Smart India Hackathon 2024

SMART INDIA HACKATHON 2024

शिक्षा मंत्रालय
MINISTRY OF EDUCATION

About us, Our

Team name : whichCrypt

Team ID :

Theme : Blockchain & Cybersecurity

PS Category : Software

Problem Statement ID : 1681

Problem Statement : Identification of algorithm from the given dataset using AI/ML Techniques.

Neural Hash Predictor

AI/ML Model to predict crypto-algorithms

- **whichCrypt** is an AI/ML-Powered tool which is based on CNN (Convolutional Neural Network) and is trained on a large labeled dataset.
- Once deployed, Our **whichCrypt AI** can precisely identify which cryptographic algorithm is being used on a dataset/cipher with a certainty up to 97%.
-

Our Approach

SMART INDIA
HACKATHON
2024

Feasibility and Viability

AI/ML Model to predict crypto-algorithms

- 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.
- 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. Lightweight architectures and mechanisms allow algorithms to learn from new data with randomness and multiple model integration to avoid any compromise or wrong outputs while balancing computational and accuracy.

Impacts and Benefits

Impacts

- Potential Data Breaches & Cyber Attacks can be detected in real time scenarios such as Financial systems where real-time security is extremely crucial
- This solution can serve as a foundation for better research in cryptanalysis leading to development of more advanced cryptographic algorithms.
- Regular audits of cryptographic practices can be more thorough and accurate with automated tools, helping

Benefits

- Potential Data Breaches & Cyber Attacks can be detected in real time scenarios such as Financial systems where real-time security is extremely crucial
- This solution can serve as a foundation for better research in cryptanalysis leading to development of more advanced cryptographic algorithms.
- Regular audits of cryptographic practices can be more thorough and accurate with automated tools, helping

SMART INDIA HACKATHON 2024

Research and References

Our Backbone,

- **whichCrypt** is an AI/ML-Powered tool which is based on CNN (Convolutional Neural Network) and is trained on a large labeled dataset.
- Once deployed, Our **whichCrypt AI** can precisely identify which cryptographic algorithm is being used on a dataset/cipher with a certainty up to 97%.
-

SMART INDIA HACKATHON 2024