Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 11, November-2022

CryptoCam: An Approach to Enhance Cryptography with Machine Learning

Dhanraj Chavan
Department of Computer Science & Engineering
KIT's College of Engineering, Kolhapur
Kolhapur, Maharashtra, India

Abstract— **Every day, millions of text and other files are exchanged across the web. It is critical to safeguard the confidentiality and integrity of the data being sent. Cryptography plays a significant role in data security by providing different techniques. The computational difficulty of mathematical problems determines the security of cryptographic algorithms. Any breakthrough in the solution of such mathematical problems can expose a cryptographic technique. In this paper, the author will demonstrate a concept that can be used with machine learning to enhance cryptography. The paper summarizes the research done in this area & provides suggestions for future directions in research.**

Keywords*— *Cryptography, machine learning, cybersecurity, data security, data confidentiality, data integrity, encryption, decryption, security, cryptographic algorithms, cipher

I. INTRODUCTION

As the world is evolving, and the demand for information services is proliferating, the need for advanced methods of securing data has increased.

Modern cryptography is built on mathematics, computer science, and cleverness. Furthermore, various technologies can be integrated into the process of cryptography to enhance encryption and decryption. When we require a machine to learn to solve a problem based on previously provided data, we call this machine learning. Machine learning can be an effective solution finder for situations that do not have a clear algorithm to solve.

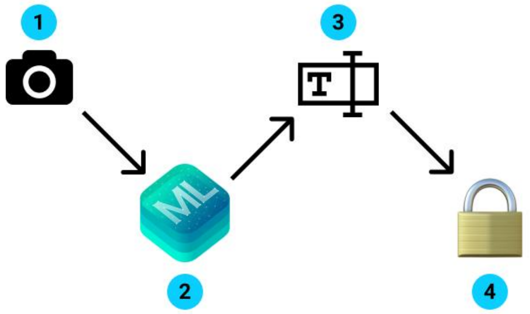
This paper presents an overview of a new approach to how various technologies can be integrated into the cryptography process to innovate the future of Data Security, Data Confidentiality & Data Integrity.

II. METHODS

CryptoCam aims to introduce & demonstrate a new concept of how machine learning can be used with cryptography to improve data security.

CryptoCam is a camera that uses Machine Learning to encrypt and decode data inside a physical item. CryptoCam uses VisionKit which provides the camera's live video used to recognize images or feed of objects & MobileNetV2 Machine Learning Model [1] which contains 53 layers of deep neural network and can categorize photos into 1000 categories.

A. Encryption:



Step 1:
Click on the "Encrypt" Button. Hold the camera steady focusing on the Object & it will capture the object.

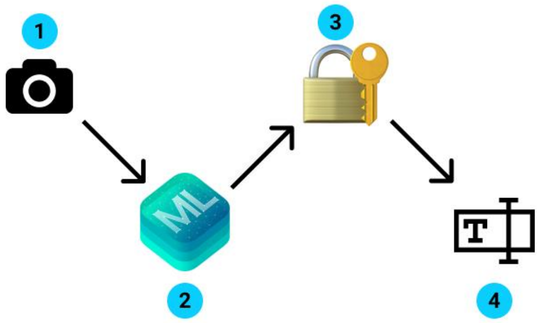
Step 2:
It will start to analyze & classify the image of the object. CryptoCam will use the MobileNetV2 ML model to identify the name of the object in the image frame.

Step 3:
It will provide an alert with the name of the detected object; validate the name of the object. If it's not correct, then feel free to scan it again.

Step 4:
In the Text Field, Add the message that you want to encrypt & tap on the "Save" button. CryptoData will save this encrypted message.

Your message is encrypted inside the object.

B. Decryption:



Step 1:
Click on the "Decrypt" Button & Hold the camera steady focusing on the Object.

Step 2:
It will start to analyze & classify the image of the object. After finishing the countdown, it will identify the name of

the object in the camera frame using ML Model & VisionKit.

Step 3:

If the indicated item is found in CryptoData, the message will be decrypted. After decrypting the message successfully, it will play the Success sound. Otherwise, it will play a Fail sound if the object is not found.

Step 4:

The message is decrypted.

III. RESULTS

In basic cryptography [2], encryption requires two parameters: plaintext & key whereas decryption requires two parameters: encrypted text & key. In the case of CryptoCam, it uses the same key for both encryption & decryption. Let's break down the process of Cryptocam & understand how the key is created dynamically with the help of an example.

1. Consider an object in our day-to-day life. Ex. Keyboard
2. When a user scans & captures the object using encrypt button, the live feed is monitored in real-time.
3. After the countdown finishes, the feed is passed to the MobileNetV2 ML model.
4. MobileNetV2 analyzes the feed & gives a result in the dictionary format. This dictionary is an array of key-value pairs where the key is the object name & value is the confidence percentage.
5. CryptoCam uses the top 5 results from the dictionary to create a dynamic key which is required for encryption.
6. An alert with the top 3 results & a text field will be shown where the user can verify the identity of the object & add a message in the text field.
7. CryptoCam will use the top 5 results as a key & user input as plaintext to encrypt.
8. For a demonstration of this concept, it will only store the combination of the top 5 results & plaintext. No further encryption algorithm is used. In the future, it will be stored & retrieved using a specific cryptographic algorithm. AppStorage database from Apple Developer is used to store all the values.
9. For decryption, if you scan the same object, MobileNetV2 will identify the object & gives a result in the form of a dictionary.
10. CryptoCam will use the top 3 results in decryption. If these top 3 results are found in the stored results of AppStorage, the decrypted message will be shown to the user.
11. If these top 3 results do not found in the top 5 results of any stored results of AppStorage, it will throw an error that indicates that identification has failed.

IV. DISCUSSION

The concept of the cryptographic algorithm used in CryptoCam is based on Object Identification done by MobileNetV2 ML Model. CryptoCam stores the results in AppStorage in a non-encrypted form. CryptoData is referred to as AppStorage here.

MobileNetV2 [1] has been trained to identify the dominating object in a camera frame or image. It has 75% top 1 accuracy & 92.5% top 5 accuracy [3].

For the demonstration purpose of this concept, top(top 5 for encryption, top 3 for decryption) results with high confidence values are chosen to maintain accuracy. To achieve high accuracy, other models can be used, but the size of the model increases as accuracy increases. To eliminate the size issue of the ML model, the ML model can be hosted on any cloud service & applications can connect to it via APIs. Hence, high accuracy with low size can be achieved in the future.

This project aimed to demonstrate a new concept of how Machine Learning can be used with Cryptography.

REFERENCES

[1] MobileNetV2, Apple Developer CoreML Models

[2] Wade Trappe, Lawrence C. Washington - "Introduction to Cryptography with Coding Theory"

[3] MobileNetV2, TensorFlow Models, GitHub(tensorflow/models)