CELTIC-NEXT
Eureka Cluster

Project Report

CISSAN

Collective intelligence supported by security aware nodes

D5.3 Blockchain-based security solutions for IoT networks

Editor: Ilgin Safak, University of Jyväskylä and Jari Partanen, Bittium

Abstract

The fast growth of IoT networks creates new security concerns related to their distributed nature, heterogeneity, and resource limitations. This report presents a blockchain-based IoT network security system for establishing trust, transparency, and collaboration in a zero-trust environment. Blockchain technology enables decentralized trust management, data sharing, and tamper-proof logging of cybersecurity incidents. In addition, blockchain is used for implementing distributed access controls and blacklisting compromised devices, which allows making informed security decisions without centralization. With the use of artificial intelligence-based anomaly detection methods, risk assessment and collective intelligence, the efficiency of cybersecurity is improved significantly. The report also outlines the collective intelligence mechanisms used, including how they are applied and validated in the use cases on the CISSAN platform, as well as the validation results of the blockchain-based network security system. Furthermore, the report discussed integration and implementation challenges, including related to scalability and performance, as well as the impact and business value of the system. Overall, this report shows that blockchain can be useful for creating secure, scalable, and distributed IoT environments, especially for critical infrastructures.

Project CISSAN
Public Report
April 2026

Participants in project CISSAN are (in alphabetic order with the project coordinator first):

- University of Jyväskylä (coordinator)
- Affärsverken Karlskrona AB
- Arctos Labs Scandinavia AB
- Blekinge Tekniska Högskolan
- Blue Science Park
- Bittium Wireless Ltd
- Bittium Biosignals Ltd
- Clavister AB
- Councilbox Ltd
- Geodata ZT GmbH
- Mattersoft
- Mint Security Ltd
- Netox Ltd
- Nodeon Ltd
- Savantic AB
- Scopesensor Ltd
- Techinova AB
- Wirepas Ltd

CISSAN-Collective intelligence supported by security aware nodes

D5.3 Blockchain-based security solutions for IoT networks

Editor: Ilgin Safak, University of Jyväskylä and Jari Partanen, Bittium

Project coordinator: Ilgin Safak, University of Jyväskylä.

CELTIC published project result

Preface

The accelerated digitalization of critical infrastructure, industries, and public services in Europe has elevated the role of Internet of Things (IoT) and operational technology (OT) networks as key enablers of economic activity, sustainability, and strategic autonomy. However, these networked cyber-physical entities also pose unparalleled cybersecurity risks, given the heightened sophistication of cyber-threats targeting these networks. This situation has rendered the enhancement of the cybersecurity and resilience of these networks not only a technological challenge but also a strategic imperative consistent with the European Union's Cybersecurity Strategy, NIS2 Directive, Cyber Resilience Act, and Horizon Europe. This specific challenge will be dealt with in this report, which proposes a blockchain-based IoT security system. This system will be based on the principles of leveraging the power of collective intelligence in a zero-trust environment using trust, anomaly scoring, and risk scoring while also having device-level robustness and secure access at its core. This research activity aims to play a role in Europe's strategic goal of developing sovereign, interoperable, and resilient digital capabilities with a competitive edge and to highlight Europe's leading role in the development of new-generation strategic cybersecurity solutions.

Executive Summary

The rapid development of IoT and OT systems' connectivity in critical infrastructures such as transportation, smart grids and tunnel construction, leads to increasing cybersecurity threats. As more of these critical infrastructures undergo digital transformation, the classical hierarchical approach to security is no longer effective or capable of meeting the scalability, transparency, and trustworthiness needed for such complex environments. Centralized solutions for solving these problems often fail because of their inability to handle heterogeneity, scalability, and dynamics typical of modern critical infrastructures.

This report describes the blockchain-based IoT network security system designed within the CISSAN project that uses collective intelligence methods and artificial intelligence (AI) in a zero-trust environment to increase resilience, interoperability, and situational awareness. This project report is a ‘must read’ for those organizations that aim to enhance the security, resilience, and governance of their IoT and operation technology domains, which are increasingly challenged by the dynamic nature of cyber threats.

The CISSAN blockchain-based IoT network security system uses blockchain technology to facilitate decentralized trust and device management, secure device onboarding, distributed access control, and tampering resistant logging. The ability of a blockchain to provide a shared and verified view of the status of connected devices ensures coordinated actions when it comes to decisions about blacklisting malicious devices, for example. Additionally, it also enhances device lifecycle management in a transparent and auditable manner to minimize risks and response times to incidents. The use of collective intelligence and AI based anomaly detection methods allows performing distributed detection of anomalies, assessing trust and risk scores, verifying data quality, and sharing threat intelligence information between different systems.

Moreover, this report covers the implementation of the proposed system architecture in the CISSAN environment and its interaction with other systems. In particular, the use cases cover both internal implementations of the system, such as connecting the Councilbox Eventchain System to the CISSAN servers, including the CISSAN Management Server, CISSAN Orchestrator, and Security Information and Event Management (SIEM) server, and its interaction with external heterogeneous systems. The scalability and performance analysis of the system is discussed to ensure its usability in practice.

This research was verified using several use cases: transportation, smart grids, tunnel construction, manufacturing execution systems, and the joint use case, which is related to the mitigation of cross-domain critical infrastructure attacks using automated disaster recovery. These use cases showcase the efficiency of the blockchain-based IoT network security system by leveraging collective intelligence mechanisms in terms of improving detection accuracy, coordinating threat responses, and increasing system resiliency.

The results obtained are invaluable to organizations since they allow implementing blockchain technologies and the zero-trust paradigm in the context of security and risk management in critical infrastructure systems, thus making it possible to ensure the necessary level of cybersecurity, mitigate operational risks, and comply with the emerging regulatory requirements. Besides, this approach can become the basis for creating scalable cybersecurity services in the European ICT environment.

In conclusion, this report proves that the fusion of blockchain technology with collective intelligence and AI is a paradigm shift in securing IoT/OT infrastructures. With this approach, organizations will be able to improve business continuity and establish trust in the digital world with customers, partners, and regulatory bodies. While perimeter defence or even control was the norm in securing these systems in the past, the methodological design of this strategy will enable organizations not only to counter the dangers of the future but also future-proof their architecture in the face of the ever-autonomous digital world, contributing to increased system resiliency, digital sovereignty, and sustainability of critical infrastructures in Europe.

List of Authors (alphabetically by partner name)

- Lars-Göran Magnusson, Arctos Labs
- Anders Liden, Clavister
- Rodrigo Martinez, Councilbox
- Klaus Chmelina, Geodata
- Ilgin Safak, University of Jyväskylä
- Veikko Markkanen, University of Jyväskylä
- Mikko Lehkonen, University of Jyväskylä
- Pasi Tapanainen, University of Jyväskylä
- Stella Palenius, University of Jyväskylä
- Xiaobang Sun, University of Jyväskylä
- Teemu Kemppainen, Mattersoft
- Oliver Bölin, Techinova

Table of Contents

List of Figures

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
BFT	Byzantine Fault Tolerant
BKVS	Blockchain Key Value Store
BMES	Bittium Manufacturing Execution System
CTI	Cyber Threat Information
DMZ	Demilitarized Zone
DQ	Data Quality
ECDSA	Elliptic Curve Digital Signature Algorithm
GNSS	Global Navigation Satellite System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
IoT	Internet of Things
ITxPT	Information Technology for Public Transport
ML	Machine learning
MQTT	Message Queuing Transport Telemetry
OT	Operational Technology
PASAD	Process Aware Stealthy Attack Detection
PQC	Post-Quantum Cryptography
REST	Representational State Transfer
RTU	Remote Terminal Unit
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
STIX	Structured Threat Information eXchange
VPN	Virtual Private Network
WASM	WebAssembly Module
ZTA	Zero Trust Architecture

1 Introduction

1.1 Introduction

The growth in the size of the Internet of Things (IoT) and operational technology (OT) networks is causing a paradigm shift in industries, public sectors, and critical infrastructures by allowing unprecedented levels of automation, optimization, and data-driven intelligence. This growth in interconnections, however, brings forth unprecedented cybersecurity threats due to the inability of centralized security models to deal with the volume, diversity, and real-time needs of today's cyber-physical systems. Resource-constrained, long-lived, and varied ownership scenarios in device-centric systems are commonly beyond the purview of mainstream security controls, thereby presenting attack surfaces for malicious actors. With evolving levels of sophistication and attack coordination, the requirement for adaptive and cross-boundary security models has become an important concern for network security and safety.

In response to the rising complexity and risk exposure of large-scale IoT and OT systems, the project adopts a zero-trust security paradigm and implements the same through a blockchain-based IoT network security system to ensure safe communication of devices as well as collective intelligence during runtime. This is justified due to the need to address the risks of both external as well as internal threats within distributed and heterogeneous architectures, where devices or network segments cannot be trusted.

