4. Oktober 2021 Studie · Privatsphäre & Krypto · Web & Cloud

Herausforderungen durch Verschlüsselung: Wiederherstellung und Verarbeitung

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Stand 2021-09-30
Quelle https://technology2.a-sit.at/veroeffentlichungen/herausforderungen-durch-verschluesselung-wiederherstellung-und-verarbeitung/

Verschlüsselung stellt ein fundamentales Werkzeug dar um die Vertraulichkeit von Daten zu gewährleisten und findet somit Anwendung in Bereichen, die mit sensitiven Daten umgehen. Beispiele hierfür sind digitale Repräsentationen in IoT Systemen (so genannte Digital Twins), medizinische Daten oder Identitätsdaten. Verschlüsselung erlaubt es nun (1) solch sensitive Daten sicher an Systeme auszulagern, auch wenn diesen Systemen nicht vollständig vertraut wird (beispielsweise in der Cloud), sowie (2) die Daten mit ausgewählten Dritten zu teilen.

Verschlüsselung brigt jedoch auch Herausforderungen. Datenverlust droht falls das Schlüsselmaterial verloren geht (beispielsweise weil das Gerät defekt wird). In diesem Fall können die verschlüsselten Daten nicht mehr entschlüsselt werden. Für Schlüsselmaterial als auch verschlüsselte Daten wird eine Wiederstellungsstrategie benötigt. Weiters ist es nicht mehr möglich die Inhalte der verschlüsselten Daten direkt zu verarbeiten.

Dieses Projekt widmet sich den Herausforderungen der Verschlüsselung und präsentiert Lösungsansätze im Kontext eines Digital Twin Systems. Ein Digital Twin ist die stets aktualisierte digitale Repräsentation eines physischen Objektes. Diese Digital Twins werden in der Cloud erstellt. Da Digital Twin Daten von sensitiver Natur sein können wurde in einem vorangegangenen Projekt eine Sicherheitsarchitektur vorgeschlagen in der die Daten verschlüsselt und somit geschützt werden. Solch ein geschütztes Digital Twin System benötigt ebenso Lösungen für die Herausforderungen der Verschlüsselung. Unser Konzept nützen die Flexibilität von Proxy Re-Encryption um Zugriffsberechtigungen dynamisch zu verändern (zB um auf geänderte Vertrauensbeziehungen zu reagieren) sowie um die Daten eines Digital Twin auf einem Ersatzgerät wiederherzustellen, sollte das initiale Gerät defekt werden. Weiters integriert unser Konzept Multi-Party Computation, um auch die Verarbeitung von geschützten Digital Twin Daten zu ermöglichen,

wobei diese Daten aber nicht an die Cloud oder andere Beteiligte offengelegt werden. Die Machbarkeit und Performanz dieses Konzeptes wird abschließen anhand eines Beispiels zur Kontaktrückverfolgung von infizierten Personen evaluiert.