Searchitect

Zwischenbericht | Call 12 | Projekt ID 2099

Inhalt

1 Einleitung

Die Arbeiten am Projekt Searchitect wurden Mitte Jänner 2018 aufgenommen. Für die Durchführung der Hauptentwicklungsarbeit wurde wie geplant Ines Kramer angestellt.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - *Evaluierung Usecases Consumer*

Kurzbeschreibung der Haupttätigkeiten

Erstellung einer Onlineumfrage bezüglich möglicher Usecases des Searchitect Frameworks als Vorbereitung für die Integration im AP8.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

-

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

Aufgrund von zeitlicher Auslastung wurde dieser Punkt auf den Sommer verschoben

2.2 Arbeitspaket 2 - *Design Architektur*

Kurzbeschreibung der Haupttätigkeiten

Festlegung der API des Webservices und der Clientbibliothek sowie der Authentifizierungsmethode.

Erkenntnisse zur Vorgangsweise

Stärker koordinierte Vorgangsweise am Beginn wäre hilfreich gewesen.

Kurzbeschreibung der erreichten Ergebnisse

Entscheidung für Microservice Architektur mit einem RESTful Interface.
Die APIs wurden festgelegt.
Die Authentifizierung erfolgt auf Basis von JWT (JSON Web Token)

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

-

2.3 Arbeitspaket 3 - *Implementierung Webservice*

Kurzbeschreibung der Haupttätigkeiten

Der serverseitige Teil der in AP2 festgelegten Architektur wurde mit Hilfe des Spring Boot Frameworks implementiert.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

Basisversion des Frameworks implementiert.
Verwendung von Test Driven Development ermöglicht konsistente Weiterentwicklung
Frühzeitige Erstellung von Dockerfiles als Vorbereitung für Integrationstests

Besondere Erfolge/ Probleme

Integration von JWT in das Security Framework von Spring Boot war aufwändiger als erwartet. Diese werden zur Authentifizierung von RESTful Anfragen an das Searchable Encryption Webservice verwendet.

Gab es große Abweichungen zum Plan? Warum?

s.o.

2.4 Arbeitspaket 4 - *Implementierung ClientLib*

Kurzbeschreibung der Haupttätigkeiten

Der clientseitige Teil der in AP2 festgelegten Architektur wurde mit Hilfe des Spring Frameworks implementiert.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

Basisversion der Clientbibliothek implementiert.
Usermanagement implementiert.
Integration von Indexerfunktionalität (Extrahierung der Schlüsselwörter aus Dokumenten) in die ClientLib.

Besondere Erfolge/ Probleme

Erkenntnis, dass deutlich mehr Searchable Encryption Logik in die Clientbibliothek einfließen muss als ursprünglich geplant bzw. erwartet.

Gab es große Abweichungen zum Plan? Warum?

-

2.5 *Arbeitspaket 5 - Demo ClientApp*

Kurzbeschreibung der Haupttätigkeiten

Erstellung von Clients die die Anwendung des Searchitect Frameworks demonstrieren.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

-

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

Aufgrund von zeitlicher Auslaustung kann dieses AP erst im Sommer gestartet werden.

2.6 *Arbeitspaket 6 - SE Verfahren auswählen und integrieren*

Kurzbeschreibung der Haupttätigkeiten

Auswahl eines ersten konkreten SE Verfahrens welches als Plugin in Server und ClientLib integriert wird.

Erkenntnisse zur Vorgangsweise

Es konnte gut auf bestehende Arbeiten aus einem Vorprojekt am Kompetenzzentrum für IT-Security aufgebaut werden.

Kurzbeschreibung der erreichten Ergebnisse

Das Verfahren DynRH2Lev aus der Clusion Library wurde ausgewählt und integriert.
Die Speicherung der Datenbank erfolgt in einer Variante Memory basiert und einer weiteren Variante persistent über das Key-Value Store RocksDB.