Blockchain technology has the benefit of serving as a promising solution in addressing the above challenges in creating a trust environment and following a governing policy in spaces where there would be no controlling or monitoring authority for all the assets. With the use of blockchain technology in the IoT and OT environment, identity security, the process of connecting devices, and governing policies for accessing those devices without the need for any centralized parties become immutable and tamper-proof in nature.

Working in concert with blockchain, collective intelligence presents a potent paradigm for threat detection and risk management in scaled-out networks. Rather than being guided by standalone security measures, collective intelligence combines disparate signals from various devices, network areas, and security components to establish a common, dynamically changing view of ecosystem behaviour. As enabled by advanced analytics and machine learning, collective intelligence delivers real-time, adaptive, and context-driven threat identification and risk analysis that correctly identifies the real-world security situation faced by the ecosystem. Working together with blockchain, these intelligence assessments can be securely validated and responded to on a scaled-out basis. Coupled with blockchain, collective intelligence presents a novel system for securing IoT/OT networks. This new system moves away from traditional, infrastructure-dependent methods for network security. Instead, its emphasis is on intelligence-led processes that rely on building on trust.

The design of the proposed system is compliant with the security requirements defined within CISSAN deliverable D2.3 report, while at the same time ensuring the compliance of the proposed solution to the standardization action plan of CISSAN deliverable D7.1 report. Using blockchain technology, which makes processes open, auditable, and secure, it is possible for organizations to realize better levels of resilience, responsibility, and situational awareness. This is especially true because blockchain, together with collective intelligence and artificial intelligence (AI), presents a novel framework that combines all aspects of secure digital transformation. Through the adoption of the zero-trust model while incorporating the benefits of the blockchain-based device management, trust scoring, and collective intelligence, CISSAN is creating a foundation for a resilient cybersecurity posture while at the same time acknowledging the inherent complexity of such a solution.

1.2 Objective of this report

The objective of this report is to provide an overview of the blockchain-based network security solution designed for IoT and OT networks using the power of collective intelligence to improve trust, resiliency, and management of cyber risks. Additionally, this report endeavours to serve as strategic reference material designed to aid decision-makers, leaders in technology, as well as cybersecurity experts in implementing next-generation approaches in security infrastructure architecture in line with European strategic imperatives on cybersecurity and the goals of Horizon Europe in developing secure and resilient digital infrastructure. Moreover, this research also provides an analysis of the

industry's need for blockchain to improve security infrastructure or security architecture in IoT and operational technology environments.

1.3 Collective intelligence mechanisms for IoT network security

In ever expanding heterogeneous IoT environments, traditional centralized security mechanisms are inadequate for managing and mitigating cyber security risks and threats, and thus, it becomes essential to employ various collective intelligence mechanisms that allow distributed components within IoT networks to collaborate and work together for providing a collaborative and coordinated response against cyber security risks and threats. Collective intelligence mechanisms that have been implemented within the blockchain-based IoT network security system are described in detail in the CISSAN D5.4 report, which includes data quality verification, anomaly detection, trust scoring, and security sub-function distribution. The Councilbox blockchain system, namely the Councilbox Eventchain System, is used for securely logging device events and ensuring a consensus of the security decisions related to the devices in the network.

Collective intelligence in Eventchain operates through three mechanisms within the consensus pipeline. First, anomaly detection is integrated into consensus: every standard transaction includes anomaly scores computed locally, and all hub nodes recompute and verify these scores during block validation, ensuring collectively agreed threat assessments. Second, trust scores from the CISSAN *TrustScoring* modules are recorded as timestamped blockchain transactions through the Metadata Application Programming Interface (API), providing a verifiable trust history per device. Third, the 51% Byzantine Fault Tolerant (BFT) consensus mechanism itself provides data quality verification, preventing any single compromised node from injecting unverified data.

Local trust scores are generated at IoT/OT devices registered in the network through trust models that incorporate i.e. device status, device responsiveness, anomaly risk scores, and believability scores as evidence. The calculations for these local rust scores are handled by the WebAssembly modules (WASMs) orchestrated and supervised by the Liquid AI software solution. For use cases one (1), three (3) and five (5) local trust scoring is handled with the *TrustScoring* module which calculates a local trust score from device responsiveness and anomaly/believability scores. A detailed description of the trust scoring can be found in the CISSAN D5.4 report. Local trust scores are used for blacklisting and are aggregated in obtaining a global trust score as per the trust model. The global trust score and its metadata are shared within the custom trust object of the Structured Threat Information eXchange (STIX) threat report, which allows for their propagation across the security system as part of various mechanisms for generating collective intelligence within IoT networks.

Through the collective intelligence mechanisms provided by the CISSAN platform, the local observations and analysis are integrated into a form of shared, trusted knowledge, which enables the coordination of decisions, the allocation of security tasks, and the adaptation of defences within the IoT/OT network, thereby increasing cyber resilience, promoting interoperability and digital sovereignty, and delivering tangible benefits to European stakeholders, critical infrastructure operators of transportation, smart grids and tunnel construction systems, and technology providers.

1.4 Trust and device management and access control

In large-scale IoT/OT environments, the importance of device governance and access control is crucial for cybersecurity, especially when only trusted and well-managed devices are expected to participate and collaborate with the network and other devices in the processes and activities related to network security. This is where trust management becomes very useful, as it helps identify abnormal and suspicious activities, even from registered and active IoT devices.

In the CISSAN platform, the device lifecycle begins with the registration of the device, which is achieved through the device ledger. This ledger ensures the integrity and consistency of the entire IoT device ecosystem, where the registration of all the devices is recorded. Depending on the results obtained from the collective intelligence mechanisms, including the trust scoring, the status of the device is managed throughout the lifecycle. In the event where the device is not trusted and is suspected of malicious activities, the device status is updated to blacklisted, which is also reflected

in the device ledger. This ensures the entire lifecycle of the device, including the decision made regarding the device, is tamper-resistant and can be traced. This updated status is then reflected in the orchestrator, where the device is marked as “blacklisted” in the device list. This ensures the device does not receive any security tasks and cannot participate in any network activities including performing security tasks or the routing of data. The deployments are updated to remove the blacklisted device and its tasks. To prevent the device from accessing services on the network layer, the device is isolated at the switch level.

Through the CISSAN platform’s trust and device management and access control mechanisms, it implements uniform access control decisions across the management, orchestration, and network layers, thus facilitating automated threat containment, operational resilience, and benefits to European stakeholders in the form of reinforced trust, accountability, and security in large-scale IoT systems.

The CISSAN Management Server interacts with the Eventchain blockchain through the Metadata API, a stateless Representational State Transfer (REST) interface. Device registration, trust score updates, and blacklisting decisions are recorded as signed blockchain transactions, each receiving a Secure Hash Algorithm (SHA) 3-256 hash as an audit reference. When a device's trust score falls below the configured threshold, the blacklisting decision --- including the final score, the threshold, and the triggering anomalies --- is recorded through the same consensus-validated pipeline. The Blockchain Key Value Store (BKVS) provides O(1) lookups for current device state, enabling the management server to query any device's status without traversing the full blockchain.

1.5 Security Requirements and Threat Landscape

In highly interconnected, critical IoT / OT networks, well-defined security requirements are vital to ensure that the systems are designed, delivered, and deployed to resist both unintended failures and cyber security attacks. The complex nature of IoT / OT systems, including the wide variety of devices, protocols, operational conditions, and stakeholders, greatly increases the attack surface of the systems, which makes ad hoc or purely reactive security approaches inadequate. Therefore, the CISSAN project has established security requirements that encapsulate the security needs of the CISSAN platform and its use case systems.

The security requirements specifications are discussed in detail within the confidential annexes of CISSAN D2.3 report, where the security requirements are discussed individually for each of the CISSAN use cases. The security threat for the IoT/OT use cases is driven by a wide range of well-recognized security threats, including those discussed within the MITRE ATT&CK for Enterprise and for Industrial Control System (ICS) frameworks, which discuss tactics and techniques for attacking industrial control systems, networks, and IoT devices. Common security threats include lateral movement within the operational environment, manipulation of sensor information, denial of service attacks on key systems, supply chain attacks, and the exploitation of legitimate credentials, which can have significant safety, operational, and economic benefits. Therefore, the security approach must align well with well-recognized security threat models while being specific to the security threats of IoT/OT systems.

In Use Case 1 (Transportation), the security requirements focus on ensuring the reliability and integrity of Global Navigation Satellite System (GNSS)-based positioning data used in public transport systems. As these systems depend on accurate location data for operations such as vehicle tracking, passenger information, and traffic management, threats such as GNSS spoofing, jamming, and data inconsistencies must be addressed. The use case requires the ability to detect anomalies in positioning data streams without disrupting existing systems, using lightweight and non-intrusive monitoring approaches. In this use case, vehicle position data is not considered sensitive, and no personal or passenger-related data is processed or transferred. This reduces privacy and data protection constraints, allowing the focus to remain on system-level integrity, availability, and anomaly detection rather than confidentiality of personal data.

