CISSAN

Collective intelligence supported by security aware nodes

D2.2 Risk, threat and impact analysis of distributed algorithms and load balancing solutions. Countermeasures.

Editors: Niko Candelin (Netox), Ilgin Safak (University of Jyväskylä)

contact: niko.candelin@netox.fi

Abstract

The integration of IoT and OT networks presents significant cybersecurity challenges due to their increasing complexity and interconnectivity requirements. This report examines distributed algorithms and load-balancing solutions in these networks, focusing on risks, threats, and implications. It discusses advanced methods for identifying and mitigating threats, including AI, threat intelligence, zero-trust architecture, and blockchain technologies. The report emphasizes the urgent need for advanced cybersecurity measures in IoT and OT networks, aiming to improve security, reduce risks, and ensure operational resilience. Implementing these strategies will enhance the cybersecurity resilience of EU enterprises, safeguard key infrastructures, and strengthen overall security and stability.

Participants in the CISSAN project are:

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

CISSAN-Collective intelligence supported by security aware nodes

D2.2 Risk, threat and impact analysis of distributed algorithms and load balancing solutions. Countermeasures.

Editors: Niko Candelin (Netox), Ilgin Safak (University of Jyväskylä)

Project coordinator: Alexey Kirichenko (University of Jyväskylä)

CELTIC published project result

Executive Summary

Integrating the Internet of Things (IoT) and Operational Technology (OT) networks in today's swiftly changing digital environment has presented considerable cybersecurity challenges. The increasing complexity of these systems and the requirements for interconnectivity have made them prime targets for cyberattacks, posing substantial risks to critical infrastructure and business operations. This research aims to address critical issues by delivering a comprehensive examination of the risks, threats, and implications related to distributed algorithms and load-balancing solutions in IoT and OT networks.

This deliverable D2.2 provides stakeholders in the cybersecurity of IoT and OT networks with a comprehensive analysis of the risks and countermeasures associated with distributed algorithms and load-balancing solutions, offering significant insights into the security of these networks. Comprehending these elements can help improve the safeguarding of infrastructures and bolster organizations' resilience against cyberthreats.

The report discusses advanced methods for identifying and mitigating cybersecurity threats, including AI, advanced threat intelligence, zero-trust architecture, and blockchain technologies. By implementing the proposed cyber-risk management strategies, stakeholders can proactively mitigate potential threats, ensuring business continuity. The focus on improved collaboration and information exchange can strengthen collaborations and collective defense strategies within the EU cybersecurity community.

The subsequent subjects addressed include investigating distributed algorithms and load-balancing strategies, identifying primary attack vectors in IoT and OT environments, and assessing architectural challenges in Collective Intelligence (CI) enabled IoT and OT networks. The proposed remedies to enhance security and efficiency and optimal strategies for mitigating cyber threats can help ensure robust protection against potential cyberattacks. The main D2.2 document is supplemented by confidential annexes presenting security assessment of selected CISSAN solutions based on distributed algorithms.

D2.2 highlights the urgent need for advanced cybersecurity measures in IoT and OT networks. By adopting the proposed solutions and methods, organizations can substantially improve their security stance, reduce risks, and achieve greater resilience of their operations.

The report can be of interest for European Union (EU) organizations since it corresponds with the EU's objectives of improving cybersecurity across member states. Implementing the suggestions will enhance the cyber resilience of EU enterprises, safeguard key infrastructures, and bolster the overall security and stability of the area.

List of Authors

- Niko Candelin, Netox
- Ilgin Safak, University of Jyväskylä

Table of Contents

List of Figures

Abbreviations

ABAC	Attribute-Based Access Control
AI	Artificial Intelligence
APT	Advanced Persistent Threat
CapBAC	Capacity-based Access Control
CI	Collective Intelligence
CISSAN	Collective Intelligence Supported by Security Aware Nodes
CRA	Cyber Resilience Act
CSF	Cyber Security Framework
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DNS	Domain Name System
DoS	Denial of Service
DT	Digital Twins
EU	European Union
FL	Federated Learning
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JIT	Just-In-Time
MFA	Multi-Factor Authentication
ML	Machine Learning
OT	Operational Technology
OTA	Over-The-Air
NIST	The National Institute of Standards and Technology
PBAC	Policy-Based Access Control
PUF	Physical Unclonable Functions
RBA	Risk-Based Authentication
RBAC	Risk-Based Access Control
SDN	Software-Defined Network
SSO	Single Sign-On
ZT	Zero-Trust
ZTA	Zero-Trust Architecture

1 Introduction

In the digital era, the convergence of Information Technology (IT), Operational Technology (OT), and the Internet of Things (IoT) has revolutionized how industries operate, and digital society works. While enhancing operational efficiency and providing unprecedented data insights, this interconnected ecosystem has also introduced a complex landscape of cyber risks. Effective cyber risk management is essential to safeguard sensitive information, ensure operations' continuity, and protect connected devices' integrity.

The European Union (EU) is regulating the digital landscape concerning IT/IoT/OT operational and technical security, as well as the development of hardware, software, and operating systems. Regulations underline the importance of cybersecurity to modern Europe and its economics.

Cybersecurity constitutes complete risk management. Effective or partially automated mitigative measures require precise data, integrity, and accessibility from the target environment/domain and about potential threats that could elevate cyber-risk.

Cyber-risk management in IT, OT, and IoT environments is a complex and evolving challenge. Organizations must adopt a holistic approach, combining technical controls, employee training, and robust policies to protect against the myriads of threats they face. By understanding the key attack vectors of each layer and implementing effective mitigation strategies, organizations can significantly reduce their risk exposure to safeguard their critical assets. The CISSAN (Collective Intelligence Supported by Security Aware Nodes) project addresses risk management research through multiple vectors and impact variables, ranging from specific IoT technical challenges and controls to a comprehensive perspective on environmental posture management.

Effective management of cyber risks necessitates a comprehensive security analysis, which detects potential vulnerabilities, evaluates the impact of these risks, and applies mitigation techniques, so maintaining the overall security and integrity of the systems.This report includes a security analysis of selected CISSAN systems created during the project, describing possible weaknesses, the steps taken to reduce risks found, and the overall efficacy of these security procedures in guaranteeing the confidentiality and integrity of the system's data and operations.

The project acknowledges the significance of collective intelligence (CI), which is implemented in practice via distributed algorithms and load-balancing methods, in managing security risks for IoT and OT networks and environments and recognizes that the risks and impacts of CI applications require analysis. Examples of such analysis for selected CISSAN solutions are presented in confidential annexes to D2.2.

1.1 Current IT/OT/IoT Ecosystems

The integration of traditional IT systems with OT systems and IoT devices characterizes IT/OT/IoT ecosystems. IT systems oversee data and application services, OT systems regulate physical processes and machinery, and IoT devices gather and transmit data. This integration enables real-time monitoring, automation, and improved decision-making while introducing multiple new avenues for cyberthreats. Each component of technical architecture, contemporary business, or procedures has distinct attack vectors, even if the potential damage may be comparable to other risks.

Modern infrastructures are vulnerable to deliberate harmful actions, particularly Advanced Persistent Threats (APT). Attackers leveraging IT, OT, and IoT weaknesses may evade detection for a prolonged time before being identified. This results from a decade of digitalization and a lack of a thorough comprehension of cyberthreats during the transformation process. Modern cyber-risk management encompasses effective components, including a multi-layered approach, prevention, detection, and response. However, these controls are predominantly handled in isolation, lacking the advantages of CI, wherein numerous controls could enhance visibility, security, or other threat-related information, facilitating prioritized cyber-risk management.

1.2 Cyber-Risk Management

Practices integrated into IT/OT/IoT ecosystems (digital business platforms) predominantly exhibit deficiencies in cyber-risk management skills. While organizational capacities are essential, they appear to represent the initial foundations for most institutions, encompassing both technological and operational dimensions. Nonetheless, the new law establishes the minimal extent of security control implementation for critical and essential organizations and their operations within the EU.

Current cyber-risk management is characterized by inefficiency, lack of coordination, IT-driven initiatives, or inadequate execution and implementation, as evidenced by continuing activities, evaluations, and threat intelligence reports. At the organizational level, it is essential to assess the adequacy of selected security controls in safeguarding vital services and functions, as well as to evaluate the consequences of potential losses resulting from cyber-attacks on those environments. Essentially, it pertains to the exposure of the environment to malevolent behaviours or agents, whether internal or external.

The project addresses cyber-risk management and identifies issues through comprehensive security posture management, ensuring visibility of all digital assets (IT/OT/IoT) for monitoring and management reasons. Every identity (device, program, user) plays a distinct function in the cyber-risk landscape. The project addresses several technological difficulties mentioned by the use cases.

Without a comprehensive understanding of digital (IT/OT/IoT) assets and potential dangers, such as vulnerabilities, you cannot manage organizational cyber hazards and risks to comply with new EU legislation, importantly the NIS2 Directive and the Cyber Resilience Act (CRA).