Besondere Erfolge/ Probleme

Erkenntnis, dass eine starke Fokussierung auf Verfahren die „Forward Security“ bieten notwendig ist um ein wirklich sicheres System zu schaffen.
Einige Bugs der DynRH2Lev Implementierung aus der Clusion Library wurden behoben, außerdem wurde die persistente Variante optimiert hinsichtlich der Reduktion der Update- und Suchlaufzeit und des Speicherbedarf des verschlüsselten Index.
Die Parametrisierung des DynRH2Lev Verfahren war für diesen Anwendungszweck nicht ausreichend dokumentiert, diese musste daher erste ermittelt werden.

Gab es große Abweichungen zum Plan? Warum?

-

2.7 *Arbeitspaket 7 - Auswahl weiterer SE Verfahren*

Kurzbeschreibung der Haupttätigkeiten

Auswahl eines zweiten konkreten SE Verfahrens welches als Plugin in Server und ClientLib integriert wurde.

Erkenntnisse zur Vorgangsweise

Die von Anfang an geplante Modularität des System hat sich hier sehr bewährt.

Kurzbeschreibung der erreichten Ergebnisse

Das Forward Secure Verfahren Sophos wurde nach Java portiert und in das System integriert.
Die Persistierung der Datenbank erfolgt nicht Memory basiert sondern über den Key-Value Store RocksDB.

Besondere Erfolge/ Probleme

Von Sophos lag bis dato nur eine C++ Implementierung vor, die portiert werden musste.

Gab es große Abweichungen zum Plan? Warum?

-

2.8 *Arbeitspaket 8 - Integration in Drittsoftware*

Kurzbeschreibung der Haupttätigkeiten

Auf Basis der Ergebnisse von AP1 soll Searchitect in eine bestehende Software integriert werden

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

-

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

Aufgrund der Verzögerung von AP1 kann dieses AP erst im Sommer gestartet werden.

2.9 *Arbeitspaket 9 – Hosting*

Kurzbeschreibung der Haupttätigkeiten

Anschaffung und Installation eines Servers für das Hosting einer Demoinstanz von Searchitect.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

Server bestellt

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

Aufgrund von zeitlicher Auslastung konnte die für die weitere Vorgangsweise notwendige Hardware erst im Juni 2018 durchgeführt werden.

2.10 *Arbeitspaket 10 – Wartung*

Kurzbeschreibung der Haupttätigkeiten

Kontinuierliche Bereitstellung einer Demoversion des Frameworks

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

-

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

Aufgrund der zeitlichen Verzögerung von AP9 konnte dieser Punkt noch nicht gestartet werden.

2.11 *Arbeitspaket 11 - Integrationstests & Quantitative Analyse*

Kurzbeschreibung der Haupttätigkeiten

Das System und die implementierten Verfahren werden getestet um sinnvolle Vergleiche anstellen zu können und die Grenzen des Systems auszuloten.

Erkenntnisse zur Vorgangsweise

Beschränkung auf künstlich erstellte Testdaten ist nicht ausreichend.

Kurzbeschreibung der erreichten Ergebnisse

Erstellung von synthetischen und Real-World Testdaten
Visualisierung der Messwerte.

Besondere Erfolge/ Probleme

Verwendeter Indexer musste an die Struktur der verwendeten Daten angepasst werden (z.B. Datumserkennung, Filterung von Headern).

Gab es große Abweichungen zum Plan? Warum?

-

2.12 *Arbeitspaket 12 - Dokumentation erstellen*

Kurzbeschreibung der Haupttätigkeiten

Erstellung von Dokumentationen für die Verwendung von Searchitect für alle möglichen Benutzergruppen.

Erkenntnisse zur Vorgangsweise

Regelmäßige Dokumentation während des Entwicklungsprozesses ist sehr sinnvoll.

Kurzbeschreibung der erreichten Ergebnisse

Codedokumentation
Ausführliche README Dateien in allen Projekten
Dynamische API Dokumentation mittels Swagger

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

-

2.13 *Arbeitspaket 13 – Paper*

Kurzbeschreibung der Haupttätigkeiten

Die Ergebnisse des Projektes sollen wissenschaftlich verwertet und publiziert werden.