In Use Case 2 (Smart Grids), the security requirements centre on protecting critical infrastructure operations under an evolving threat landscape where adversaries increasingly operate “inside the environment” through stolen credentials, remote maintenance access, or misuse of legitimate tools. This shifts the requirement from perimeter-only protection toward runtime security visibility within the OT segment, including the ability to detect abnormal behaviour on field devices without introducing disruptive overhead. Because smart-grid field assets are resource-constrained and process-optimized, the use case requires lightweight monitoring and response mechanisms that can run on

or close to operational devices, support local resilience even under degraded connectivity, and reduce dependency on external third parties for detection and decision-making. A further requirement is coordinated defence within the segment, where devices can share security-relevant observations and collectively raise confidence in detected events, enabling timely containment actions (e.g., restricting participation or isolating a suspicious device) while preserving operator oversight through centralized monitoring.

In use case 3 tunnel construction, a specific security requirement is to provide untampered monitoring data for tunnelling process control and decision making. Tampered data may lead to wrong or missing decisions and actions causing construction delays, damages, etc.

Due to the conflicting interests of parties involved in a tunnel project (e.g. client - contractor, employer – employee), the tampering of data is sometimes seen as a way to avoid problems or achieve specific gain (e.g. financial advantage). Thus, in most cases, internal actors are responsible for data tampering rather than outsiders. Therefore, data protection at all possible attack points between sensor and server is paramount. Devices such as sensors, data loggers, gateways or the central data management server may be entry points of attacks. Their identification and isolation help avoid the mentioned impacts on tunnel projects.

In use case 4 Manufacturing Execution system, the security functions monitor the device data with help of device management system which is authorising the device functionality with correct software and executes automatically the predetermined test cases for the device functionality as well as for the addressed security functionalities. The outcome of these tests is verified for the correctness also to enable tampering detection. If there is anomaly or deviation noted the system or its interfaces, the device gets automatically either updated or blacklisted from the system. Therefore, data protection at all possible attack points between device, gateways and manufacturing execution servers is a necessity.

In use case 5 (Joint Use Case, Automated Disaster Recovery), the security requirements centre on maintaining the integrity and trustworthiness of device governance decisions across a multi-organizational, multi-domain deployment. The primary threats addressed by the blockchain-based security system include Byzantine faults, whereby one or more nodes may produce incorrect or malicious validation results; impersonation attacks, in which a compromised node attempts to submit validations under another node's identity; data tampering, where an adversary seeks to alter recorded trust scores, anomaly events, or access control decisions after the fact; and insider threats inherent in multi-organizational environments, where parties with legitimate access may have conflicting interests. The Eventchain system addresses these threats through its zero-trust architecture: hub node identity is determined cryptographically from Elliptic Curve Digital Signature Algorithm (ECDSA) signatures rather than from claimed identifiers, per-hub RabbitMQ queues with regex-restricted permissions prevent cross-hub interference, and the dual-broker architecture ensures that compromise of the external message broker does not expose the internal transaction processing pipeline.

2 Blockchain-Based Network IoT/OT Security System

In heterogeneous IoT / OT environments, where assumptions of inherent trust within devices, networks, and stakeholders are untenable and where perpetual mitigation of external and internal security threats is an absolute necessity, zero-trust architecture (ZTA) provides an essential framework for effective and resilient cybersecurity solutions. ZTA, in essence, creates a robust framework in which data can be secured, and potential security breaches can be curtailed. The implementation of a ZTA involves the continuous monitoring and verification of the security status through risk and trust analysis, the inclusion of advanced technologies such as AI / machine learning (ML) for real-time security threats, and the creation of organizational culture in terms of security awareness and verification.

This approach has several advantages, including constant verification of device and system behaviour, improved control over compromised device and system security, and improved traceability and support for distributed security solutions. However, this approach has its disadvantages, including increased complexity and operational overhead, and the need for effective integration with legacy systems and performance-constrained devices.

For a single proprietor environment, where there are no or very little inter-organizational frictions, a traditional ZTA can be implemented. However, in cases where there are several parties involved, the implementation of a blockchain-based ZTA can provide several advantages. In the CISSAN project, research and development of a blockchain-based IoT/OT network security system with a ZTA on the CISSAN platform have been conducted. A blockchain-based ZTA can provide the advantage of creating a shared trust fabric that can be extended across several networks and organizational boundaries, which cannot be achieved through traditional ZTAs. A blockchain-based ZTA can be advantageous in cases where there are several parties involved, such as in the context of multi-party IoT/OT environments.

The blockchain-based IoT/OT network security system developed in the CISSAN platform adheres to this zero-trust, security-by-design and other security principles defined in D2.3 and meets the CISSAN platform security requirements specification outlined in its annex, as well as the regulatory and standards compliance requirements outlined within the standardisation action plan within Deliverable D7.1.

This section provides an overview of the blockchain-based IoT/OT network security system architecture, devices, and methodologies implemented therein, highlighting how zero-trust principles, blockchain, and collective intelligence are integrated to support effective and enhanced device and network security.

2.1 System architecture

The system architecture of the blockchain-based IoT network security system architecture is depicted in Figure 1.

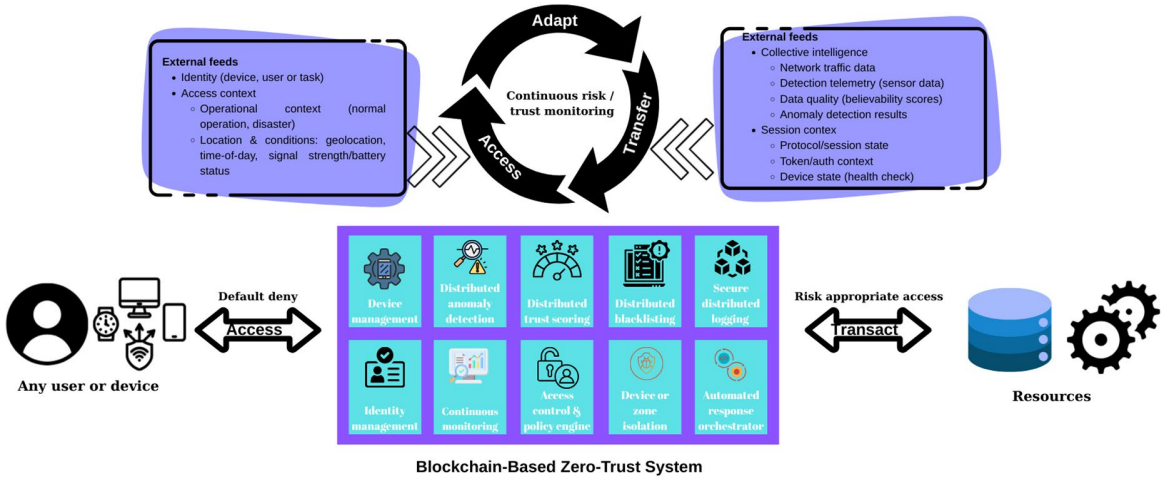

Figure 1. Blockchain-based IoT network security system architecture

The attributes of the system are as follows.

Blockchain-based data logging: A method of recording data entries on a decentralized, tamper-proof ledger within the blockchain infrastructure of the Councilbox blockchain system. This method ensures that any data entries made are immutable, transparently verifiable, and not reliant upon a single trusted entity.

Access control: The regulation of permissions to access certain resources for users or devices, providing the minimum necessary access privileges while continuously verifying identities prior to access. This includes the prevention of unauthorized connections to the network through the detection, restriction, or prevention of unapproved network access via the Radius server, the Virtual Private Network (VPN) tunnel, the firewall, the switch, and the device blacklist within the blockchain-based ledger.

Demilitarized Zone (DMZ): The network segment that separates the external network from the internal network, providing a strict access control mechanism while continuously verifying access to the network between the untrusted zone and the trusted zone.

Air-gapped network: A network that is not connected to any other network, either external or unsecured, thus providing no means of remote access to the network while requiring stringent control mechanisms to be employed for any type of data transfer to be made possible.

Post-quantum cryptography (PQC): A method of encrypting the data while in transit as well as at rest ensures that any external communications as well as the data at rest remain confidential while ensuring verifiability against any quantum threats. While the current system has not yet integrated PQC methods, it is planned to support PQC for encrypting payload data and performing digital signing to secure communications between the CISSAN Management Server and external systems post-project.

Policy enforcement: Provided through the Radius and CISSAN Management servers, which apply predefined security policies to control the behaviour of users, devices, and applications while ensuring that any access request is continuously evaluated to ensure compliance with strict access control policies.

Data/access segmentation: Involves the partitioning of the network/systems/data to segments to limit the lateral movement and only provide access to authorized segments or data sets.

User registration/authentication: Achieved through the RADIUS server and Windows machines to securely enrol users and authenticate their identity through Windows machines to ensure only authorized users can request or access the resources.