The CISSAN project builds sophisticated security algorithms for network nodes, empowering them to analyse traffic and manage data and signalling. This strategy seeks to tackle the intrinsic security difficulties of IoT and OT systems and the supplementary dangers resulting from the cohabitation of diverse technologies.

1.3 IT/OT/IoT Environmental Specific Risks

Managing cyber-risks is paramount for organizations operating in IT, OT, and IoT environments. The convergence of these domains presents unique challenges as each brings specific vulnerabilities and attack vectors. Effective cyber-risk management requires a comprehensive understanding of these threats and the implementation of robust mitigation strategies.

CISSAN intends to conduct risk, threat, and impact analysis for distributed functions and solutions, to develop corresponding countermeasures, and to contribute to an implementation framework for CI-enabled solutions. To this aim, the project Use Cases were examined and confirmed via threat modeling sessions conducted by Mint Security and via project workshops. The hypotheses concerning security threats aimed at IoT devices and the incidence of cybersecurity events were validated. The trend is concerning, given security threats aimed at IoT devices have escalated in recent years due to the expanding integration of IoT and OT technologies into daily activities and vital infrastructures.

2 Architectural Issues in IoT and OT Networks

This section discusses the general IoT architecture (providing a framework for IoT and OT networks) and key architectural issues in CI-enabled networks, while potential solutions are then presented in Section 3.

2.1 Architectural Issues in CI-Enabled IoT Networks

The IoT architecture (see Figure 1) has a multi-tiered framework intended to address the complexity and heterogeneity of IoT systems. The predominant model is the three-tier architecture, comprising the perception, network, and application layers. The perception layer comprises sensors and devices that gather data, the network layer manages data transfer, and the application layer processes and employs the data for diverse applications. Additional concepts include middleware architecture, service-oriented architecture and five-layer architecture, each catering to distinct requirements such as scalability, interoperability, and effective data management. The IoT environment comprises four principal elements: devices, connectivity, data processing, and user interface. Devices comprise sensors and actuators that gather and respond to data. Connectivity denotes the diverse communication networks and protocols for data flow among devices. Data processing encompasses the analysis and administration of gathered data, frequently employing cloud or edge computing technologies. The user interface includes the applications and services that enable users to engage with the IoT system, offering insights and control over connected devices. This extensive framework emphasizes the interrelated characteristics of IoT components and their functions in establishing a viable IoT ecosystem [1].

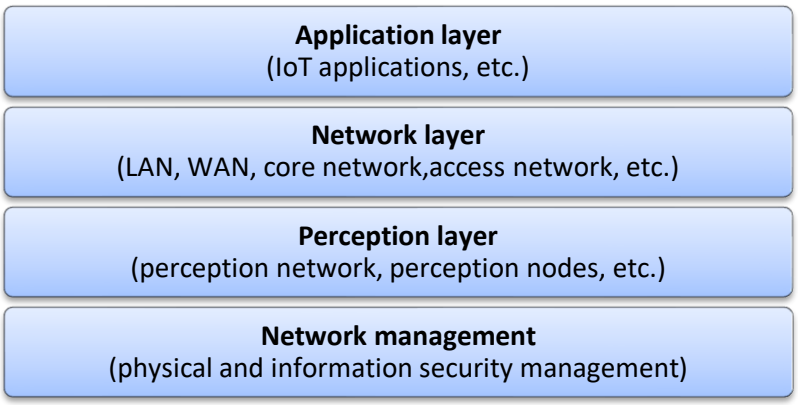

Figure 1. IoT layered architecture

Implementing CI into IoT networks presents transformational opportunities, allowing objects to collaborate in a decentralized and autonomous fashion. On the other hand, this transition faces considerable architectural challenges, especially regarding preserving security, scalability, and efficiency in dynamic, distributed settings. Architectural concerns must be addressed to guarantee CI-enabled IoT networks are scalable, self-organized, and safe, especially in contexts where devices may be susceptible to attacks or failures. As CI enables IoT devices to cooperate in decision-making, resource sharing, and data processing, the assurance of security and resilience inside these networks becomes more challenging.

We discuss below architectural challenges that arise with CI-enabled IoT systems including coordination and synchronization of distributed intelligence, adaptive learning and decision-making, decentralization and trust management, scalability, interoperability, security, resilience, and software implementation and configuration issues.

2.1.1 Coordination, Distribution, and Synchronization of Intelligence

In CI-enabled IoT networks, the coordination, distribution, and synchronization of intelligence for network security pose distinct issues not commonly encountered in standard IoT networks. This entails distributing security functionalities across the network in an efficient way, collaboratively analysing data and rendering decisions, and efficiently communicating and synchronizing actions independently of a central control so that IoT nodes can ensure network security collectively.

A fundamental challenge is ensuring the **uniformity of shared knowledge** throughout the network. As devices autonomously collect and analyse data, inconsistencies may occur, resulting in divergent

interpretations and judgments. To ensure that all devices maintain a consistent and up-to-date understanding of the network condition, sophisticated techniques for data fusion and consensus formation are needed. These algorithms must be sufficiently robust to accommodate the dynamic characteristics of IoT environments, where devices often enter and exit the network, and data streams are perpetually updated.

A crucial element is the **management of conflicting decisions** from various devices. In a CI-enabled IoT system, each device may possess distinct perspectives and priorities informed by its local data and aims. When differing perspectives clash, the network must devise strategies to settle conflicts and attain a consensus aligned with the larger system's goals. This needs sophisticated coordination protocols capable of negotiating and reconciling discrepancies in real-time, to ensure that the collective decision-making process is both efficient and successful. The network must also adapt to evolving situations and learn from previous interactions to enhance future coordination efforts.

Ensuring **real-time coordination** within a potentially extensive and dynamic network presents considerable difficulties. In IoT networks empowered by CI, devices must consistently exchange information and synchronize their behaviours to rapidly resolve emergent problems. This necessitates low-latency communication connections and effective data dissemination mechanisms to guarantee that all devices are informed of the latest events and can respond appropriately. The network must also exhibit resilience to communication outages and delays, which can hinder the synchronization process and result in suboptimal conclusions. Utilizing decentralized control methods, like distributed consensus algorithms and peer-to-peer communication protocols, might alleviate these problems by diminishing dependence on single points of failure and facilitating more flexible and adaptive coordination.

Distributing security functionalities over a CI-enabled IoT network poses considerable challenges due to the dynamic and heterogeneous characteristics of these networks. A primary challenge arises in identifying the appropriate criterion for allocating security tasks among devices. IoT networks are intrinsically dynamic, characterized by devices that regularly join and leave the network, differing in processing capability, energy resources, and data quality. This fluctuation complicates the establishment of a consistent distribution of security functions that remain effective over time. The fluid characteristics of IoT networks necessitate a security architecture that is exceptionally adaptive. Security functions, including intrusion detection, anomaly detection, and threat response, must be assigned in a manner that adapts to variations in network topology and device availability. This necessitates real-time surveillance and decision-making algorithms capable of reallocating workloads as required to ensure optimal security coverage. Nevertheless, creating such adaptable algorithms is intricate and requires significant processing resources, particularly when attempting to distribute the load among devices with varying capabilities.

Implementing security features throughout an IoT network requires both **design-time and real-time** considerations to ensure robust and adaptable security [2]. During the design phase, the architecture must be structured to address the dynamic characteristics of IoT environments, considering the diversity of devices, differing computational capacities, and energy limitations. This entails designing protocols for data encryption, authentication, and secure communication, in addition to implementing frameworks for decentralized decision-making and task allocation. Real-time considerations involve the ongoing assessment of network conditions and device statuses to adaptively modify the allocation of security responsibilities. This necessitates the implementation of adaptive algorithms capable of reallocating jobs according to current network load, device availability, and threat levels. Real-time coordination and synchronization are essential to ensure the uniform application of security measures throughout the network, thereby decreasing latency and enhancing responsiveness. By combining design-time planning with real-time adaptation, the network can uphold a high degree of security while effectively managing resources and swiftly addressing emergent risks.

The **optimization of resource utilization** is another challenge. IoT devices frequently possess constrained processing capabilities and battery longevity; therefore, security functions must be allocated to optimize energy efficiency while enhancing security efficacy. This involves finding a balance between processing tasks locally on the device and offloading them to more powerful nodes in the network, such as edge or fog nodes. Determining the requirements for this balance can be challenging, as it relies on elements such as the existing network load, the significance of the data being safeguarded, and the energy levels of the devices involved.

Interoperability challenges exacerbate the dissemination of security features. IoT devices from diverse manufacturers may employ disparate communication protocols and standards, complicating the implementation of a cohesive security policy throughout the network. Facilitating the participation of all devices in the collective security initiative necessitates standardization and the creation of

middleware solutions to integrate disparate systems. This introduces an additional layer of complexity to the distribution of security functions.

Data privacy and integrity are also critical concerns. As security functions are decentralized, sensitive data must be safeguarded during its transmission between devices. This entails the use of robust encryption and authentication protocols to guarantee that data remains secure against interception or alteration. Nonetheless, these security mechanisms deplete resources, complicating the optimization of security task distribution.

