LISA

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

Programm / Ausschreibung	IWI, IWI, Basisprogramm Ausschreibung 2023	**Status**	abgeschlossen
Projektstart	01.01.2024	**Projektende**	31.12.2024
Zeitraum	2024 - 2024	**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 bzw. für Blockchains DLT4IT 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 € 1,2 Millionen, davon schon rund € 1 Million verbraucht) am Institut für IT-Sicherheitsforschung der FH St. Pölten in den vergangenen vier Jahren durchgeführt wurden. Die daraus entstandenen Proof-of-concept Implementierungen zeigen, 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

Die Ergebnisse des vorliegenden Projekts LISA liefern erstmalig eine komplette Lösung für eine ausreichend sichere Dezentralisierung von IT-Anwendungen mit einer feingliedrigen Zugriffskontrolle auf Datenbanken und Dateien und Berechtigungsverwaltung. Dabei werden die IT-Anwendungen direkt am IT-Arbeitsplatz des Benutzers verarbeitet und die Daten sofort nach der Verarbeitung noch am IT-Arbeitsplatz quantencomputersicher und entsprechend der rollenbasierenden Berechtigungsverwaltung feingliedrig (bei Bedarf bis auf einzelne Datenelemente in Datenbanken bzw. Bytes in Dateien) verschlüsselt. Die Daten befinden sich unverschlüsselt nur mehr bei den Berechtigten vor Ort an ihren Arbeitsplätzen. LISA enthält dazu ein neuartiges quantencomputersicheres kryptografisches Zugriffskontrollsystem und Schlüsselmanagement sowie eine sichere, kryptografische Berechtigungsverwaltung. LISA enthält eine Vielzahl an Alleinstellungsmerkmalen (USPs), die auch patentrechtlich geschützt wurden, und kann aus einzelnen existierenden Lösungen des Marktes nicht gebildet werden.

Durch die umfangreichen Forschungsergebnisse aus einem Josef Ressel Zentrum, das mit rund 1,2 Millionen Euro dotiert war, waren zum Projektstart der Großteil der erforderlichen Forschungstätigkeiten abgeschlossen. Bei den noch offenen Forschungstätigkeiten im ersten Projektjahr ging es vor allem um die Quantencomputer-sichere Kryptografie.

Von den zu entwickelnden Komponenten erfolgten im ersten Projektjahr vier Komponenten: a.) die Entwicklung der Software zur Erzeugung der mehrfach durch Hardware-Token signierten rollenbasierenden Berechtigungsliste (Berechtigungsverwaltung); b.) die Entwicklung der Middleware, die sich „zwischen“ der IT-Anwendung und dem DBMS (Datenbankmanagementsystem) und Dateisystem im Arbeitsplatz befindet, bestehend aus einem Proxy und der quantencomputersicheren und formaterhaltenden Ver-/Entschlüsselungsfunktion, basierend auf der Berechtigungsdatenbank; c.) die Entwicklung der Steuerungssoftware im Arbeitsplatz, die vor allem alle LISA-Komponenten vor Ort steuert, die aus der Berechtigungsliste die Berechtigungsdatenbank erzeugt, die in Verbindung mit dem TPM-Chip am Arbeitsplatz die Entschlüsselung und Verwaltung der Schlüsselliste durchführt und die die Serverkommunikation steuert; d.) die Entwicklung der Serversoftware, die für die gesamte Transaktions-Replikation und -Synchronisation zuständig ist, sodass die Datenbanken, Dateisysteme und Systemparameter in allen Arbeitsplätzen stets die gleiche Datenbasis enthalten.

Die Serversoftware ist auch dafür zuständig, dass nach der Inbetriebnahme eines Arbeitsplatzes nach einer Betriebspause dieser entsprechend aktualisiert wird.

Projektpartner

- insitu software gmbh