End-to-end encryption: Involves the use of Hypertext Transfer Protocol Secure (HTTPS) and post-quantum cryptographic techniques to encrypt the data sent to or from other systems to ensure only the intended recipient can access the data without the option for an intermediary to access the data.

Device management: Involves the use of device management techniques such as device registration, whitelisting, blacklisting, and isolation to ensure only trusted devices access the resources while untrusted devices are restricted or isolated from the resources. The orchestration server and the blockchain system involve the discovery of devices to be added to a device list and then registering the devices by recording the device details in the blockchain system.

Device authentication: Involves the authentication or validation of the identity and trustworthiness of the device before access to the network or resources is provided to the device to ensure only trusted devices communicate within the system or network. Device authentication is achieved through the handshake protocol with the server and the use of public key authentication with the blockchain system.

Network traffic monitoring: An ongoing analysis of data flows, detection of anomalies, and ensuring that all data communications comply with security standards. This is done through the firewall, Security Information and Event Management (SIEM), and devices that have the *AnomalyDetection* module deployed.

Data quality verification: Verifies the data quality (e.g., accuracy, completeness, plausibility) by applying empirical rules, ensuring that only reliable and accurate data is stored, shared, and used. This function is performed by any device having installed one of the Data Quality Verification modules.

Trust management: Involves the continuous assessment and management of the level of trust of the device, allowing access or restricting access as necessary. This function is performed by any

device that has the *TrustScoring* module deployed on it, the CISSAN Management Server and the blockchain system.

Anomaly detection: The automatic identification of unusual patterns and activities within a system or network, which might be a threat. This function is performed by any device installed with the *AnomalyDetection* module and the SIEM server.

2.2 Blockchain-Based Trust and Device Management System

2.2.1 Device identity and onboarding

In the CISSAN platform, the process of registering a device is performed as an automatic business process with the objective of ensuring that all connected devices are constantly tracked and trusted from the time they are introduced into the system. Once a device is automatically discovered by the CISSAN orchestration server or manually added by a security admin, it is added to the list of devices on the platform. The CISSAN Management Server recognizes the change in the device list and sends a request to update the status of the device on the device ledger on the Councilbox blockchain system. Therefore, as soon as a new device is added to the list of devices on the platform, it is immediately registered as a process, ensuring synchronization with the inventory of devices in operation, the blockchain system, and the security services provided on the platform.

Device registration is executed through the Metadata API by submitting a registered event with the device metadata (manufacturer, model, firmware, hardware identifier, capabilities). The API signs the resulting BKVS transaction and submits it to the consensus pipeline. After BFT validation, all nodes hold an identical registration record. The BKVS stores device state under a namespace derived from the API's public key, preventing unauthorised cross-key writes.

From a business process point of view, the process of registering a device on the platform is important as it aids in the management of the security state of the registered device during the process of updating its status, e.g., if the device has a low trust score, it may be blacklisted by the CISSAN Management Server.

2.2.2 Blockchain-based access control

In the CISSAN blockchain-based IoT network security system, access control is performed as an ongoing, trust-based process rather than a one-time access decision. New devices added to the network will undergo a registration process and will be recorded in a ledger on a blockchain, thereby establishing a trusted identity and state for each device. Once registered, devices will undergo an ongoing process of monitoring, utilizing decentralized anomaly detection and data quality verification techniques, in addition to continuously monitoring the device’s health by the CISSAN Orchestrator. Communication between the CISSAN Management Server and the IoT/OT devices is handled with Message Queuing Transport Telemetry (MQTT) and Hypertext Transfer Protocol (HTTP) protocols depending on the device. MQTT is used for the Remote Terminal Unit (RTU) devices on the ICS Zone and HTTP is used for Raspberry Pis on the IoT Zone of the CISSAN platform. The results of each of these processes will be combined to determine trust scores representing the current state of each device in terms of its overall security and trustworthiness. If a device has a trust value below a set threshold, it will automatically be blacklisted by the CISSAN Management Server, and its status will be recorded in the device ledger system of the Councilbox blockchain system to ensure traceability and consistency across the CISSAN platform. The actual implementation of access control is performed by preventing access to network resources and isolating the device at the switch level triggered by the CISSAN Management Server, thereby maintaining network security and resiliency through a policy-based governance system.

Access control decisions are enforced through consensus-validated transactions: no single component can unilaterally alter a device's access state. When the management server determines that a device's trust score has fallen below the threshold, it issues a blacklisting request to the Metadata API, which records the decision (final score, threshold, triggering anomalies) and submits it to the consensus pipeline. The block is accepted only after 51% of hub nodes validate it.

Eventchain's zero-trust model strengthens access control at the infrastructure level. Hub identity is verified cryptographically from ECDSA signatures rather than claimed identifiers, preventing

impersonation attacks. BKVS namespace isolation ensures each API key can only write to its own namespace. Per-hub RabbitMQ credentials with regex-restricted permissions prevent cross-hub access.

2.2.3 Logging and auditability

Logging and auditability can be viewed as the foundational components that facilitate the achievement of transparency, accountability, and trust within the security decisions and collective intelligence mechanisms in the CISSAN platform. This is achieved by logging device events on the Councilbox blockchain system, including security-related events such as device registration, updates to the trust score, anomaly risk score, believability score, and access control decisions such as blacklisting. Critical state changes, including updates to the status of the device and trust decisions, are stored within the blockchain-enabled device ledger. This ensures that the audit trail is immutable and unalterable and can be accessed by authorized stakeholders. The concept of integrating operational logs and blockchain-enabled records can be viewed as a means of facilitating the analysis and verification of security decisions and automated decisions made by the system. By ensuring that security decisions are observable and verifiable, the logging and auditability of device events can be viewed as a means of enhancing the level of governance and trust within the security decisions and automated decisions made by the CISSAN platform.

Eventchain records every device governance event (registration, trust score update, anomaly detection, and blacklisting) as a signed transaction. Transactions are hashed with SHA3-256, organised into Merkle trees (up to 1000 per tree), and included in blocks that require 51% BFT consensus before being permanently appended. No recorded event can be altered or removed after consensus.

The Blockchain Explorer provides a web-based visualisation interface that enables operators and auditors to inspect recorded events in real time. Events are browsable by block height, transaction hash, or device identifier, providing multiple access paths for audit and investigation purposes. For programmatic access, the BKVS API supports O(1) lookups for current device state by key, as well as namespace-scoped key listing, enabling integration with external monitoring and compliance systems.

For external verifiability, Eventchain employs periodic Bitcoin anchoring: every 180 blocks, the system computes a Merkle root over the epoch's block hashes and records it as an OP_RETURN transaction on the Bitcoin blockchain. This anchoring mechanism provides an external, independently verifiable proof of the Eventchain state at each epoch boundary, ensuring that the integrity of the audit trail can be verified against a public, permissionless blockchain without reliance on the Eventchain infrastructure itself. A full cryptographic proof chain can be constructed from any individual transaction up through its Merkle tree, the containing block, the epoch Merkle root, and the corresponding Bitcoin transaction.

2.3 Collective Intelligence for Threat Detection

2.3.1 Data sources and telemetry

In this section, the data sources and telemetry used to facilitate collective intelligence within the CISSAN platform and its use case solutions for threat detection are described, as well as how disparate data feeds of information are converted into actionable security information. A summary of the various data types collected from devices, networks, security services, and management components, as well as a description of how each data source is used in anomaly detection, data quality verification, trust scoring, and decision-making are provided. A description of how local data is combined to create global situational awareness, used in automated defence, device management, and resilient operation of IoT and OT networks is also described.

Use case 1: Transportation

Use Case 1 addresses the resilience of GPS-based positioning used in public transport systems, such as buses and trams. These systems rely on satellite-based positioning for operational services including vehicle tracking, passenger information, and route management. As part of critical

infrastructure, disruptions to positioning data—whether caused by signal interference, spoofing, or other anomalies—may affect the reliability and trustworthiness of transport services.

Within the CISSAN platform, the use case focuses on analysing positioning data streams originating from public transport vehicles to identify anomalous behaviour. The data is transmitted through existing operational telemetry systems and made available to the CISSAN environment via standardized interfaces. The platform enables monitoring of positioning consistency and supports the identification of irregular patterns that may indicate GNSS-related issues.

Mattersoft contributed to the use case by providing domain expertise and access to real-world public transport positioning data and system context. The implementation and execution of anomaly detection mechanisms were carried out within the CISSAN environment by project partners, while Mattersoft supported the definition of requirements, interpretation of results, and assessment of operational relevance.

The use case demonstrates how existing transport data flows can be leveraged to improve situational awareness and resilience without introducing changes to operational systems. It showcases the potential of integrating cybersecurity monitoring capabilities with positioning-dependent services in a scalable and non-intrusive manner (Table 1).