2.1.2 Adaptive Learning and Real-Time Decision-Making

The integration of adaptive learning with real-time decision-making introduces a distinct layer of complexity to CI in IoT networks. Devices must perpetually learn from one another and adjust their behaviour according to shared information. This entails analysing extensive data and incorporating feedback from other devices to enhance model refinement and decision-making precision. AI methods for enabling CI such as hierarchical machine learning (ML) and federated learning (FL) can be used for collaborative learning among devices while maintaining the confidentiality and security of raw data. Nevertheless, these strategies must be meticulously crafted to accommodate the heterogeneity of IoT devices, which may exhibit diverse processing capabilities, data quality, and network conditions.

Moreover, the fluid characteristics of IoT settings necessitate that the network adapts to emerging threats and evolving conditions. This necessitates ongoing surveillance and assessment of the network condition, together with the capacity to promptly implement updates and reconfigure the system in reaction to arising difficulties. Self-organizing principles, wherein devices independently modify their behaviour according to local interactions and overarching goals, can improve the network's adaptability and robustness. Achieving this level of self-organization necessitates advanced algorithms that can harmonize local autonomy with global coordination, ensuring that the network's collective behaviour coincides with the intended goals.

2.1.3 Decentralization and Trust Management

Enabling CI in IoT networks requires decentralization of security functions across network nodes. This may result in challenges related to scalability and interoperability, particularly when managing heterogeneous devices. Trust management is essential in decentralized systems, since it ensures the integrity and validity of data shared across nodes. This presents technological challenges owing to the need for effective systems to identify and counteract tampered, captured, or injected devices [3], [4]. Challenges related to the technologies and methods typically used for decentralization and trust management in IoT networks are summarized below.

The decentralization of IoT networks can be achieved through digital ledger technology (DLT), which offers enhanced security and transparency over non-DLT approaches by ensuring data integrity through immutable and verifiable records of all transactions and interactions within the network [5]. However, integrating DLT with IoT networks may be resource-intensive, requiring substantial processing power and storage, which may not be viable for all IoT devices [6]. Additionally, the lack of standardization for DLT-IoT integration may confound integration efforts. Scalability is a significant challenge since both DLT and IoT systems must manage extensive volumes of data and transactions effectively. Interoperability also presents a significant challenge as it might obstruct flawless communication among diverse devices and systems. Security and privacy issues are amplified due to the sensitive nature of IoT data and the need for strong safeguards against cyber-attacks. Moreover, latency and bandwidth constraints might hinder real-time data processing, while the energy efficiency of IoT devices may decline owing to the heightened computing requirements of DLT [7].

Trust Management: The dynamic and heterogeneous nature of IoT environments presents significant challenges in establishing and maintaining trust. Moreover, the resource limitations of IoT devices, including restricted processing capacity and energy, provide considerable challenges for implementing trust in IoT networks. Moreover, continual updates are needed to accommodate emerging attack vectors, hence increasing the complexity of implementation and maintenance. Trust management systems are vulnerable to collusion and defamation attacks, when malicious devices conspire to artificially inflate their trust ratings. Moreover, they may have sluggish convergence, resulting in prolonged periods during which a device's reputation fails to correctly represent its behaviour, so allowing malicious devices to inflict damage before detection. In identity-based methods, the centralized structure of Public Key Infrastructures (PKI) for digital certificate management may lead to bottlenecks and singular points of failure. Moreover, protecting digital

certificates from various cyber-attacks, such as man-in-the-middle assaults, remains an ongoing worry. Sustaining low latency and energy efficiency when implementing trust management systems may also be challenging. Disadvantages of access control mechanisms include management complexity, bad user experience, and scalability challenges, which may be alleviated by automation, user education, and centralized administration. A significant challenge is maintaining an accurate blacklisting, since IoT devices often alter their states and activities, complicating the effective tracking of hostile entities [8]. Moreover, blacklisting may result in false positives, causing honest devices to be erroneously blocked, thereby disrupting standard operations. The distributed nature of IoT networks challenges the establishment of a centralized blacklist, requiring a distributed methodology that might be resource-demanding and intricate to oversee. Furthermore, banned devices may rejoin the network under new identities, so compromising the efficacy of the blacklist. Robust and adaptive blacklisting methods that integrate real-time monitoring and ML approaches are crucial for improving the dependability and security of IoT networks [9], [10].

Methods for evaluating the trustworthiness of an IoT network include reputation-based, behaviour-based, social networking, fuzzy, routing-based, cooperative, identity-based, and access control methods, which are summarized as follows.

Reputation-based methods assess trust by aggregating historical behavioural data of entities within a network to generate a reputation score, while behaviour-based trust models evaluate trust by persistently monitoring and analysing the current actions and interactions of entities to ascertain their trustworthiness. Reputation-based systems compile ratings and reviews to provide a reputation score for each device, which is then used to inform trust choices.

Behaviour-based methods use advanced algorithms to identify anomalies that may signify malicious behaviour, such as atypical communication patterns or unforeseen data flows. Both methodologies use behavioural data to inform trust evaluations, with reputation systems concentrating on historical activities and behaviour-based methods prioritizing real-time actions. Fuzzy logic may be used to assess trust by considering several criteria, including energy usage, packet delivery ratio, and other performance metrics. This method facilitates a more sophisticated assessment of trust by addressing ambiguity and imprecision.

Social networking methods use social ties and interactions between devices to build trust. They replicate human social trust frameworks, using notions such as friendship and community to assess trustworthiness.

Trust can also be governed by secure routing protocols that include trust metrics in their decision-making processes. These techniques are designed to guarantee safe and dependable data transfer by using reliable pathways.

Identity-based trust mechanisms in IoT networks emphasize the authentication of devices and users to cultivate trust. These techniques generally use digital certificates, biometric authentication, passwords, and other identity verification methods to guarantee that only authorized entities may engage in the network.

Collaborative approaches for trust management in IoT networks include devices cooperating to assess and build trust. These approaches use the aggregated input and interactions of several devices to evaluate the reliability of each node [10].

Access control defines the permissible actions of authenticated entities inside the network, establishing permissions and enforcing policies to guarantee that only approved activities are executed. Common access control strategies used in IoT networks include whitelisting, blacklisting, risk-based access control (RBAC), attribute-based access control (ABAC), and capability-based access control (CapBAC), all of which facilitate the management and security of device interactions inside the network. Whitelisting and blacklisting limit access and guarantee that only trustworthy nodes engage with a network where trustworthy entities are whitelisted and untrustworthy ones are blacklisted. Whitelisting techniques, including application, internet protocol (IP), email, and rule-based whitelisting, are crucial for bolstering security by permitting access only to pre-approved organizations. In IoT networks, blacklisting is often executed by compiling a list of recognized harmful or untrusted devices and setting network security measures to prevent these devices from accessing the network. This necessitates continuous monitoring of network traffic and device activity to identify potential threats. Upon identification of a device as malicious, its unique identifiers, including IP address or Media Access Control (MAC) address, are included in the blacklist. Network security systems, including firewalls and intrusion detection systems, use this blacklist to obstruct and prohibit access to certain devices, hence preventing communication with other devices or access to network resources. Frequent updates to the blacklist are crucial for addressing emerging threats and ensuring network security.

RBAC in IoT networks allocates rights according to the user's organizational role and their designated responsibilities inside the network, guaranteeing users' access only to the resources essential for their job responsibilities. This is often accomplished by defining roles that align with certain access privileges and responsibilities, thereafter, assigning these roles to devices or users. Each role has a defined set of permissions that govern the activities a device or user may execute and the resources they may access. RBAC streamlines access control management by categorizing permissions into roles, hence facilitating the enforcement of security rules and ensuring that only authorized devices or users may execute certain tasks. Consistently upgrading roles and permissions is crucial for adapting to network changes and ensuring security. ABAC enhances access decisions by using diverse variables, including user traits, resource categories, and contextual factors. Policy-based access control (PBAC) employs established policies to regulate access, facilitating more detailed and adaptable control. Just-in-time (JIT) access provides ephemeral access to resources solely when required, hence limiting the danger of extended exposure. CapBAC in IoT networks is a security method that confers access privileges via capabilities, which are unforgeable tokens or access tokens. These tokens delineate the rights conferred to a device or user, enabling access to certain resources or the execution of specified tasks inside the network. CapBAC is especially appropriate for IoT contexts because to its decentralized architecture and capacity to manage the resource limitations of IoT devices. The procedure entails the issuance, transfer, and revocation of capabilities as required, guaranteeing that only authorized organizations may access network resources. This approach diminishes the burdens linked to conventional access control lists and RBAC, making it a streamlined and scalable solution for access management in IoT networks.