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

Veröffentlichung des Position Papers „Searchitect – A Developer Framework for Hybrid Searchable Encryption“, welches die Architektur von Searchitect beschreibt, auf der „3rd International Conference on Internet of Things, Big Data and Security (IoTBDS)“.
Fertigstellung der Masterarbeit „A Practical View on Dynamic Symmetric Searchable Encryption“ durch Ines Kramer in welcher das Framework und Messergebnisse beschrieben werden.

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

-

2.14 *Arbeitspaket 14 – Öffentlichkeitsarbeit*

Kurzbeschreibung der Haupttätigkeiten

Bekanntmachung von Searchitect, Erstellen von Blogposts

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

- *Für einen Artikel zum Thema „Speichersysteme der Zukunft“ der Zeitschrift Heureka 7/2017 (Wissenschaftsbeilage des Falter) wurde Mathias Tausig interviewt.*
- *6 netidee Blogposts die über den laufenden Stand des Projekts berichten*
- *Präsentation von Searchitect am Open-House Tag der FH- Campus Wien*
- *Domain Searchitect.eu wurde angeschafft*

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

2.15 *Arbeitspaket 15 – Projektmanagement*

Kurzbeschreibung der Haupttätigkeiten

Verwaltung des Projektes

Erkenntnisse zur Vorgangsweise

-

Kurzbeschreibung der erreichten Ergebnisse

Anstellung von Ines Kramer
Erste Förderrate abgerufen.
Zwischenbericht abgegeben.
Alle bis dato notwendigen FH internen Verwaltungsschritte durchgeführt.

Besondere Erfolge/ Probleme

-

Gab es große Abweichungen zum Plan? Warum?

-

3 Zusammenfassung Planaktualisierung

Alle Anpassungen des Plan-Excels kurz zusammengefasst

- AP1 wird erst 07/18 (statt 01/18) gestartet und entsprechend später fertiggestellt
- AP2 hat aufgrund von Adaptierungen länger als geplant gedauert (bis 04/18 statt 01/18)
- AP3 wurde erst 05/18 fertiggestellt (statt 03/18)

- AP4 wurde erst ein Monat später gestartet und dauerte etwas länger (02-05/18 statt 01-03/18)
- AP5 wird erst 08/18 gestartet
- AP6 hat sich um ein Monat verzögert (04-05/18 statt 03/18)
- AP7 hat sich um ein Monat verzögert (05-06/18 statt 04-05/18)
- AP8 wird erst 08/18 gestartet
- AP9 konnte erst mit Verspätung gestartet werden (06/18 statt 01/18), die geplante Fertigstellung wurde nur auf 08/18 verschoben
- AP10 wird erst 08/18 gestartet
- AP11 wurde mit einem Monat Verspätung (07/18 statt 06/18) gestartet
- AP12 wurde mit einem Monat Verspätung (02/18 statt 01/18) gestartet
- AP13 wurde 6 Monate früher als geplant begonnen (12/17 statt 06/18)

4 Öffentlichkeitsarbeit/ Vernetzung

Beschreibung der bereits erfolgten Öffentlichkeitsarbeit oder Vernetzung, bzw. Beschreibung des Plans künftiger Aktivitäten

Ende 2017 ist ein Artikel in der Wissenschaftsbeilage des Falter („Heureka“) erschienen zum Thema „Speichermedien der Zukunft“, für welchen unter anderem Mathias Tausig interviewt wurde. Die Ziele des Projektes sind in den Artikel eingeflossen.
Ein Position Paper zur Architektur von Searchitect wurde auf der „3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)“ präsentiert, es ergaben sich anrgende Diskussionen mit den anwesenden Wissenschaftlern

Bereits fix geplant ist eine Vorstellung des Projektes auf der Privacy Week im Oktober 2018 in Wien.
Darüber hinaus ist eine weitere wissenschaftliche Publikation mit den Endergebnissen für Ende 2018/Anfang 2019 geplant.

Die Webseite zum Projekt wird ab dem Herbst unter der Domain „searchitect.eu“ erreichbar sein.