Table 1. Collective intelligence in use case 1

Data Source / Component	Type of Data	Purpose in Collective Intelligence	Processing / Analysis Used	Output / Used By
GNSS Receivers (Public Transport Vehicles)	Raw GNSS positioning data (latitude, longitude, timestamp)	Provide primary positioning input for detecting anomalies across multiple vehicles	Basic validation of position consistency (performed within CISSAN environment)	Input to CISSAN analysis components
Onboard Systems / Driver Terminal	Processed vehicle positioning and operational context data	Provide contextualized positioning data and ensure integration with transport systems	Data forwarding and formatting	Transmitted to backend systems
Transport Backend Systems	Aggregated vehicle position data streams	Enable centralized access to positioning data from multiple vehicles	Data aggregation and routing	Data forwarded to MQTT interface
MQTT Interface	Real-time telemetry data streams	Enable standardized and scalable data exchange with CISSAN platform	Message brokering and data transmission	Data delivered to CISSAN platform
CISSAN Platform (Analysis Environment)	GNSS positioning data streams	Detect anomalies using collective intelligence across multiple data sources	Pattern-based anomaly detection and consistency checks (implemented by project partners)	Anomaly indicators and alerts

Use case 2: Smart grids

The smart grids use case aims to detect anomalies in both operational and cybersecurity data across distributed grid assets, with a focus on identifying and localizing faults as well as detecting potential cyberattacks such as data manipulation or unauthorized control actions. This includes monitoring signals and logs from field devices such as RTUs (Table 2).

. **Table 2.** Collective intelligence in use case 2

Data Source / Component	Type of Data	Purpose in Collective Intelligence	Processing / Analysis Used	Output / Used By
Process Aware Stealthy Attack Detection (PASAD)	Raw Feeder L1-L3 and U1-U3 data	Provide data for anomaly detection	AI algorithms	Output to CISSAN Management server & PASAD Graphical User Interface (GUI)
NodeEye	Raw Feeder L1-L3 and U1-U3 data	Provide data for anomaly detection and classification	Multiple machine learning algorithms	Output to CISSAN Management server & NodeEye GUI
ROTOR	System logs	Provide data for anomaly detection		Output to Management Server
MQTT Interface	Real-time telemetry data streams	Enable standardized and scalable data exchange with CISSAN/GUI platforms	Message brokering and data transmission	Data delivered to CISSAN platform/Platform GUIs
PASAD GUI	Stream of feeder data and anomaly alarms	Detect anomalies using collective intelligence across multiple data sources		Anomaly indicators and alerts and graphs
NodeEye GUI	Stream of feeder data and anomaly alarms			Anomaly indicators and alerts and graphs

Use case 3: Tunnel construction

The tunnel construction use case aims to detect anomalies in tunnel monitoring data, especially caused by data tampering attacks. To achieve this, three systems/technologies have been developed as part of the use case solution:

- a data quality verification service,
- a blockchain-based data transfer system and
- a data signing system based on security chips.

The three systems/technologies are described in CISSAN deliverable reports D4.5 and D4.4 in detail.

Below Table 3 lists the main data sources, components, data types, their roles and purposes and the processing and analyses performed by them.

Table 3. Collective intelligence in use case 3

Data Source / Component	Type of Data	Purpose in Collective Intelligence	Processing / Analysis Used	Output / Used By
Sensors	Input: - Output: Sensor readings	Generation of OT data (tunnel monitoring data)	-	Sensor readings / Security chips, IoT Gateways
Security chips	Input: Sensor readings Output: Signatures (hashes)	Signing of sensor readings	Hash generation	Signatures / IoT Gateways
Loggers / IoT Gateways	Input: Sensor readings, signatures Output: Sensor readings, signatures	Collection and transfer of senor readings, verification of signatures	Signature verification	Sensor readings and signatures / Lightning nodes
Lightning Nodes	Input: Sensor readings and signatures Output: Sensor readings and signatures	Redundant, parallel transfer of sensor readings and signatures	-	Sensor readings and signatures / GeodataHub server
GeodataHub Server	Input: Sensor readings and signatures from Lightning nodes Believability scores from data quality verification service Believability thresholds from users Output: Sensor readings to data quality verification service Alarms to end users	Mgt/storage of sensor readings, and believability scores Verification of signatures Alarming of end users	Verification of signatures Check of believability scores against thresholds Alarm generation and sending	Sensor readings / data quality verification service Alarm messages / end users
Data quality verification service	Input: Sensor readings, data quality (DQ) rules & parameters Output: Believability scores	Calculates believability scores for sensor readings	Time series analysis (empirical rules, AI)	Believability scores / GeodataHub server

Blockchain	Sensor readings (hashed)	Permanent anchoring of sensor readings	-	-

Use case 4: Bittium Manufacturing Execution System (BMES)

At the moment, Bittium use case 4 does not use the CISSAN blockchain-based IoT network security system. This will be revalidated for the next stage of BMES architecture. The used monitoring methods are as follows Table 4.

Table 4. Collective intelligence in use case 4

Data Source / Component	**Type of Data**	**Purpose in Collective Intelligence**	**Processing / Analysis Used**	**Output / Used By**
IoT devices	Device readings, status, metadata, ping data, SW version data	Detect anomalies and faults	Data quality verification, anomaly detection	Anomaly scores, trust scores
Network monitoring	Traffic metadata, flow statistics	Detect network-level attacks	Anomaly detection, correlation	Network risk indicators
Security agents	Alerts, logs, events	Provide local security evidence	Correlation, aggregation	SIEM system

Use case 5: Joint use case

The following Table 5 represents the joint use case approaches related to collective intelligence.

Table 5. Collective intelligence in use case 5

Data Source / Component	**Type of Data**	**Purpose in Collective Intelligence**	**Processing / Analysis Used**	**Output / Used By**
IoT devices / sensors	Sensor readings, status, metadata, ping data	Detect anomalies and faults	Data quality verification, anomaly detection	Anomaly scores, believability scores, trust scores
Network monitoring	Traffic metadata, flow statistics	Detect network-level attacks	Anomaly detection, correlation	Network risk indicators
Security agents	Alerts, logs, events	Provide local security evidence	Correlation, aggregation	STIX reports, trust inputs
Device ledger (blockchain)	Device identity, status, history	Track device lifecycle and trust	Trust scoring, policy checks	Device status updates (e.g. blacklist)
Orchestrator	Task status, deployment info	Coordinate defence and recovery	Optimisation, policy enforcement	Task distribution actions
Trust scoring service	Trust values, thresholds	Support access control decisions	Trust model evaluation	Blacklisting / isolation decisions

External Cyber Threat Information (CTI) (optional)	Threat indicators, advisories	Enrich situational awareness	Correlation, validation	Enriched threat context
Remote Terminal Units (IIoT)	System signals, logs, process/file/network state, resource metrics	Gain local security visibility required for CI	OS-level collection	Rotor-monitor modules
Rotor-monitor (modules)	Structured anomaly events (JSON)	Local intelligence, that seeds CI sharing and peer validation	Lightweight rule-, deviation, and threshold-based checks	Peer comparison & trust evaluation service, SIEM aggregation
Peer comparison & Trust evaluation service	Incoming peer report, local snapshot report (JSON)	Validate peer observations and convert consistency into trust evidence	Comparison of anomaly categories, consistency computation, EMA for local trust update	Management server (trust management), SIEM
Management server	JSONL logs, JSON (STIX2.1)	Aggregated visibility of CI inputs and outcomes, decisions based on CI logic	Trust calculation, Web interface visualisation, STIX report generation (CTI)	Automated security actions, Blockchain system, Human analysts, CTI sharing infrastructure
SIEM (Wazuh)	Security telemetry	Operator-facing oversight and correlation across devices/time	Parsed/decoded rules, indexing, visualization, alerting	Human analysts

2.3.2 Anomaly detection and risk scoring methods

Anomaly detection techniques are used as collective intelligence techniques to identify potential threats, faults, and anomalies based on the analysis of patterns in distributed data sets and system components. The CISSAN platform uses statistics and machine learning based anomaly detection techniques for decentralized and hybrid anomaly detection in device, network, and service telemetry for the transportation use case, allowing for local and cross-domain detection of anomalies in the expected behaviours of different systems. The results of the different anomaly detection techniques are converted to risk scores, which quantify the severity, confidence, and potential impacts of the identified anomalies, allowing different types of observations to be compared, integrated, and used uniformly. These risk scores are further correlated, used, and shared as inputs to other reasoning processes such as trust scoring, orchestration, and access control. Anomaly detection techniques, along with risk scoring, enable the platform to identify potential threats at an early stage by continuously combining local detection results to system-wide risk scores, thus allowing for coordinated, adaptive defence in the network.

2.3.3 Trust scoring methods

Trust scoring is used as a collective intelligence technique for threat detection, in which information is gathered from networked devices in the CISSAN platform and interpreted to provide a collective understanding of the behaviour of devices and systems. Rather than using a single sensor to detect

potential threats, the CISSAN platform aggregates information such as results obtained from anomaly detection, data quality verification, the reliability and health status of devices, and correlated security events to calculate trust scores. These trust scores provide a comprehensive understanding of the overall risk and trust associated with a given device or system. Trust scoring is a technique by which the overall behaviour of devices and systems is understood in a collective manner, which is crucial in the detection of subtle, evolving, or coordinated threats. These threats may not be easily recognizable by a single entity. Trust scores, which fall or rise above a given threshold, are used to detect potential compromises, misbehaviour, and insider threats.