2.1.4 Scalability

The network architecture supporting billions of devices, encompassing mobile and diverse nodes, must be scalable, dynamic, and self-organizing to facilitate CI. Scalability challenges in CI-enabled IoT networks are considerable owing to the extensive number of networked devices and the substantial amount of data they produce. As the network proliferates, bandwidth management becomes ever-challenging, often resulting in sluggish connections and bottlenecks. Ensuring a reliable connection among a growing multitude of devices presents a considerable problem, intensified by the diverse communication protocols and standards employed by various IoT devices. The dynamic characteristics of IoT settings, characterized by mobility, changing channel conditions, and constant addition and removal of devices from the network, hinder scaling initiatives. Efficient data management is essential since the immense volume, speed, and diversity of IoT data might be beyond the capabilities of conventional data processing and storage systems. In addition, developing scalable routing protocols and data storage techniques is essential in managing the growing number of devices while enabling effective communication [11]. Scalability challenges in DLT usage in IoT networks are also substantial. DLTs often encounter difficulties in rapidly processing a substantial number of transactions, posing challenges for IoT networks that produce extensive data. The consensus techniques used in DLTs, such as proof-of-work, may be resource-intensive and sluggish, resulting in latency problems. The storage demands for sustaining a distributed ledger might be considerable, presenting difficulties for IoT devices with limited storage capacity. The scaling difficulties need the creation of more efficient consensus algorithms and streamlined DLT solutions specifically designed for IoT networks [5]. Scalability issues concerning the trust management of IoT networks are considerable and necessitate efficient algorithms to handle the extensive volume of trust evaluations and modifications. The wide array of devices and their distinct capabilities complicates scaling since trust management solutions must address varied performance and security needs. Moreover, the need for real-time trust evaluations may impose pressure on network resources, resulting in latency and bandwidth issues. Maintaining continuous and reliable trust assessments inside a constantly growing network requires resilient, scalable infrastructures and inventive methods to protect security and performance [10].

2.1.5 Security

Security issues in CI-enabled IoT networks are complex owing to the multitude of networked devices and the sensitive data they manage. Ensuring robust authentication is crucial to prevent unauthorized access; yet the diversity of devices and their varying capabilities complicates this task. The security of data during transmission and storage is paramount, as IoT networks are vulnerable to cyber threats such as man-in-the-middle attacks, data breaches, and malware. The portability of devices and the fluid characteristics of IoT environments exacerbate these security issues. Moreover, preserving user privacy while facilitating smooth inter-device communication requires advanced encryption and anonymization methods. The absence of established security protocols across various IoT platforms presents a difficulty, requiring the creation of cohesive security frameworks to

provide uniform protection. These challenges underscore the need for ongoing innovation and stringent security protocols to protect IoT networks empowered by CI [3].

Key attack vectors and risks introduced by the interconnectedness of IoT devices include:

- Insecure Interfaces: Weak authentication and authorization in IoT device interfaces can be exploited by attackers.
- Data Privacy Breaches: IoT devices frequently gather sensitive information, rendering them susceptible to cybercriminal targeting.
- Botnets: IoT devices can be hijacked to form botnets that launch large-scale attacks like distributed denial of service (DDoS).
- Physical Attacks: Many IoT devices are deployed in unsecured locations, making them susceptible to physical tampering.

Mitigation strategies include:

- Strong Authentication: Implement robust authentication mechanisms for IoT device interfaces.
- Data Encryption: Encrypt data both in storage and during transmission to safeguard it against illegal access.
- IoT Device Management: Regularly update device firmware and monitor for unusual behaviour to prevent hijacking.
- Physical Security: Deploy IoT devices in secure locations and use tamper-evident seals to deter physical attacks.

2.1.6 Resilience

Resilience is the ability to endure operations and promptly respond to incidents, including hardware malfunctions, network congestion, or cyber-attacks. IoT networks encounter significant hurdles stemming from their decentralized nature and the number of connected devices. Overseeing interdependencies across many tiers, including edge and cloud, may lead to connectivity disruptions and reduced performance. The dynamic nature of IoT settings affects the maintenance of consistent and reliable performance. The diversity of IoT devices hinders the implementation of standardized resilience solutions. Security threats, such as physical tampering and cyber-attacks, intensify resilience issues, requiring continuous monitoring and proactive defensive strategies. Moreover, IoT systems often traverse many administrative domains, each possessing unique resilience requirements and possible single points of failure, hence complicating coordination and increasing the risk of disruptions. These challenges highlight the need for strong protocols to guarantee the stability of IoT networks enhanced by CI. Effective resilience plans must consider the scalability of the network, ensuring that resilience measures can be maintained as the network grows [12].

2.1.7 Software Implementation and Configuration Issues

Software implementation and configuration in IoT networks encounter numerous challenges, including compatibility, update management, and resource limitations. Compatibility concerns arise from the variability of operating systems and software environments across different devices. Managing upgrades is intricate due to the varied and sometimes remote locations of IoT devices, complicating the verification that all devices are functioning on current software versions. Resource constraints, such as limited processing power and memory, might hinder the functionality of IoT applications. Employing containerization and virtualization technologies enhances compatibility, implementing over-the-air (OTA) updates streamlines update management, and optimizing software for optimal performance on low-resource devices mitigates resource constraints.

2.1.8 Example Threat Scenario

We will now examine these challenges via a hypothetical APT scenario depicted in Figure 2 and consider resolving the architectural issues to safeguard IoT networks. APT attacks are long-term intrusions into networks that covertly monitor and acquire data over extended periods without detection rather than inflicting immediate harm to the network. This makes them elusive and difficult to identify. The multi-phase nature of these attacks, including penetration, dissemination, and data extraction, makes them challenging to identify using conventional security methods. Malicious entities frequently employ sophisticated techniques that emulate standard network behaviours, rendering their activity ostensibly lawful.

An APT attack may involve the following stages [13]:

- Reconnaissance: The attacker collects information about the target IoT network, pinpointing susceptible devices and access points. This may include probing for unprotected ports, vulnerable passwords, or obsolete firmware.
- Initial Compromise: The attacker leverages a vulnerability in an IoT device to get initial access. This may occur via a phishing email that deceives a user into downloading malware or by using a known software vulnerability. Upon gaining entry, the attacker installs malware on the infiltrated device to ensure continued access. This virus often incorporates backdoors or rootkits that enable the attacker to control the device.
- Lateral Movement: The attacker navigates laterally throughout the network, infiltrating more IoT devices and systems. This is performed to get wider access and to identify important data or essential systems. Methods such as social engineering and exploiting computer vulnerabilities are typically used.
- Pivoting: The attacker contacts a remote server to get directives and transmit stolen information. This correspondence is often encrypted to prevent discovery. Techniques such as pass-the-hash, pass-the-ticket, and remote desktop protocol are frequently employed for this objective.
- Data Exfiltration: The attacker gathers and removes sensitive information from the IoT network. This may include personal information, intellectual property, or other critical data. To avoid detection by intrusion detection systems and antivirus software, attackers frequently employ programs that segment data prior to transmission. Proficient hackers distribute the segmented components to several Domain Name System (DNS) servers and subsequently aggregate the fragmented files to diminish the likelihood of detection.
- Post Stage: The attacker secures sustained access to the network by installing supplementary backdoors or establishing new user accounts. This enables their return even if the original breach is identified and rectified. The perpetrator obscures their acts to evade detection. This may include the deletion of logs, the use of anti-forensic tools, or the alteration of system files to obscure their existence.

Common mitigating strategies for APTs include routine security audits, multi-factor authentication (MFA), network segmentation, and ongoing surveillance for anomalous behaviours. Traditional APT mitigation strategies mostly emphasize direct defensive measures; however, continuous integration and access control techniques enhance security through fostering collaboration and meticulously limiting access, respectively. In this example, CI may be used to detect and address the attack by:

- Sharing indicators of compromise, including strategies, methods, and processes within a network of trustworthy companies, facilitates early detection of active attack vectors. The gathered data help identification of anomalies that may otherwise remain undetected.
- Using ML methods, including FL, to analyse data from several sources to identify patterns that may signify harmful behaviour. Minor fluctuations in network traffic or atypical access to critical data may be identified and examined.
- As additional data is collected and analysed, the CI system continuously improves its understanding and detection abilities. Feedback from each identified occurrence enhances the systems' capacity to anticipate and alleviate future hazards.
- Upon detection of a potential APT, collaborative response tactics can be formulated and disseminated throughout the collective network. This approach not only contains the threat more efficiently but also ensures that preventive measures are widely disseminated, thus strengthening the defensive posture of all participants.

