For Your Keys Only (FYKO)!

Local storage supported. ANN model will be stored in localstorage

Illustrating ANN model fetch in tfjs format followed by secure message exchange...

Step1: Prepare a payload to request a Simple ANN Model from Server. Payload = {"format":"tfjs"}

Step2: Fetch a Simple ANN Model in TFJS Format

Response from Server = { "ann_id": "simple_tfjs_model_1683982529.550654", "format": "tfjs", "is_encrypted": false }

ANN ID obtained from Server = simple_tfjs_model_1683982529.550654

Step 3: Form the url to load model.json. URL = http://localhost:8000/tfjs/simple_tfjs_model_1683982529.550654/model.json

Step 4: Load the tfjs model using tf library
Model simple_tfjs_model_1683982529.550654 loaded into localstorage.

Step 5: Use the ANN model to generate AES Key
Current UTC Time in Seconds = 1683982530
Random String = c278e4ad-bd52-4b34-9ac0-78abd686faf5
Get MD5 Hashes of current UTC seconds and random string. Combine their binary bits and feed into ANN.

AES Key Generated = f22cc0c673a54b9ecf1925c5b2ad3526f706454dd7e5c53f983114f4ad1e8b4c

Step 6: Prepare a secret message to be sent to the server using AES Key generated.

secret_message = message id:a593e91d-3d17-416b-a238-91b49e75f417 English: FYKO is a cool project Telugu: FYKO ఒక మంచి ప్రాజెక్ట్ Hindi: FYKO एक अच्छा प्रोजेक्ट है Portugese: FYKO é um projeto legal Thai: FYKO **เป็นโครงการที่ยอดเยี่ยม** Chinese: FYKO是一個很酷的項目 Japanese: FYKOはクールなプロジェクトです Korean: FYKO는 멋진 프로젝트입니다 Irish: Is tionscadal fionnuar é FYKO Arabic: FYKO مشروع رائع

secret_message_uri_encoded = message%20id%3Aa593e91d-3d17-416b-a238-
91b49e75f417%0AEnglish%3A%20FYKO%20is%20a%20cool%20project%20%0ATelugu%3A%20FYKO%20%E0%B0%92%E0%B0%95%20%E0%B0%AE%E0

secret_message_b64_string =
bWVzc2FnZSUyMGlkJTNBYTU5M2U5MWQtM2QxNy00MTZiLWEyMzgtOTFiNDllNzVmNDE3JTBBRW5nbGlzaCUzQSUyMEZZS08lMjBpcyUyMGElMjBjb

encrypted_message =
1aPCzuBs4OLAid7f9w101oTaHNZfvjJJ2cz/WrRW9bB0ySvncurRUStc397w0XnSzxtHWtpdZ5fudgSRmHw1s46YMJ+OxS8PnJ91CVVGqevv8z/ccsjd48HKrMkP/r

Step 7: Send encrypted message to server

Sending message = {"format":"tfjs","is_message_uri_encoded":true,"random_string":"c278e4ad-bd52-4b34-9ac0-
78abd686faf5","utc_time_seconds":1683982530,"encrypted_message":"1aPCzuBs4OLAid7f9w101oTaHNZfvjJJ2cz/WrRW9bB0ySvncurRUStc397w0XnSzxtHWtpd

Step 8: Verify if Server is able to decrypt the message correctly

Response from server after decoding = { "request_message": "message id:a593e91d-3d17-416b-a238-91b49e75f417\nEnglish: FYKO is a cool project \nTelugu: FYKO \u0c12\u0c15 \u0c2e\u0c02\u0c1a\u0c3f \u0c2a\u0c4d\u0c30\u0c3e\u0c1c\u0c46\u0c15\u0c4d\u0c1f\u0c4d \nHindi: FYKO \u090f\u0915 \u0905\u091a\u094d\u091b\u093e \u092a\u094d\u0930\u094b\u091c\u0947\u0915\u094d\u091f \u0939\u0948 \nPortugese: FYKO \u00e9 um projeto legal \nThai: FYKO \u0e40\u0e1b\u0e47\u0e19\u0e42\u0e04\u0e23\u0e07\u0e01\u0e32\u0e23\u0e17\u0e35\u0e48\u0e22\u0e2d\u0e14\u0e40\u0e22\u0e35\u0e48\u0e22\u0e21 \nChinese: FYKO\u662f\u4e00\u500b\u5f88\u9177\u7684\u9805\u76ee \nJapanese: FYKO\u306f\u30af\u30fc\u30eb\u306a\u30d7\u30ed\u30b8\u30a7\u30af\u30c8\u3067\u3059 \nKorean: FYKO\ub294 \uba4b\uc9c4 \ud504\ub85c\uc81d\ud2b8\uc785\ub2c8\ub2e4 \nIrish: Is tionscadal fionnuar \u00e9 FYKO \nArabic: FYKO \u0645\u0634\u0631\u0648\u0639 \u0631\u0627\u0626\u0639" }

Original Message: = message id:a593e91d-3d17-416b-a238-91b49e75f417 English: FYKO is a cool project Telugu: FYKO ఒక మంచి ప్రాజెక్ట్ Hindi: FYKO एक अच्छा प्रोजेक्ट है Portugese: FYKO é um projeto legal Thai: FYKO **เป็นโครงการที่ยอดเยี่ยม** Chinese: FYKO是一個很酷的項目 Japanese: FYKOはクールなプロジェクトです Korean: FYKO는 멋진 프로젝트입니다 Irish: Is tionscadal fionnuar é FYKO Arabic: FYKO مشروع رائع

Message decoded by Server: = message id:a593e91d-3d17-416b-a238-91b49e75f417 English: FYKO is a cool project Telugu: FYKO ఒక మంచి ప్రాజెక్ట్ Hindi: FYKO एक अच्छा प्रोजेक्ट है Portugese: FYKO é um projeto legal Thai: FYKO **เป็นโครงการที่ยอดเยี่ยม** Chinese: FYKO是一個很酷的項目 Japanese: FYKOはクールなプロジェクトです Korean: FYKO는 멋진 프로젝트입니다 Irish: Is tionscadal fionnuar é FYKO Arabic: FYKO مشروع رائع

Is the original secret message sent equal to the request message in response: = true

Step 9: Replay Attack Scenario
Response from server ={ "error_message": "Stale Request: Rejecting it" }

Step 10: Send future message
Response from server ={ "error_message": "Request from the future: Rejecting it" }