Applied in the ICS Zone of the CISSAN platform, trust scoring provides the primary decision signal for runtime containment actions. In this segment, trust scores are derived from peer consistency: devices exchange security observation reports and compare received reports against a locally generated snapshot, under the assumption that benign devices operating under comparable conditions should broadly agree. Each peer translates agreement or divergence into an evolving trust value using an exponential moving average, maintaining a local trust table that reflects its current confidence in other participants. These local trust assessments (“peer opinions”) are then shared to the management server, where they are aggregated into a global trust score per device. When the aggregated trust for a device falls below a configured threshold due to persistent or significant inconsistency, the platform triggers a state change (trusted --> untrusted) and can isolate the device to contain risk.

The trust scoring of IoT devices on the CISSAN platform is demonstrated with Raspberry PI devices, representing IoT devices of the different use cases in the CISSAN platform. Execution of the trust scoring is handled with dedicated WASM-modules that calculate local trust scores for individual devices based on device responsiveness and the scores derived from the different anomaly detection methods. The derived trust scores range from zero (0) to one (1), with 0 indicating low trust and 1 indicating high trust. Trust scores are stored locally at device level and shared with the management server for global trust scoring of the network. In cases where the trust score of a device falls below a set threshold, the management server will blacklist the device. The status of the device is recorded in the Councilbox blockchain system for traceability and consistency Details on the trust scoring is presented in the CISSAN D5.4 report.

2.3.4 Data quality verification and believability scoring methods

Cyberattacks can affect OT data (e.g., sensor data, measuring data) and manifest themselves in specific data patterns and changes of OT data quality parameters. Sometimes, attacks like data tampering might not leave any other traces in IoT environments than the change of OT data. To detect such cases, an empirical methodology and related software system have been developed - the Data Quality Verification System (Figure 2). It aims to detect attacks through a comprehensive, domain-specific OT data quality analysis and monitoring, and to respond to them through sending alarms and flagging the affected data.

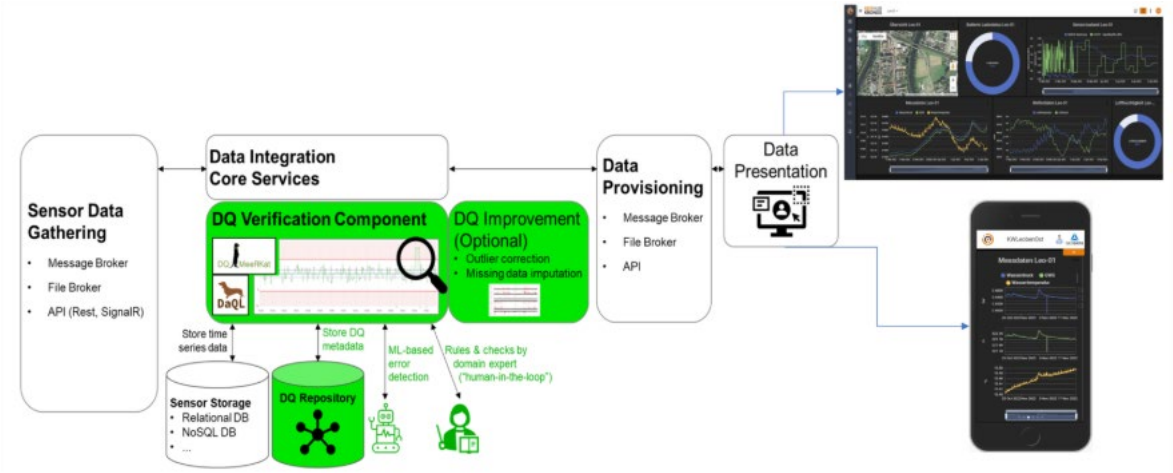

Figure 2. Data Quality Verification System (green part) connected to an IoT platform used in the tunnel construction use case

The developed system is described in CISSAN deliverable D4.5 report in detail. The fundamental attack detection approach is based on calculating the data quality dimension ‘believability’ that is represented by Believability Scores. A Believability Score is defined as a calculated numerical value between zero (0) and one (1) for a certain granularity level and a certain believability aspect of the data.

“0”: data is unbelievable

“1”: data is believable

(0,1): believability is between unbelievable and believable

The Believability Scores are processed by domain-specific Data Quality Rules that apply special mathematical/statistical methods and sophisticated concepts such as dynamic time warping, clustering, windowing and aggregation. The scores are assigned at different granularity levels to single (sensor) data values, a sequence of (sensor) data values (= a time series window), an entire (sensor) time series, a group/cluster of several (sensor) time series, and can be aggregated to a total score for all OT data available in a data system.

The Data Quality Rules analyse the accuracy, timeliness, noise, frequency, trends, change points, etc. of the OT data, search for outliers and compare the OT data with reference data (e.g. predicted, expected OT data) and, finally, return Believability Scores. If the scores exceed certain (user-defined) thresholds, the data is assumed to be unbelievable/implausible (e.g., tampered by a cyberattack), flagged, and an alarm is generated in the system. Figure 3 illustrates an example where the believability scores of a sensor time series have been processed for the believability aspects frequency (blue line) and noise (green line) at 4 different points in time. The example shows the degrading overall believability score (yellow line) of the time series that includes a period of missing data, noisy data and an outlier.

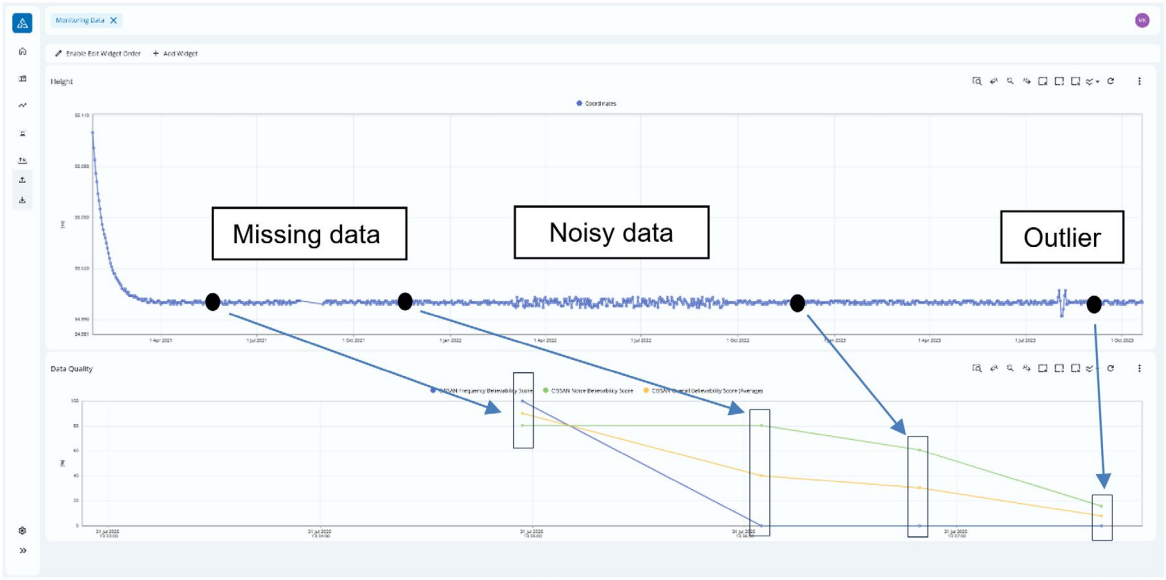

Figure 3. Example of a sensor time series (upper diagram) and its Believability Scores (lower diagram) displayed in a dashboard of the developed DQ verification system.

2.3.5 Collective threat intelligence sharing mechanisms

STIX is used as a collective threat intelligence sharing mechanism by providing a common, structured, and machine-readable way to share, correlate, and reason about CTI across distributed components and domains. Within the platform, security events, anomaly findings, trust-related information, and supporting evidence are packaged into STIX 2.1 objects and bundles, allowing heterogeneous systems to exchange not just raw alerts but contextualised and linked threat knowledge. By using STIX format, evidence from different sources can be correlated into coherent threat reports, enabling a shared situational awareness that goes beyond what any single component can achieve alone. These STIX-based reports are then ready for sharing via CTI infrastructure, and to be consumed by decision-making, orchestration, and governance services, ensuring that collective intelligence is built from consistent, interoperable, and explainable threat representations. In this way, STIX contributes to collaborative threat detection and response, transforming distributed

observations into coordinated, system-wide security actions. The application of the STIX report format in CISSAN is detailed in CISSAN deliverable D5.4 report.