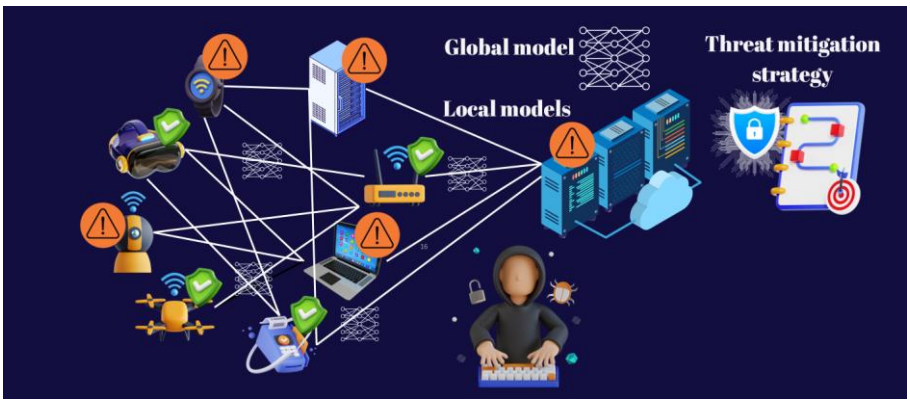

Figure 2. Example threat scenario

Trust management solutions are essential for thwarting APT assaults in IoT networks by persistently assessing and monitoring device trustworthiness, therefore identifying and alleviating dangerous behaviours before compromising the network. These technologies enhance security by allowing communication and data sharing exclusively among trusted devices within the network. By limiting access to critical resources solely to authorized users, organizations can impede lateral movement inside the network, a common tactic in APT attacks. When integrated with CI, which utilizes shared information and coordinated defensive techniques, this becomes considerably more effective. This collaboration facilitates a more dynamic and informed security strategy, enabling ongoing refinement of access controls based on the most recent threat information and collaborative insights.

However, access of clients into IoT networks, both with and without backbone connections, poses several issues as follows:

Client integration with backbone connection: In this scenario, a client (Client A) accesses an IoT network with a backbone connection. This process typically consists of the following steps in a CI-enabled IoT network with a cloud-based architecture:

1. Client A requests to connect to a registered neighbouring IoT client B.
2. Client B checks whether the IoT client A is blacklisted or registered to the IoT network.
    a. If client A is blacklisted, client B terminates the connection.
    b. If client A is already registered, client B connects and interacts with it.
    c. If client A is neither blacklisted nor registered to the IoT network, client B forwards the request to the cloud service provider via the router.
3. After receiving the registration request from the registered client B, the cloud service provider initiates the registration process of client A. Firstly it performs a blacklist and registration check.
    a. If client A is neither blacklisted nor registered, it then performs a whitelist check.
    b. If client A passes the device whitelist check, it adds client A to the IoT network by assigning a public key pair and updating the device registry.
4. The cloud service provider shares the key pair with client A and completes the registration process. After registration is completed, the IoT client A can access the IoT network.

Client integration without backbone connection: As client A accesses the IoT network without a backbone connection,

- Client A requests to connect to a registered neighboring IoT client B.
- Client B checks whether the IoT client A is blacklisted or registered to the IoT network against its local blacklist.
    - If the client A is blacklisted, client B terminates the connection.
    - If client A is already registered, client B connects and interacts with it.
    - If client A is neither blacklisted nor registered to the IoT network, it should ‘deserve’ or ‘prove’ its reliability before registering to the network.

In both scenarios, in addition to whitelisting and blacklisting related issues discussed previously, upon successfully infiltrating the network, a malicious client may use a covert strategy by staying dormant and refraining from any activities that may expose its existence. This unobtrusive characteristic allows it to blend with genuine network traffic, so confounding detection. During this period of inactivity, the malicious client could gain vital information on the network's architecture and security protocols. It could initiate a variety of attacks at the appropriate time. For example, it may conduct eavesdropping, intercepting, and monitoring conversations to get sensitive information. It may also launch a man-in-the-middle attack, interposing itself between two interacting entities to modify or expropriate information covertly. The malicious client may as well launch DoS attacks, bombarding network resources to impair services and induce substantial downtime. Moreover, the attacker may use complex methods to sustain a prolonged presence inside the network for an APT attack, engaging in espionage, data exfiltration, and evading detection for longer durations. These strategies emphasize the need for ongoing surveillance and stringent security protocols to identify and alleviate such dangers.

2.2 Architectural Issues in OT Environments

OT are ecosystems that utilize device, edge, and cloud computing capabilities, similarly to the IoT case but with a clear focus on controlling physical industrial processes.

Key Attack Vectors and Risks:

- Unauthorized Access: Attackers can gain control of OT systems through unsecured remote access points or credentials.
- Supply Chain Attacks: Compromising third-party vendors that have access to OT systems can introduce vulnerabilities.
- Denial of Service (DoS): Attacks that flood OT systems with traffic can disrupt critical industrial processes.
- IoT Devices: Inadequately secured IoT devices integrated into OT systems (or IoT capabilities integrated to OT devices) can serve as entry points for attackers.
- IT Devices: Insufficiently secured IT devices incorporated into OT system monitoring or management can directly introduce IT-specific risks that impact OT devices or production.

Mitigation Strategies include:

- Secure Remote Access: Implement MFA and VPNs for remote access to OT systems.
- Vendor Management: Conduct thorough security assessments of third-party vendors and enforce stringent security policies.
- Network Segmentation: Segment OT networks to isolate critical systems and limit the impact of DoS attacks.

3 Solutions for Efficient Cyber Risk Management

3.1 Frameworks for Cyber Risk Management

3.1.1 Zero Trust Architecture

The Mint Security Threat Report highlights the necessity of adopting the **Zero-Trust Architecture (ZTA)** (NIST 800-207) to ensure digital sovereignty and secure operations in mission-critical environments. According to ENISA (2017), the fragmented and slow implementation of IoT security standards and legislation constitutes significant barriers to the secure deployment of IoT. The Zero Trust (ZT) paradigm operates on the principle that no entity, inside or outside the network, should be trusted by default. Verification is required from everyone attempting to access resources. Implementing ZT involves continuous monitoring, strict access controls, and ensuring that devices and users are authenticated and authorized. Fundamental concepts of ZT include providing users and devices with the minimum access needed to perform a task, segmenting the network into smaller, secure zones to restrict threat mobility, and implementing several MFAs, and verification (see Figure 3) [14].

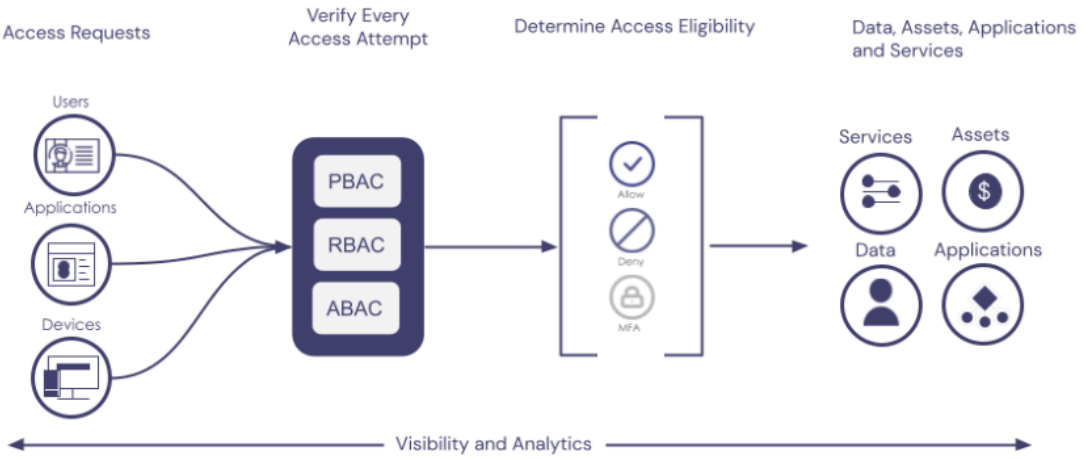

Figure 3. High-level ZTA *[15]*

ZTA is an essential security architecture that mitigates the risks associated with the increasing proliferation of connected devices in IoT networks. Conventional network security approaches often regard devices inside the perimeter as inherently trustworthy. This presents vulnerabilities when interacting with untrusted or possibly hacked IoT devices. ZTA aims to bolster security by presuming that attacks may originate from internal and external sources [16], [17].

The NIST outlines seven fundamental principles to facilitate the effective realization of ZTA [14]:

1. Resource: Refers to any data source or computational service.
2. Communication Security: Communication is safeguarded regardless of location.
3. Session Security: Access to resources is allocated on an individual session basis, and authentication and authorization for one resource do not confer rights to others.
4. Access Control: Resource access is governed by a dynamic policy that considers the observable state of client identification, application, and requested assets.
5. Minimum-Security Posture: The enterprise guarantees that all owned and affiliated equipment is maintained in the most secure condition and continuously monitors assets to uphold this standard.
6. Continuous Authentication: All resource authentication and authorization are dynamically and rigorously enforced. An organization seeking to use ZTA may possess an Identity, Credential, and Access Management system along with MFA to enhance security. Ongoing monitoring during user engagement, coupled with the potential for seamless re-authentication and authorization, may prove beneficial.

7. Information Logging: The organization gathers extensive data regarding the present condition of the network infrastructure and communications, utilizing this data to enhance its security posture.

