial systems and defence, where real-time security is extremely crucial
2. This solution can serve as a foundation for better research in cryptanalysis leading to development of more advanced cryptographic algorithms.
3. Automated solutions reduce the dependency on highly specialized cryptography experts, making cryptographic analysis & security operations more accessible and cost-effective.
4. By identifying potentially weak or outdated cryptographic methods, organizations can better manage risks associated with data protection.

• Benefits

1. The system's ability to adapt to new cryptographic algorithms as they emerge ensures that it remains relevant and effective over time.
2. It significantly increases the efficiency by determining symm and asymm values and furthermore increases the efficiency even more by identifying the block cypher.
3. After a security breach, the solution can be used during **Post-Attack Forensics** to analyze encrypted data and identify the cryptographic methods used by attackers, aiding in understanding the breach and preventing future incidents.
4. This solution could be scaled across various Industries & environments allowing organizations to effectively manage & update their cyber security practices.

SMART INDIA HACKATHON 2024

RESEARCH AND REFERENCES

TEKATHON-3.0 2024

- www.scopus.com
- https://pytorch.org/docs/stable/index.html
- https://www.tensorflow.org/api_docs
- https://scikit-learn.org/0.21/documentation.html
- https://kivy.org/doc/stable/