2.3.6 Monitoring, logging, data analytics and alerting

The CISSAN platform aggregates monitoring, logging, and event data from the networked devices in the CISSAN platform and security tasks running on the devices, thereby creating a unified observation platform that represents the real-time status of the infrastructure. Data analytics processes this variety of data to identify patterns, trends, and correlations that may indicate faults, attacks, or potential threats, and the alerting mechanisms ensure that relevant findings are communicated to relevant parts of the infrastructure. This way, the monitoring and analytics platform combines local observations with cross-domain analytics and shared alerts to create a shared understanding of the environment that facilitates collective decision-making, response, and adaptation to changing situations. This way, monitoring and analytics transform raw data into useful collective knowledge that improves threat detection, accountability, and network security.

In the OT segment, this monitoring and analytics loop is realised as a collective intelligence workflow that turns device-local visibility into shared, actionable awareness. Each RTU produces structured security observations from its local monitoring cycle and publishes them over the security communication overlay, allowing peers and the management layer to consume the same event evidence with minimal delay. Peer devices do not merely forward alerts: they validate incoming observations against a fresh local snapshot and translate agreement or divergence into trust updates, which are then logged and aggregated centrally. This combines three views into a unified operational picture: local anomaly evidence from the source device, peer corroboration signals that indicate whether the event aligns with the segment’s expected state, and the evolving trust state that governs eligibility and containment actions. In this way, monitoring and logging support both human-facing alerting and machine-facing decision signals enabling the OT network to react collectively to suspicious behaviour even when individual devices are resource-constrained and cannot sustain continuous, heavyweight analytics on their own. The applied CI flow is detailed in D5.4.

Eventchain contributes to the CISSAN platform's monitoring, logging, and analytics in the following way:

- Monitoring. The Blockchain Explorer provides a real-time web view of blocks, transactions, consensus validations, and BKVS entries. Operators observe governance events as they are recorded, providing continuous visibility into the network's security state.
- Logging. Every governance event is recorded as a signed, timestamped blockchain transaction. Unlike conventional log systems where entries can be modified or deleted, the append-only blockchain structure and BFT consensus guarantee tamper-proof logging. Each transaction carries a hash and signature enabling independent verification.

2.3.7 Integration with security operations (SIEM and SOAR)

Integration with security operations tools, including the SIEM, and SOAR (namely the CISSAN Orchestrator), enables collective intelligence by harnessing the distributed and automated capabilities of the system with existing organizational security workflows. In this way, security events, alerts, and detailed threat intelligence generated by the system can be propagated to SIEM systems for correlation and analysis, while SOAR systems can utilize this data to launch or orchestrate automated response playbooks. At the same time, knowledge and decision-making generated by the CISSAN management server, such as analyst judgments and incident response actions, can be propagated back into the system to improve trust scores, refine threat context, and influence orchestration and access control decisions. This bidirectional flow of information ensures that machine-driven collective intelligence is complemented by human-driven capabilities to improve detection and response effectiveness.

In the OT/ICS lab deployment, a central aggregation point for security monitoring is the SIEM, where Rotor outputs are mirrored for centralized visibility and post-event analysis. In practice, the same security overlay used for peer exchange is also used to forward structured anomaly reports from the RTUs to the management/server layer, where they are serialized into log streams suitable for SIEM ingestion. In the lab setup, a Wazuh agent in the management zone monitors these Rotor log streams and relays them to the Wazuh SIEM server for indexing, visualization, and correlation. This provides a single place for operators to inspect event sequences across multiple RTUs, correlate device-local

findings with peer reactions and trust evolution and retain evidence for incident analysis and validation of the collective-intelligence workflow.

3 Implementation and Integration

3.1 Implementation on CISSAN Platform

In the Smart Grids use case, the Rotor framework enables RTUs to translate device-local anomaly observations into peer-verifiable trust updates that support collective, runtime security decisions. Each RTU is able to generate a structured anomaly report from its local monitoring cycle, or based on a prompt by a peer, where detected events are represented as categorized findings and can be interpreted as risk-relevant indicators of abnormal behaviour. Rather than relying on a single detector, Rotor uses these anomaly outputs as the evidence base that peers exchange over the MQTT-based CI overlay, allowing the segment to reason collectively about whether a device's reported security state is plausible.

Operationally, local trust scores on the RTUs are derived from peer consistency, using anomaly evidence as the input. When a report is received, the peer device compares the sender's anomaly categories against its own locally generated snapshot for the same moment, producing a consistency score (φ) that captures agreement versus divergence in observed security state. This consistency result is then converted into an evolving trust value using an exponential moving average, so that sustained agreement builds trust gradually, while repeated disagreement drives trust downward in a stable but responsive way. Each RTU maintains a local trust table for its peers and publishes compact trust updates ("trust deltas") upstream, where the management server aggregates them into a global trust view used to support containment actions such as blacklisting or isolation when trust falls below threshold. The operational details of the anomaly detection and trust calculation in relation to Rotor, are explained in more depth in CISSAN deliverable reports D5.2, D5.4 and D2.3.

Trust scoring for use cases one (1), three (3) and five (5) on the CISSAN platform is handled with the *TrustScoring* WASM. The module was first implemented in Python and then translated to a WebAssembly. WebAssembly was chosen for its capability to be run on heterogeneous hardware without modification. Managing, distributing and executing the WASM-modules are handled with the Liquid AI-based orchestrator located on the CISSAN Orchestrator server and supervisors running on the Raspberry PIs representing IoT devices for the transportation and tunnel construction use cases. In the CISSAN platform the Raspberry Pis are located in the IoT zone.

The module takes as input a list of peer devices in the network, the risk scores of the *AnomalyDetection* module and the believability scores of the Data Quality Verification modules. The module checks the responsiveness of its peer devices, generating an initial score for device trust. Risk/believability scores are used to generate another score which is merged with the first score to create the local trust score ranging from zero (0) to one (1), with zero representing low trust and one representing high trust. The scores are stored locally and shared with the management server for blacklisting purposes, generating global trust scores and for storing in the Councilbox blockchain. A more detailed description of the trust scoring module is found in the CISSAN report D5.4.

3.2 Integration with external systems

Arctos Labs optimization solver integration

The CISSAN platform integrates with the Arctos Labs Optimization Solver via the Optimization Solver API (specifications defined in CISSAN deliverable report D6.2 - Annex 3). The API is implemented with HTTP as the mechanism to operate on the API endpoints.

The purpose with the API is to provide the client with the optimal distribution of tasks over the network given characteristics and constraints for tasks and network devices respectively. The API is based on a few endpoints each supporting a selected set of HTTP operations. Via the '*taskandnetwork'* endpoint the clients prepare the optimization by providing supplementing data on the task and the network subject for optimization. Via the *'deploymentoptimization'* endpoint the client can, create, list poll and delete optimization jobs.

The optimization solver does not explicitly use the features of the CISSAN blockchain-based IoT network security system, but works in conjunction with the system.

Clavister smart grids system integration

The CISSAN platform integrates with Clavister PASAD, which is used for local software-based relay fault detection in smart grid substations. Voltage anomaly events detected locally in substations are correlated centrally to provide actionable incident events for the grid operator, which contain information about affected substations, affected sensors, incident duration and incident origin information. These correlated incident events are distributed to the CISSAN platform a via MQTT interface to allow the grid operator to have a single pane of glass of cyber security and operational incidents.

Clavister PASAD does not explicitly use the features of the CISSAN blockchain-based IoT network security system, but rather it provides intelligence via correlated incident events shared with the CISSAN platform, working in conjunction with the system.

Councilbox blockchain system integration

The CISSAN platform integrates with Eventchain through the Metadata API, a stateless REST service with JWT authentication (HS256). The management server and other components record and query device events through standard HTTP calls without direct blockchain interaction.

The API exposes four operations: device registration, trust score updates, anomaly event recording, and blacklisting. Each operation produces a signed transaction (ECDSA secp256k1), and the caller receives a SHA3-256 transaction hash as an audit reference. Device state is stored in the BKVS with namespace isolation, enabling O(1) lookups.

The integration flow: the management server issues an authenticated request to the Metadata API, which signs and submits a BKVS transaction to the consensus pipeline. Hub nodes validate the block through BFT consensus, and the event is permanently recorded. All events are queryable by device identifier and event type.

Mattersoft GPS system integration

In the transportation use case, Mattersoft integrates real-time GNSS location data from operating public transport vehicles into the CISSAN platform to support GPS/GNSS anomaly detection research. The integration is implemented as a secure, read-only, MQTT-based interface that provides near real-time fleet-wide access to vehicle positioning measurements. The data is published using Information Technology for Public Transport (ITxPT)-compliant message formats, including GNSSLocation messages (approximately 1 Hz) and AVMS Runmonitoring messages that provide trip and operational context. This combination enables the CISSAN platform to analyse GNSS behaviour under real-world conditions and to develop and evaluate methods for detecting spoofing, jamming, and other positioning anomalies while maintaining interoperability with existing public transport systems. Please see CISSAN deliverable D6.2 - Annex 2 for a complete integration description.