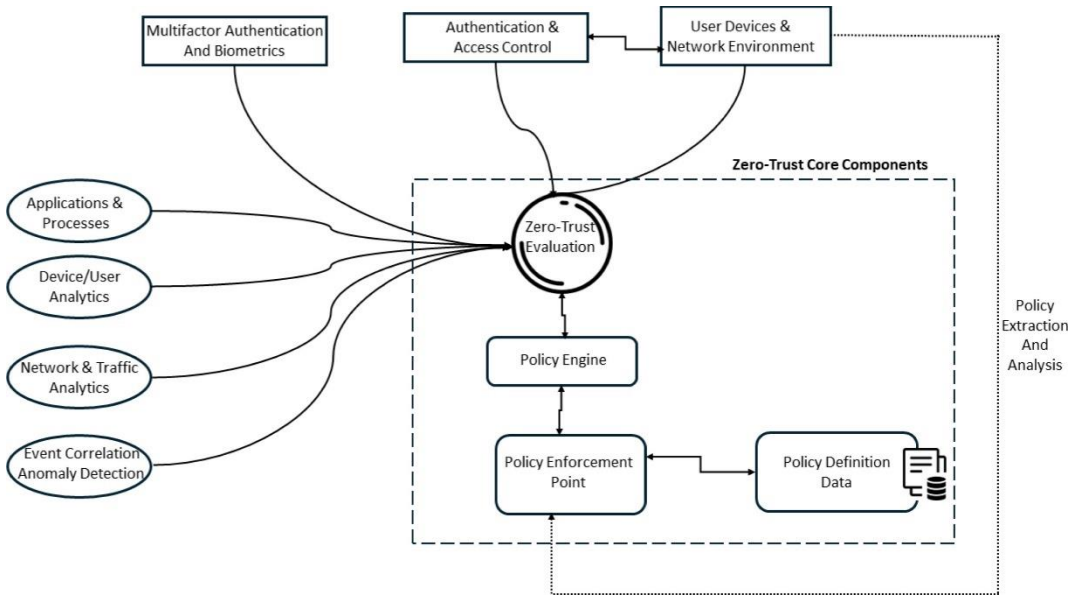

Figure 4. Key elements of ZTA *[18]*

The use of ZTA for CI allows secure and verified information exchange while ensuring internal security, visibility and collaborative efforts within a framework of stringent oversight. Key elements of ZTA include the following (see Figure 4) [18]:

- Policy Engine: Determines access decisions utilizing policies, regulations, and trust scores.
- Policy Administrator: Implements the determinations established by the Policy Engine.
- Policy Enforcement Point: Regulates access to resources following the determinations made by the Policy Engine and Policy Administrator.
- Identity, Credential, and Access Management: Oversees user identities and access rights, perpetually evaluating trustworthiness. This guarantees that only authorized individuals can access designated resources by limiting access to a need-to-know basis and confirming the identity of users and devices (see Section 3.5.1).
- Endpoint Security: Guarantees that devices connecting to the network are secure and adhere to security protocols.
- Data Security: Safeguards data using encryption and additional security protocols.
- Resource Protection: Preserves essential resources and infrastructure.
- Trust Scoring: Continuously assesses and allocates trust levels to users and devices depending on their behaviour and contextual factors, hence dynamically modifying access rights (see Section 3.3).
- Threat Intelligence: Gathers and examines data regarding prospective threats to guide security decisions and strengthen defences (see Section 3.6).
- Anomaly Detection and Monitoring: Detects atypical patterns or behaviours that may signify security incidents or breaches, and continuously oversees security data, facilitating the identification of anomalous behaviours and the swift reaction to incidents and dynamically modifying trust levels (see Section 3.4).
- Security Automation and Orchestration: Automates security operations and synchronizes responses to attacks, using anomaly detection and monitoring to enhance efficiency and efficacy.

Authentication: ZTA uses sophisticated authentication mechanisms such as biometric, MFA, behavioural, risk-based, certificate-based, single sign-on (SSO), contextual, and device authentication to bolster security.

- **Biometric authentication** employs distinctive biological characteristics such as fingerprints, facial recognition, or iris scans for identity verification.
- **MFA** generally encompasses a mixture of knowledge-based elements (such as a password), possession-based elements (such as a smartphone or hardware token), and biometric elements (such as a fingerprint or face recognition).
- **Behavioural authentication** examines user behaviour patterns, such as typing speed and mouse movements, to identify anomalies.
- **Risk-based authentication (RBA)** is a flexible security mechanism that modifies authentication criteria according to the evaluated risk level of a login attempt. It assesses multiple parameters like the user's geographical location, device category, access time, and behavioural habits. Should an attempt be classified as high-risk, such as an atypical login location or time, supplementary authentication measures, like MFA, may be necessitated. In contrast, low-risk endeavours may encounter fewer obstacles. This method maintains an equilibrium between security and user experience, bolstering defences against unwanted access while reducing interruptions for legitimate users.
- **Certificate-based authentication** utilizes digital certificates to verify the identification of users and devices.
- **SSO** enables users to authenticate a single time to access numerous applications, enhancing ease while preserving security.
- **Contextual authentication** evaluates variables such as location, device type, and access time to adapt authentication criteria dynamically.
- **Device authentication** guarantees that only authorized devices can access the network by validating device identity using mechanisms such as device certificates, hardware tokens, or device posture evaluations. Device posture evaluations guarantee that only secure and compliant devices can access the network. This procedure entails evaluating the security condition and configuration of a device before access authorization, encompassing elements such as operating system and software updates, antivirus and anti-malware status, encryption, adherence to security regulations, device health, and configuration settings. Furthermore, it employs whitelisting and blacklisting to permit only authorized devices and to obstruct recognized compromised ones.

The requirements for whitelisting often include elements such as the device's manufacturer, firmware version, security features, and historical network behaviour. Blacklisting criteria may include the identification of devices exhibiting known vulnerabilities, old firmware, or anomalous activity patterns, hence preventing potentially compromised devices from accessing the network. Continuous monitoring and assessment of these criteria facilitate device posture evaluations, ensuring that only trustworthy and compliant devices access sensitive resources, hence augmenting the overall security posture.

Implementing sophisticated authentication mechanisms in IoT networks has numerous obstacles, including constrained device resources, heterogeneous device kinds, and scalability concerns. Biometric and behavioural authentication may be limited by the processing capabilities and memory of IoT devices. Certificate-based and MFA can provide challenges in standardization across diverse devices and protocols. RBA and contextual authentication necessitate ongoing monitoring and data processing, potentially overburdening network resources. To mitigate these issues, lightweight authentication protocols and security agents can be designed to align with the capabilities of IoT devices. Standardizing security frameworks and implementing uniform protocols helps guarantee consistent implementation across many devices. Moreover, utilizing edge computing helps alleviate demanding processing duties, hence improving the viability of various authentication approaches in IoT networks. Automated tools and orchestration platforms facilitate scalability management, enabling strong and efficient authentication procedures [19].

Access control: As we already outlined about trust management, access control mechanisms, such as RBAC, ABAC, PBAC, and JIT, are crucial in ZTA for guaranteeing that only authorized users and devices can access designated resources. Furthermore, least privilege access guarantees that users and devices possess only the essential level of access required to execute their functions, hence reducing potential attack vectors. The integration of these methods with ongoing monitoring and real-

time modifications establishes a resilient access control framework within ZTA, therefore augmenting overall security.

Implementing access control techniques such as RBAC, ABAC, PBAC, JIT access, and least privilege access in IoT networks poses numerous issues because of the heterogeneity and resource limitations of IoT devices. These devices frequently possess constrained processing capabilities and memory, hindering the implementation of complex access control policies. The vast quantity of devices may result in scalability challenges, and the absence of standardization among various IoT platforms hinders uniform policy enforcement. To mitigate these issues, lightweight access control protocols specifically designed for IoT devices can be created, guaranteeing effective policy enforcement without taxing device resources excessively. Standardizing security frameworks and implementing uniform protocols can enable consistent access control across many devices. Automated tools and orchestration platforms can be used to facilitate scalability management, while edge computing can be used to alleviate processing chores, hence improving the viability of access control systems in IoT networks [16].

Micro-segmentation is a security methodology that partitions a network into smaller, isolated segments or zones, each governed by distinct security standards. In ZTA, micro-segmentation fortifies security by constraining the lateral movement of threats within the network. Establishing detailed security protocols for each segment ensures that, even if an attacker breaches one segment, they cannot easily infiltrate other parts of the network. This containment method minimizes the attack surface and safeguards critical data and resources, rendering it an essential element of a robust ZTA [14].

