Data Sharing in the Internet of Things with Proxy Re-Encryption

Advisor(s): Felix Hörandner

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

IoT devices collect a variety of different – sometimes sensitive – data. To benefit from these data, they have to be sent to a processing application in real time. Also, some data should be stored for further use. These scenarios, require to ensure the data's confidentiality and integrity.

Proxy Re-Encryption (PRE) is an advanced cryptographic primitive, that can be employed to fulfill these requirements. PRE extends asymmetric encryption, by enabling a semi-trusted proxy to transform ciphertext encrypted for one user into ciphertext encrypted for another user, without learning the underlying plaintext in an intermediate step. This cryptographic concept enables secure end-to-end data sharing.

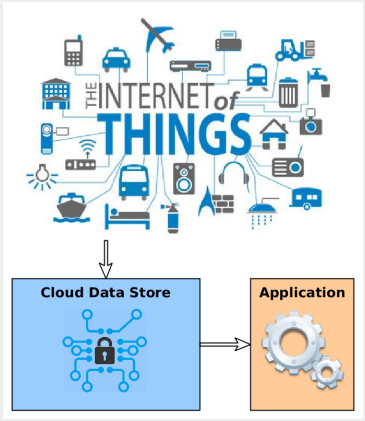
With PRE we can build a publish-subscribe platform, which gives the user full control over the shared data. IoT sensors capture data and encrypt it themselves or with the help of a gateway. This encrypted data is then uploaded to our cloud platform. This process can be seen publishing to user-controlled topics, to which processing application can subscribe. Once the user has given authorization and generated a re-encryption key, the cloud platform can re-encrypt the events for the processing application. In the end, these applications obtain and decrypt the events. During this whole process, the cloud platform does not learn anything about the plaintext of the shared events, which solves a big challenge of modern IoT solutions.

This topic is scalable from bachelor's to master's thesis. We can arrange and adjust the scope according to your scheduled effort, interests, and ideas.

Goals and Tasks

- Create and analyze a concept employing PRE
- Implement an IoT prototype including: sensors, a sharing service, and an application

Figure



Literature

- M Blaze, G Bleuner, and M Strauss
  Divertible protocols and atomic proxy cryptography
  EUROCRYPT 1998

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in modern IT security
- Programming skills

Advisor / Contact

felix.hoerandner@iaik.tugraz.at