3.3 Scalability and performance considerations

Eventchain employs several mechanisms to accommodate growing device counts and transaction volumes without degrading performance.

Tree-based transaction organisation. Transactions are organised into Merkle trees, with multiple trees per block. This batching decouples transaction throughput from block creation frequency, absorbing bursts of IoT events without increasing consensus overhead.

Lightweight consensus. Consensus validation scales linearly with hub count: each hub independently verifies the block hash, signature, Merkle root, and anomaly model version. For very large deployments, network latency between geographically distributed nodes is expected to be the limiting factor rather than computational cost.

Efficient state queries. The BKVS provides O(1) lookups for current device state, maintained as a local cache on each node. Read operations do not impose load on the consensus pipeline.

Asynchronous Bitcoin anchoring. The periodic Bitcoin anchoring runs asynchronously and does not block the consensus pipeline.

Storage growth. Each node maintains a full blockchain copy. For high-volume deployments, pruning strategies that preserve Merkle roots for verifiability may be needed.

4 Validation of Blockchain-based IoT/OT Network Security System in CISSAN Use Cases

4.1 Use case 1: Transportation

Use Case 1 (Transportation) validates the use of collective intelligence for detecting anomalies in GNSS-based positioning data from public transport vehicles. Real-world positioning data is ingested into the CISSAN platform via a read-only interface without modifying operational systems, and anomaly detection is applied to identify irregularities in positioning behaviour that may indicate issues such as signal interference or inconsistencies (GPS spoofing and/or jamming). The outputs of anomaly detection contribute to trust scoring, where lower trust values indicate potentially unreliable data. As the integration is non-intrusive and observational, no direct enforcement actions such as device isolation or blacklisting are applied, and the approach focuses on improving situational awareness while maintaining compatibility with existing transport infrastructure.

4.2 Use case 2: Smart grids

Trust scoring using the Rotor framework is described in Section 3.1. Its validation is reported in D6.3, has been observed in separate demonstrations during the research process, and is planned for demonstration during the final workshop. In this scenario, an attack will be displayed targeting one of the RTUs, the framework is run, and the compromised node isolated based on the networks collective understanding of its status. Validation is straightforward because both the trust outcome and its supporting evidence are visible through the platform interfaces. Following anomalous activity on a target RTU, Rotor's peer-consistency updates propagate into the centrally aggregated global trust score, which can be observed directly from the management GUI. When the global trust score drops below the configured threshold, the unit is blacklisted and isolated, preventing it from participating in segment communications and containing further impact. Supporting evidence remains available via the SIEM views and local logs on participating components, enabling auditability and post-event analysis if results require further verification.

4.3 Use case 3: Tunnel construction

The results of the Data Quality Verification modules are used for calculating the local trust scores of the IoT devices with the *TrustScoring* WASM-module. The *TrustScoring* module is described in Section 3.1 with a more detailed description in CISSAN report D5.4. The module takes the results of the Data Quality Verification module and with results from checking peer device responsiveness, calculates a local trust score ranging from zero (0) to one (1) for IoT devices. These are stored locally and shared with the management server, where they are used for calculating a global trust score for the network. In a case where a device's local score is below an acceptable threshold, the device is blacklisted by the management server. Validation is straightforward. The results of the anomaly detection and trust scoring can be observed via platform interfaces. Global trust scores derived from the local trust scores can be seen via the management GUI along with the blacklist status of all the devices. Scores can also be checked on the Councilbox blockchain where they are recorded for traceability.

4.4 Use case 5: Joint use case

The Joint Use Case combines multiple CISSAN use cases into a single, shared platform deployment, where trust scoring functions as a common decision signal across segments. In this setting, trust inputs are produced by the use-case-specific mechanisms and are then aggregated centrally into a unified network-level trust view. This enables consistent enforcement actions, such as blacklisting and isolation, based on comparable trust-threshold violations, while preserving cross-use-case visibility for operators through centralized monitoring. The validation approach therefore follows the same principle as in UC2: trust score changes are observable in the management view, supporting evidence is retained in monitoring/logging components, and state changes can be verified operationally. More detailed validation steps per contributing use case are provided in their respective sections/deliverables.

5 Impact and Business Value

The CISSAN blockchain-based network security system generates considerable impact and business value due to the changes it brings to the way in which an organization secures, operates, and recovers complex IoT and OT infrastructures. The integration of zero trust, security by design and CISSAN security principles, and collective intelligence features such as decentralized anomaly detection, data quality verification, trust scoring, and collaborative security task distribution enables the system to improve the speed of detection, improve the accuracy of decision-making, and enable trustworthy disaster recovery. The integration of blockchain technology in the management and auditing of devices increases the level of transparency and trust in the actions performed by the system. From a business point of view, these features enable the organization to reduce downtime, lower operational risk, improve compliance with regulatory requirements, and protect critical services and reputation, thereby creating a scalable, resilient, and future-proof platform for digital operations.

5.1 Use case 1: Transportation

The transportation use case demonstrates how GPS positioning data from public transport vehicles can be monitored for anomalies within the CISSAN platform. The approach builds on existing operational data streams and does not require changes to the underlying transport systems. By analysing positioning behaviour, the platform can help identify irregularities that may indicate interference or inconsistencies affecting positioning-dependent services. The results show that collective intelligence can support improved situational awareness and contribute to more reliable and resilient public transport operations, while remaining compatible with current system architectures.

5.2 Use case 2: Smart grids

Use case 2 showcases methods to analyse cybersecurity and operational data to find anomalies on edge grid assets and alerting to CISSAN platforms for further analyzation.

By combining blockchain-based network security system, it can be ensured that the data is tamper-free and trustworthy. The platform could also provide additional zero trust securities and improve false-positive rates and negate any risks of spoofing alerts.

5.3 Use case 3: Tunnel construction

The CISSAN blockchain-based network security system enables the detection of data tampering attacks through applying anomaly detection and data quality verification methods, and the identification of the device(s) affected / point(s) of attack. The data can be excluded from further use, the devices blacklisted and deactivated. Therefore, the impact is that construction delays, damages and other negative consequences can be avoided. Tunnelling simply becomes more secure, efficient and economical.

5.4 Use case 4: Manufacturing execution system

As the use case 4 does not use block-chain based methods at the moment, however device management and network security system enables the detection of data tampering attacks through applying anomaly detection and data verification methods, and further the identification of the device(s) affected / point(s) of attack. The data can be excluded from further use, the devices blacklisted and deactivated.

5.5 Use case 5: Joint use case

The CISSAN blockchain-based network security system, which incorporates collective intelligence, significantly enhances the value and efficacy of mitigating multi-domain infrastructure attacks with an automated disaster recovery system by ensuring that the resulting disaster recovery process is trusted, resilient, and audit-worthy. The use of blockchain technology in device governance and security state management provides an unalterable and transparent record of device identities, trust levels, and access control decisions, thus ensuring a high degree of trust in automated actions taken during a crisis situation. The collective intelligence mechanisms, which include decentralized

anomaly detection, data quality verification, trust scoring, and task distribution and orchestration, ensure timely and precise detection of incidents, better prioritization of actions, and dynamic adaptation in response to cascading failures in complex infrastructures. From a business perspective, this results in lower system downtime, lower operational risks, and higher continuity of critical operations, while also reducing the reliance on manual intervention and expert resources, which are often scarce and valuable. From an operator's and stakeholder's perspective, it means higher trust in automated systems, better support for regulatory requirements, and protection of brand reputation, thus resulting in a more cost-effective, scalable, and forward-thinking approach to ensuring resilient digital operations in critical IoT and OT infrastructures.

6 Conclusions

This report outlines the design and implementation of the CISSAN blockchain-based IoT network security solution that leverages the power of collective intelligence to enhance the effectiveness of mitigating security threats in complex IoT/OT environments. This solution is built on the foundation of zero-trust architecture and is consistent with the overarching security principles that guide CISSAN. The solution ensures that trust is continually assessed, enforced, and auditable rather than simply assumed. The solution leverages the power of blockchain technology in order to provide enhanced anomaly detection, data quality verification, trust scoring, as well as the collaborative distribution of security tasks in order to provide distributed elements of the solution with the ability to work in collaboration with each other in order to provide enhanced detection, assessment, and recovery of threats in a timely manner. The solution leverages the power of blockchain technology to provide enhanced governance of devices, as well as the ability to assess and enhance trust to provide enhanced auditing of access control decisions such as blacklisting and isolation. In addition, the solution leverages standardized threat intelligence sharing technologies such as STIX to provide enhanced integration with industry standards and regulations. The system leverages the power of collective intelligence to provide enhanced, proactive, resilient, and trustworthy approaches that are more effective than more traditional approaches to security. Although further work is necessary to provide enhanced industrial adoption of this solution, the work has been validated for the use cases represented on the CISSAN platform and provides a strong foundation for providing enhanced, scalable, compliant, and future-proof approaches to blockchain-based network security for critical infrastructures that provide clear operational and business benefits for industrial stakeholders.