However, implementing micro-segmentation in IoT networks poses numerous obstacles. IoT devices frequently possess constrained processing capabilities and memory, complicating the implementation and management of intricate security measures. The vast quantity of IoT devices may result in scalability challenges, as each item requires specific segmentation and monitoring. The heterogeneity of IoT devices, characterized by disparate operating systems and communication protocols, exacerbates the challenge of implementing uniform security measures. Resolving the practical issues in micro-segmentation in IoT networks necessitates a multifaceted approach. To accommodate the restricted processing power and memory of IoT devices, lightweight security agents and protocols should be employed, ensuring that segmentation policies do not exceed device capabilities. Scalability challenges can be addressed by utilizing automated tools and orchestration platforms that facilitate the deployment and maintenance of micro-segmentation among numerous devices. Uniformity in security measures across various IoT devices can be attained by implementing standardized frameworks and protocols, hence enabling consistent policy enforcement. Furthermore, utilizing edge computing can transfer processing workloads from IoT devices to more proficient edge nodes, hence improving performance and security. By employing these solutions, enterprises can successfully address the issues of micro-segmentation and ensure strong security for their IoT networks [15].

Micro-segmentation can be utilized for CI and collective defense to provide comprehensive insights into network traffic and device behavior. By observing segmented areas, security systems can collectively identify irregularities and prospective threats with more efficacy. This information can be distributed throughout the network to enhance threat detection and reaction times, so establishing a more robust defense system. Moreover, micro-segmentation facilitates customized security policies for various device kinds and usage contexts, hence improving the overall security stance of the IoT network.

3.1.2 NIST 2.0

Netox research concentrates on the consolidation of **IoT, IT, OT, and cloud-based threat intelligence** to improve comprehensive situational awareness and mitigation strategies. Cyber-risk management was researched with logical separation into strategic-, tactical-, and operative purposes. While all three domains have specific needs and audiences, a common framework for information security management is highly recommended [20], [21].

The **NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) 2.0** [20], an evolution of its predecessor, provides a robust, comprehensive, and flexible foundation for managing cyber risks across IT, OT and IoT environments. The NIST CSF 2.0 is designed to help organizations understand, manage, and reduce their cybersecurity risks. This holistic approach not only mitigates risks but also enhances the overall security posture, ensuring the continuity and reliability of critical operations. By integrating the framework's core functions, Identify, Protect, Detect, Respond, and Recover, with the NIST 2.0 framework, organizations can create a resilient and secure infrastructure and enhance their cyber-risk management strategies, ensuring

comprehensive protection across all facets of their digital and operational landscapes. Each function encompasses a range of activities and processes that collectively aim to secure an organization's data and operations:

- Identify: Understanding the context, resources, and risks that could affect the security of the organization's operations.
- Protect: Implementing safeguards to ensure the delivery of critical infrastructure services.
- Detect: Developing and implementing activities to identify the occurrence of a cybersecurity event.
- Respond: Taking action regarding a detected cybersecurity incident.
- Recover: Maintaining plans for resilience and restoring any capabilities or services impaired due to a cybersecurity incident.

3.2 Artificial Intelligence and Machine Learning

AI and ML offer promising solutions for enhancing cyber risk management. These technologies can analyse vast amounts of data to identify patterns and predict potential threats. AI-driven security systems can adapt to new threats in real-time, providing proactive defence mechanisms.

AI can be used to process extensive data produced by aggregated inputs, which provide insight into threats, to make or support informed decisions using predictive analytics, anomaly detection (see also Section 3.4 below), pattern recognition, clustering, natural language processing, and other approaches.

Important types of distributed ML (Hierarchical ML and Federated Learning) and risks that the use of ML can bring (such as model poisoning and model evasion) are discussed in Section 3.1.1 of CISSAN deliverable D1.1. Cybersecurity applications of generative AI are discussed in Section 3.5 of D1.1.

3.3 Trust Scoring

Assessing trust in IoT/IT/OT networks is essential because of the ubiquitous and interconnected characteristics of these systems, which frequently manage sensitive information and execute vital operations. Trust evaluation guarantees the dependability, security, and integrity of devices and their data exchanges, thereby limiting risks including unauthorized access, data breaches, and harmful assaults. With the growing integration of IoT devices across diverse sectors such as healthcare, transportation, and smart homes, establishing trust is crucial for sustaining user confidence, ensuring adherence to regulatory standards, and safeguarding against potential vulnerabilities that could jeopardize the entire network. Consequently, a comprehensive trust evaluation methodology is essential to ensure the operation and security of IoT ecosystems. A metric such as 'trust score' may be defined to provide a numerical representation of the level of trust hence the credibility and trustworthiness associated with entities inside an IoT network, such as IoT devices or users. A trust metric can also be defined to assess a network's overall trust level.

An essential requirement for fostering trust in IoT/IT/OT devices is remote attestation, a security mechanism that authenticates the existing condition of possibly hacked devices. Attestation techniques include hardware-based solutions such as Trusted Platform Modules, which offer robust security assurances but are more appropriate for high-end systems due to their complexity and power demands. Software-based techniques, such as Control Flow Integrity, ensure that a program's execution flow adheres to a predetermined path, identifying deviations induced by malware. These provide limited security assurances and are vulnerable to specific assaults. Hybrid methodologies, such as Physical Unclonable Functions (PUFs), integrate hardware and software characteristics to generate distinctive, device-specific reactions to stimuli, so augmenting security while remaining suitable for resource-limited systems [22]. PUFs are hardware security techniques that leverage the intrinsic physical variances in integrated circuits (ICs) to produce unique, device-specific responses to specified inputs. These variances occur inherently during the manufacturing process, rendering each PUF distinctive and challenging to imitate or duplicate. PUFs operate analogously to human biometrics, offering a distinctive identity for each silicon unit. PUFs can augment device authentication and facilitate secure key creation. Each PUF is unique, enabling it to produce a specific answer to a challenge, which can be utilized to authenticate the device's identification. This renders it exceedingly challenging for adversaries to counterfeit or replicate the device's identification. Furthermore, PUFs may produce cryptographic keys dynamically, so obviating the

necessity to keep sensitive keys in non-volatile memory, which is susceptible to physical attacks. Integrating PUFs enables IoT devices to get enhanced security, guaranteeing that only authenticated devices can access the network and interact safely [23].

However, defining trust inside a ZT network is particularly difficult due to adaptive baselines, as changing patterns of “normal” behaviour complicate differentiating legitimate activities from malicious ones [24], [25].

Trust metrics can be computed for individual devices and the entire network by assessing the aggregated behaviour of all nodes. This entails evaluating elements such as behavioural consistency, contextual adherence (e.g., geolocation and access time patterns), compliance with security protocols, historical trust metrics, and anomaly detection outcomes. The network undergoes analysis of aggregated parameters such as overall traffic patterns, inter-device communication consistency, and anomaly density. Individual and network-wide metrics are weighted and amalgamated using ensemble ML or risk-scoring algorithms to provide a composite trust score. If several devices display associated departures from the baseline, such as intermittent unlawful requests, this may decrease the network's trust score, resulting in network-wide limits or enhanced surveillance. The optimal strategy in this case is to implement hierarchical trust models, wherein device-level trust scores contribute to a superior network trust assessment. Dynamic adaptation rates must be meticulously regulated to avert the integration of harmful activities into baselines and highlighted abnormalities should be omitted. Time-decay functions prioritize recency, whereas feedback mechanisms incrementally improve trust metrics. This system can dynamically evaluate and enforce trust at device and network levels by integrating individual and aggregated data with sophisticated algorithms.

Trust scores can be calculated by analysing a wide range of data points, including device type, shared secrets, data traffic, device behaviour, historical data, validity of certificates, identification of suspicious activity, etc. These scores may be used to determine whether to allow or restrict access, flag threats, or prompt users with warnings about potentially malicious entities. Trust scores can be automatically updated based on the latest data and activities. Choosing data points for trust scoring in a ZTA with dynamic baselines necessitates the selection of metrics that accurately assess the reliability of devices, users, and the network while accommodating changing surroundings. Essential device-level metrics encompass behavioural consistency (e.g., activity patterns, departures from baselines), compliance (e.g., patch levels, encryption standards), anomaly scores, and contextual elements such as location and connection type. User-level data metrics encompass authentication robustness, access behaviours, and behavioural biometrics. Trust scoring at the network level depends on traffic patterns, inter-device interactions, and anomaly density, while historical metrics such as incident history and external reputation scores provide further context. The data points must be weighted and prioritized according to relevance, with context-sensitive thresholds implemented to align with the network's specific needs. For example, a smart city IoT network may identify trust difficulties if a temperature sensor displays anomalous data spikes associated with irregular traffic among linked devices, exacerbated by contextual anomalies such as off-peak activity or unexpected IP addresses.

The integration of real-time data and feedback loops guarantees the efficacy of selected measures, facilitating precise and adaptable trust scoring that harmonizes flexibility and security in complex, evolving contexts. Elements essential for establishing appropriate intervals for trust score updates include [26]:

- Data Freshness: Trust updates must consider the timeliness of observed data to ensure relevancy. Obsolete data is allocated diminished weights or discarded if too antiquated.
- Network Dynamics: The system adjusts to the mobility patterns and communication behaviours of nodes, ensuring that trust scores accurately represent real-time interactions and environmental fluctuations.
- Trust Decay and Reinforcement: It is essential to analyse the implementation of decay functions to reduce trust ratings over time in the absence of interactions, offset by reinforcement mechanisms when positive behaviours are observed.
- Computational Overhead: It is essential to balance the frequency of trust score updates with processing power and energy usage in resource-limited mobile networks to ensure system efficiency.
- Risk Sensitivity: In high-risk contexts, such as during attacks or major network anomalies, more frequent updates are necessary compared to steady, low-risk situations.

