netidee

STIPENDIEN

Mail authorship verification and phishing recognizing with machine learning on iOS

Zwischenbericht | Call 14 | Stipendium ID 4407

Inhalt

1 Einleitung

Dieser Zwischenbericht dient der Schaffung eines Überblicks über den Fortschritt des Projektes bzw. der damit verbundenen Masterarbeit. Offizieller Start war im November 2019, geplante Abgabetermin der Masterarbeit ist spätestens 19. Mai 2020 (= erster möglicher Termin für Masterarbeiten im Jahr 2020 an der FH Joanneum, Studiengang IT- and Mobile Security). Somit ist mit Anfang Februar rund 40% des Gesamtlaufzeit absolviert.

Der aktuelle Status der Masterarbeit ist zusammenfassend folgender: Der zu entwickelte Prototype einer iOS-App ist fertiggestellt und dessen Source-Code ist auf GitHub verfügbar. Die nötigen Datensets für die Evaluierungen, mit welchen die Forschungsfragen beantwortet werden, wurden zusammengestellt und für die Durchführung der Evaluierungen vorbereit. Auch die Durchführung der Evaluierungen ist bereits abgeschlossen, sodass alle nötigen Daten zur Beantwortung der Forschungsfragen nun vorliegen. Die Masterarbeit selbst (wissenschaftliche Ausarbeitung) ist in einer ersten Version fertiggestellt. Das heißt, dass diese erste Version schon alle nötigen Kapitel enthält und auch alle formalen Kriterien erfüllt. Jedoch ist hierzu das erste Feedback des Betreuers noch ausständig. Anhand dieses Feedbacks wird eine inhaltliche Finejustierung erfolgen sowie eine orthograhischer und grammatikalischer Check.

GitHub-Link: https://github.com/cfinker/postal-demo-extended-with-authorship-verification

2 Status

2.1 Meilenstein 1 – Implementierung iOS-App (Prototyp)

Status: abgeschlossen

Die Implementierung der iOS App umfasst, die Verwendung des Framework Postal zur Erstellung eines reduzierten Mail-Clients. Dieser wird mit uClassify und Core ML kommunizieren, um das Machine Learning bereitzustellen. Dieses Machine Learning ist die Kernkompenente für die Verifizierung der Autorschaften der Mails.
Eine Herausforderung bei der Implementierung was die Integration von Core ML 3, da dieses erst im Sommer 2019 veröffentlicht wurde und es daher kaum Informationen zu diesem Framework gab. Daher war die Erstellung eines on-device updateable Models mit unerwarteten Problemen behaftet, wie Build-Errors oder die Tatsache, dass nur zwei bestimmte Algorithmen unterstützt werden. Jedoch konnten diese Probleme behoben werden.

Schlussendlich konnte die App wie geplant implementiert werden. Die angestrebten Funktionalitäten sind umgesetzt und auch in den folgenden Evaluierungen funktionierte die App wie gewünscht. Der Source-Code der App ist auf GitHub öffentlich einsehbar und kann dort heruntergeladen werden.

GitHub-Link: https://github.com/cfinker/postal-demo-extended-with-authorship-verification

2.2 Meilenstein 2 – Durchführen der Evaluierungen

Status: abgeschlossen

Um die gestellten Forschungfragen zu beantworten, war es nötig anhand geeigneter Datensets zu evaluieren, welche Ergebnisse die verwendeten Machine Learning Provider uClassify und Core ML 3 lieferten. Daher wurden drei verschiedene Datensets an Mails zusammengestellt. Eines dieser Datensets sind die veröffentlichen Mails von Hillary Clinton mit über 6500 Mails von mehr als 85 Personen. Ursprünglich waren nur zwei kleinere Datensets geplant, aber um die Aussagekraft der Ergebnisse besser zu fundieren, wurde dieses dritte, größere Datenset ergänzt.
Mit diesen drei Datensets wurde die Genauigkeit bzw. Zuverlässigkeit der Ergebnisse der Autorschaft-Verifizierung evaluiert, in dem die Mails von der entwickelten App empfangen und verarbeitet wurden. Die erzielten Ergebnisse wurden in Tabellen dokumentiert und in der Masterarbeit präsentiert und analysiert.

2.3 Meilenstein 3 – Erstellung einer ersten inhaltlichen Version

Status: abgeschlossen

Im Laufe der letzten Monate wurde auch eine erste Version der Masterarbeit geschrieben. Das heißt, es wurden alle nötigen Researchetätigkeiten durchgeführt sowie die Erkenntnisse aus diesen Researchen und den eigenen Implementierungen und Evaluierungen zu Papier gebracht. Bereits mit der Fertigstellung der ersten vier (von insgesamt acht) Kapiteln wurde der damals aktuelle Stand von dem Betreuer der Arbeit gelesen und dessen Feedback ist bereits wieder in die Arbeit eingeflossen. Nun, nachdem alle Kapiteln in einer ersten Version fertiggestellt sind, wurde letzte Woche der aktuelle Stand wieder an den Betreuer übermittelt für ein neuerliches Feedback. Dieses Feedback ist noch ausständig.

2.4 Meilenstein 4 – Inhaltlicher Feinschliff

Status: offen

Sobald das Feedback des Betreuers zur ersten vollständigen Version der Masterarbeit vorliegt, wird eine entsprechende Überarbeitung der Masterarbeit erfolgen. Diese Überarbeitung wird sich primär auf inhaltliche Verbesserungen konzentrieren. Eine explizite orthographische und grammatikalische Korrektur erfolgt durch professionelle Hand sobald die inhaltlichen Arbeiten abgeschlossen sind.

2.5 Meilenstein 5 – explizite orthographische und grammatikalische Korrektur

Status: offen

Mit Abschluss der inhaltlichen Arbeiten, wird die Masterarbeit von zwei AHS-Englisch-Lehren mit Erfahrungen im wissenschaftlichen Schreiben einer orthographischen und grammatikalischen Korrektur unterzogen. Die Verbesserungsvorschläge der beiden werden abschließend in die Masterarbeit eingearbeitet. Auch bei dieser Überarbeitung, wie auch bei den vorherigen, gilt es zusätzlich auch ein Auge auf die formalen Anforderungen bzw. auf die Erfüllung dieser zu legen.

3 Zusammenfassung Planaktualisierung

Folgende Änderungen wurden vorgenommen:

- Die zeitlichen Markierungen von den erledigten Phasen wurden grün markiert sowie großteils um ein oder zwei Wochen nach vorne (früher) verschoben, da die Arbeiten schneller als geplant vorangingen.
- Die Fertigstellung der ersten Version der Masterarbeit konnte schon früher als geplant erfolgen, dass diese sogar vor Erstellung der Zwischenberichtes abgeschlossen war. Daher wurde die Reihenfolge der entsprechenden Zeilen angepasst, um weiterhin eine chronologische Reihenfolge zu bilden.
- Der angegeben GitHub-Link wurde aktualisiert, da das endgültige Repo doch eine andere URL hat, als im November noch angenommen.
- Die Liste der vorhandenen Blog-Beiträge wurde auf den neuersten Stand gebracht.