LISA

Entwicklung einer Lösung zur sicheren dezentralen Verarbeitung von IT-Anwendungen mit einer Berechtigungsverwaltung

Programm / Ausschreibung	IWI 24/26, IWI 24/26, Basisprogramm Ausschreibung 2025	**Status**	laufend
Projektstart	01.01.2025	**Projektende**	31.12.2025
Zeitraum	2025 - 2025	**Projektlaufzeit**	12 Monate
Keywords			

Projektbeschreibung

In offenen IT-Arbeitsplätzen (PCs, Laptops etc.), IoT-Geräten, Maschinen etc., wo Anwendungen inklusive einer gemeinsamen Datenbasis über mehrere Arbeitsplätze bzw. einer Zentrale verarbeitet werden, können ein logisches Zugriffsberechtigungssystem und eine Berechtigungsverwaltung, wie in einem Hostumfeld üblich, aus Sicherheitsgründen nicht eingesetzt werden. Ausreichend sichere Lösungen basieren in der Regel auf dem Einsatz von geeigneter Kryptografie bzw. Spezialverfahren wie z.B. Fragmentierung. Doch der Stand der Technik, insbesondere das heutige Lösungsangebot am Markt, liefert dazu keine ausreichend geeignete Lösungen für eine komplexere Berechtigungsverwaltung und feingliedrigen Zugriffskontrolle, wie im Hostumfeld üblich und die z.B. bei Datenbanken bzw. Dateien bzw. Ausgabefelder am Bildschirm (Bildschirmmasken) bis auf einzelne Elemente operieren.
Bei IT-Anwendungen in Zentralen / externen Clouds können die Benutzer nicht überprüfen, ob die Daten auch von Unberechtigten, wie z.B. Systemadministratoren, Geheimdiensten oder Hacken, gelesen oder analysiert bzw. mit anderen Daten verknüpft werden. Nur bei der dezentralen Verarbeitung am IT-Arbeitsplatz des Benutzers kann garantiert werden, dass nur Berechtigte die Daten lesen und verarbeiten können. Der Bedarf nach Dezentralisierung umfasst neben der Datensicherheit auch die Verarbeitungstransparenz, die Verfügbarkeit und Verarbeitung vor Ort.
Die Ergebnisse des vorliegenden Projekts (Vorhabens), nachfolgend LISA genannt, liefern erstmalig eine komplette Lösung für eine ausreichend sichere Dezentralisierung. Dabei werden die Anwendungen direkt am IT-Arbeitsplatz des Benutzers (Berechtigten) verarbeitet und die Daten sofort nach der Verarbeitung noch am IT-Arbeitsplatz quantencomputersicher und feingliedrig (bis auf einzelne Datenelemente in Datenbanken bzw. Bytes in Dateien) rollenbasierend verschlüsselt. Die Daten befinden sich unverschlüsselt nur mehr beim Berechtigten vor Ort.
LISA enthält dazu ein neuartiges quantencomputersicheres kryptografisches Zugriffskontrollsystem und Schlüsselmanagement sowie eine sichere, kryptografische Berechtigungsverwaltung. Es enthält eine Vielzahl an Alleinstellungsmerkmalen (USPs), die auch patentrechtlich geschützt wurden, und kann aus einzelnen existierenden Lösungen des Marktes nicht gebildet werden.
Für die Entwicklung dieser "Deep Tech" Lösung waren im Vorfeld schon umfangreiche Forschungstätigkeiten erforderlich, die im Rahmen eines Josef-Ressel-Zentrums (Dotierung ca. € 1,2 Millionen) am Institut für IT-Sicherheitsforschung der FH St. Pölten in den vergangenen fünf Jahren durchgeführt wurden. Die daraus entstandenen Proof-of-concept Implementierungen

zeigten, dass die schon vorliegenden Forschungsergebnisse in einer Laborumgebung funktionieren und daher eine funktionierende Lösung mit einigem Restrisiko und noch etwas Forschungsbedarf entwickelt werden kann. Die Forschungstätigkeiten sind erforderlich, um einen ausreichend zeiteffizienten und vollumfänglichen Einsatz gewährleisten zu können, und die Entwicklungstätigkeiten der Middleware werden zum Teil komplex sein und eine Menge an Entwicklungsrisiken enthalten (siehe 1.6).
LISA enthält als Option mit ihrer speichereffizienten Verkettungsfunktion, sowohl für alle Transaktionen als auch - als USP - für die Berechtigungsverwaltung, eine Erweiterung auf eine Blockchain/DLT und wird dann DLT4IT genannt. DLT4IT eliminiert zwei große Nachteile von heutigen Blockchain-/DLT-Technologien, die fehlende rollenbasierte Berechtigungsverwaltung, was eine wichtige Basis fast aller Enterprise-Lösungen darstellt, und die Notwendigkeit der Neuentwicklung der IT-Anwendungen, was hohe Kosten und Zeit spart. Diese beiden Nachteile bremsen heute die Verbreitung und schränken die Anwendungsmöglichkeiten ein, was mit DLT4IT nicht der Fall wäre. Des Weiteren enthält DLT4IT eine auf Kryptografie basierende Löschfunktion ohne Veränderung der Blockchain, was oftmals sehr wichtig ist (z.B. Datenschutzgrundverordnung). DLT4IT beschleunigt und öffnet damit den Blockchainmarkt und macht aus einer disruptiven Technologie eine nachhaltige, was sicher viele Softwarehäuser motivieren würde mit ihren Anwendungen in den Blockchainmarkt zu gehen.

Endberichtkurzfassung

Seit mehreren Jahrzehnten gibt es in der IT den Trend zur Zentralisierung, zu einer IT-Verarbeitung in der sogenannten Cloud. Cloud-Computing ist in aller Munde und beherrscht weltweit die IT-Strategie der Unternehmen.

Seit einigen Jahren existieren aber auch die Trends: Blockchain, Data Mesh, Edge-Computing, Web 3.0 und Metaverse, die alle die dezentrale IT-Verarbeitung als Ziel haben. Diese Trends kommen erst schön langsam in Fahrt und damit auch ein neuer Bedarf nach Dezentralisierung der IT-Verarbeitung. Die Ergebnisse des vorliegenden Projektes, zusammengefasst LISA genannt, ermöglichen mit ihrem kryptografischen Zugriffskontrollsystem und Berechtigungsverwaltung eine sichere Rollen-basierte Zugriffskontrolle und Berechtigungsverwaltung mit einer dezentralen IT-Verarbeitung auf PCs (Desktop, Laptop etc.), IoT-Geräten, Maschinen etc. Dadurch ist es auch möglich, aktuell auf Servern und Hostcomputern laufende Anwendungen dezentral zu verarbeiten und damit die Datensicherheit (Unabhängigkeit von unbekannten Vorgängen in der Cloud) zu erhöhen und die Verfügbarkeit zu verbessern.

Projektpartner

- insitu software gmbh