CISSAN

Collective Intelligence Supported by Security Aware Nodes

Programm / Ausschreibung	IWI 24/26, IWI 24/26, Basisprogramm Ausschreibung 2024	**Status**	abgeschlossen
Projektstart	01.07.2024	**Projektende**	30.06.2025
Zeitraum	2024 - 2025	**Projektlaufzeit**	12 Monate
Keywords			

Projektbeschreibung

Im EUREKA-Celtic Next Projekt CISSAN hat Geodata die Entwicklung von drei verschiedenen IoT-Sicherheitssystemen für die Anwendung in den Fachgebieten Tunnelbau und Geo-Monitoring zum Ziel.
Diese Systeme bilden im Einzelnen:
* ein KI/ML basiertes SW-System zur automatischen Datenqualitätsprüfung von Monitoringdaten,
* ein System zur elektronischen Signierung von Messdaten und Sensoren mittels Security-Chips und
* ein Blockchain-basiertes System zur sicheren Messdatenübertragung.
Im Projekt wird Geodata bestehende IoT-Sicherheitstechnologien zur Verwendung für die geplanten Systeme evaluieren, geeignete Technologien auswählen, die geplanten Systeme spezifizieren, entwickeln und operationelle Prototypen für jedes System implementieren, testen und im Rahmen von Use Cases demonstrieren. In weiterer Folge wird Geodata seine drei Systeme in die gemeinsame IoT-Plattform des internationalen Projekts integrieren.
Die Forschungsleistungen werden gemeinsam mit dem Partner SCCH (Software Competence Center Hagenberg) und den internationalen EUREKA-Partnern erbracht.

Endberichtkurzfassung

Am Ende des 2.Forschungsjahrs des insg. 3-jährigen Projekts liegen bereits folgende Projektergebnisse vor:

ein erster Prototyp des geplanten (Cyber)sicherheitssstems zur Datenqualitätsprüfung.
Der Prototyp besteht aus einer Software, welche Mess- und Monitoringdaten (Sensorzeitreihen) anhand von empirischen Datenqalitätsregeln und KI-basierten Methoden (sogenannten DQ-Metriken) untersuchen kann. Als Output liefert der Prototyp sogenannte "Believability Scores", die ein Maß für die Glaubwürdigkeit der Sensordaten darstellen. Für die Anwendung von KI wurde ein Large Language Model zur Erkennung von Anomalien in Zeitserien verwendet.
Für das System wurden exemplarisch bereits 7 DQ-Metriken entwickelt und implementiert. Zum Testen des Systems wurden umfangreiche Messdaten aus Monitoringprojekten akquiriert und gezielt manipuliert bzw. simulierte Sequenzen eines Cyberangriffs eingebaut.

ein erster Prototyp des geplanten (Cyber)sicherheitssstems zur elektonischen Datensignierung .
Das System besteht aus speziellen Security Chips, welche an Messsensoren (oder in Datenloggern, Gateways) angebracht werden und deren Messdaten signieren können. Die Signaturen werden gemeinsam mit den Messdaten übertragen und am Endpunkt (am Server) verifiziert. Misslingt die Verifizierung (Public-Private-Key - System), wird ein (Cyber)angriff vermutet und die Messaten werden abgelehnt, nicht in die Datenplattform übernommen und ein Alarm wird generiert.

ein erster Prototyp des geplanten (Cyber)sicherheitssstems zur Blockchain-basierten Datenübertragung.
Der Prototyp nutzt die Technologie des Lightning Networks (=ein 2nd Layer Blockchain System) für die Übertragung von Mess- und Monitoringdaten über mehrere parallele Kanäle (sogenannte Lightning Channels) vom Sensor bis zum Endpunkt (Server). Dort wird überprüft, ob die übertragenen Daten ident sind, somit am Übertragungsweg keine Änderungen (z.B. unerlaubte Löschungen) vorgenommen wurden. Stimmen die Daten nicht überein,so werden sie abgelehnt und eine Alarmmeldung wird generiert. In weiterer Folge werden die Transaktionen periodisch in die Mainchain der Bitcoin Blockchain endgültig gespeichert/gesichert.

Projektpartner

- GEODATA ZT GmbH