TO WHOMSOEVER IT MAY CONCERN

My internship experience in detail:

I worked as Software Developer + Machine Learning Intern for almost an year at Zimperium Inc. I worked for Zimperium Inc from May 2022 to May 2023 (Full Time 40 hours per week) during my Masters for three semesters (with courses).

Worked on Java, Spring boot, Microservices architecture, RESTful API Calls, testing API endpoints using Postman. I learnt usage of Docker services, kunernetes containers. PostgresSQL, ElasticSearch, Open search databases in the backend for storage of Data.Also, have deployed features on various environments (Dev, staging, prod) using Git. Asked for Peer Review from Senior Developers and implemented the changes. Updated progress on Various JIRAs and confluence with satisfactory close. On Machine Learning Side, I have deployed three Machine Learning Models in prod environment. Also set up Data fetch cycle in Kunernetes by writing a script and training the model on the new data and give predictions. Integration of the trained model using Python, Flask and display the result on API endpoints calls. Used Blueprint controller to set the API endpoints, decided the routes and controllers.worked with data fetched from AWS S3 and Athena. Have worked unstructured data and structured data respectively. Preprocessed both the data and integrated it. Plotted the data to read it and visualized, understand the pattern (what useful data is saying) and what insight/ prediction can be captured. I tried to do this, and brought a very new idea-- useful prediction which in their previous analysis was missing. Now it's gone in prod. I detected anamoly behavior of threats among different market categories that a hacking app falsely portays. It's accuracy is 96.42 percent. Had done a comparative analysis on XGBoost , Random Forest Classifier, KNN with accuracy as metric.

Background Information about Zimperium Inc and the dataset collected for ML, I worked for from May 2022 to May 2023 (Full Time 40 hours per week) during my Masters for three semesters (with courses).

- Zipps app is the mobile threat defense app developed by Zimperium Inc. Zimperium Inc provides Cybersecurity solutions to protect your private data.
- These solutions can be used by large company enterprises/ organizations who want to provide safety of data in work profile mode in mobiles used by their employees.
- And provide multiple features like safe browsing web, review apps for privacy and security risks before downloading, check network connections for reported malicious activity or in nearby threat zones, also helps eliminate mobile malware.
- The data collected in dataset for analysis is by Zipps app. Zipps app in work profile mode in mobile will keep a track of other apps accessing your private data with any permissions the other apps are given. And will notify whenever an app is trying to access any private data. The access can be either anonymous or with user's permission, here, the user decides which data access is threat or not.
- Also, the very sole purpose of this project was to detect anomaly behavior of apps trying to access private data with user permissions saying it's a Finance app (a particular market category app) when its not.

- On Play store or app store, we have apps associated with market categories. Eg: Chase app, Wells Fargo app, etc are Finance apps. Youtube, Netflix are entertainment apps, Whatsaap, LinkedIn are Social networking apps.
- The Zipps app generates a detection ID of identified threats based on CVE Ids (Common Vulnerability Exposure IDs) they are publicly available and the whole industry considers CVE IDs as a basic standard catalog to keep track of cybersecurity vulnerabilities.
- The dataset has data captured by Zipps app. This Data has a list of detection Ids detected for a particular app belonging to a specific market category.