- Trust Aggregation and Propagation: Models are required to aggregate individual trust evaluations into composite scores and distribute trust information across the network, hence assuring uniformity in trust assessment.

Adaptive and context-sensitive trust management improves the reliability and responsiveness of mobile networks, establishing a basis for developing systems where trust is a fundamental operational component. Based on the above criteria, an optimal update frequency can be determined to ensure that trust scores reflect an accurate and precise assessment of the latest information and behaviours.

3.4 Anomaly Detection and Monitoring

Anomaly detection in IoT/IT/OT networks is essential for recognizing atypical or suspicious behaviours that may signify possible security concerns. Anomaly detection identifies deviations from established patterns by continuously analysing user and device behaviour, facilitating timely reactions to suspected breaches. This procedure operates concurrently with trust scoring, which evaluates the risk level of people and devices based on their behaviour and context, dynamically modifying access rights as needed. Monitoring offers immediate insight into network activity by providing comprehensive insights into impacted devices and network segments, facilitating prompt investigation and remediation. Furthermore, utilizing ML algorithms can enhance the precision of anomaly detection by analysing past data and adjusting to emerging hazards.

Anomaly detection and monitoring may be decentralized throughout the nodes of an IoT network. This entails the implementation of detection algorithms across several nodes and devices to collaboratively discover and address security issues. This method utilizes the decentralized characteristics of IoT networks, wherein each device or node enhances overall security by observing local activity and disseminating information. Through local data analysis, devices can identify abnormalities in real-time, including atypical traffic patterns or unforeseen behaviours. The local detections are subsequently consolidated and processed in a centralized or decentralized way to create a thorough assessment of the network's security posture using a mechanism like FL. ML algorithms can optimize this process by analysing aggregated data, thus enhancing the precision of anomaly detection progressively. Moreover, distributed monitoring guarantees that if a single node is hacked, the remainder of the network can persist in operation and counteract threats, hence augmenting the resilience and robustness of the IoT network. This facilitates the rapid identification of pervasive dangers and the formulation of more effective defence tactics.

However, identifying attacks in IoT networks is complex due to the difficulty in defining "normal" behaviour from "abnormal" behaviour, particularly when malevolent entities replicate legitimate behaviours or utilize nuanced methods to avoid detection. Attackers leverage this constraint through diverse tactics, including masquerade and mimicry attacks, when they impersonate legal nodes or modify their actions to imitate regular patterns. Subtle resource exhaustion attacks, such as low-rate DoS or battery-draining tactics, diminish performance without producing conspicuous anomalies. Routing and protocol exploitation attacks, including sinkhole, Sybil, and wormhole attacks, alter network behaviour by introducing nuanced interruptions. Additional covert methods encompass data replay or injection that seems authentic, passive eavesdropping to acquire information, and coordination among infected nodes to deliver deceptive yet credible data. Advanced threats such as sluggish reconnaissance, side-channel attacks, or concealed backdoors exacerbate detection challenges by functioning with minimal disruption. Confronting these difficulties necessitates a multifaceted strategy. One method that could be employed is signature-based detection, which identifies threats by comparing incoming data with a repository of established attack patterns or signatures, thereby successfully recognizing and preventing previously recorded threats. Another method that could be used is context-aware security, which employs metadata, including user behaviour, device state, and environmental elements, to improve real-time security decisions, yielding more precise and adaptive protection.

Establishing normal behaviour in IoT environments requires adaptive baselines, integration of domain expertise, and utilization of ML models trained on extensive datasets to discern subtle patterns suggestive of malicious conduct. An adaptive baseline is a dynamic approach for defining "normal" behaviour in a system by perpetually learning and updating the standards for typical activity patterns. In contrast to static baselines that depend on immutable thresholds, adaptive baselines progress over time to accommodate variations in IoT network behaviour, such as traffic fluctuations, usage patterns, and environmental variables, rendering them especially effective in dynamic IoT settings. The process includes an initial training step in which the system is taught based on historical

data to establish a baseline model of normal activity, incorporating traffic patterns, device interactions, and sensor readings. Throughout continuous monitoring, the system collects real-time data and intermittently refreshes the baseline utilizing statistical models, ML algorithms, or alternative dynamic techniques such as adaptive threshold tuning [27]. Anomalies are identified when deviations from the dynamic baseline beyond a predetermined threshold, considering both short-term fluctuations and long-term patterns. A feedback loop subsequently assesses observed abnormalities to differentiate between authorized actions, such as the incorporation of a new device, and potential threats, resulting in further refinement of the baseline.

Consider a smart home network consisting of an anomaly detection system with an adaptive baseline that analyses traffic from devices, including cameras, thermostats, and intelligent lighting systems. The network gradually acquires knowledge about standard patterns, such as cameras being utilized during daylight, lights being activated in the evening, and thermostats modifying temperatures throughout operational hours. The system monitors fluctuations over time, including seasonal alterations in thermostat utilization and the addition of a new camera. An adaptive baseline accommodates these fluctuations by continually revising the "normal" patterns. Consider an attacker executing a low-rate DoS attack by transmitting marginally elevated but intermittent requests to the thermostat to deplete its battery. A static baseline may overlook these nuanced alterations as they remain within predetermined thresholds. However, an adaptive baseline detects that the frequency and timing of requests consistently diverge from anticipated patterns, marking it as anomalous. Similarly, in the event of a replay attack, wherein an attacker retransmits intercepted unlock signals to a smart lock, the system identifies the anomaly due to a discrepancy between the anticipated context (e.g., absence of user activity) and the reiterated, contextually inappropriate order. By associating this with the inactivity of other devices (e.g., inactive lights or cameras), the system verifies the anomaly and issues an alarm. The system subsequently notifies administrators or autonomously implements measures to alleviate the hazard. Anomalous activity can thus be effectively discovered in dynamic and complex IoT contexts by utilizing a combination of statistical approaches, ML, and context-aware analysis.

Advantages of adaptive baselines include resilience to developing threats, hence reducing false positives and enhancing detection precision for nuanced attacks. Challenges include ongoing learning, which can be resource-demanding, and inadequately calibrated systems may adjust excessively, integrating harmful activities into the baseline and diminishing detection efficacy. To augment the efficacy, enhance the precision, and minimize the bias in the validation of anomalies of adaptive baselines, systems may incorporate context-aware security (e.g., accounting for temporal factors, device classification, or user behaviour), utilize AI methods such as Large Language Models (LLMs) [28], ensemble ML techniques [29] and implement human-in-the-loop methodologies [30]. The combined use of these methods guarantees that adaptive baselines are reactive and resilient to evasion strategies.

Detecting abnormal behaviour in IoT networks using adaptive baselines entails recognizing deviations from dynamically learned patterns of normalcy while reducing false positives and false negatives. This procedure utilizes a blend of techniques customized for the distinct attributes of IoT contexts, including dispersed systems, resource limitations, and diverse device behaviours. Anomaly detection methods in IoT networks include diverse strategies to recognize deviations from standard behaviour. Statistical techniques, such as moving averages and time-series analysis, monitor departures from anticipated trends, e.g., atypical temperature fluctuations in a thermostat. ML algorithms encompass supervised learning utilizing classifiers (e.g., Random Forest, SVM) for labelled datasets, unsupervised learning employing clustering techniques (e.g., K-Means, DBSCAN) for outlier detection in unlabelled datasets, and semi-supervised learning that integrates labelled normal behaviour with extensive unlabelled data. Temporal and contextual analysis assesses behaviour about time-sensitive patterns and device-specific norms, such as the operation of a smart lock during atypical hours. Ensemble approaches amalgamate many models to improve detection precision and fortify against evasion, whereas correlation and dependency monitoring detect anomalous alterations in inter-device interactions, such as a thermostat modifying temperature absent a matching user directive.

Challenges in anomaly detection may be due to noisy data in IoT environments, and random signal fluctuations or sensor errors. Another challenge is subtle anomalies; sophisticated attacks, such as data injection or low-rate DoS, produce minimum aberrations that are difficult to identify. Adaptive attacks also pose a significant challenge, where malicious actors might modify their conduct in reaction to detection systems, progressively circumventing anomaly detection measures. These problems can be mitigated by threshold optimization, feature engineering, and feedback and refinement. Threshold optimization dynamically modifies thresholds according to confidence levels and historical trends to minimize false positives and negatives. Feature engineering entails extracting

critical attributes such as traffic volume, device usage patterns, and temporal factors to augment the model's capacity to distinguish between normal and anomalous behaviour. Feedback and refinement integrate a feedback mechanism that enables the system to learn from errors and enhances its detection proficiency over time [27].

3.5 Distributed Ledger Technology

Existing security solutions for IoT/IT/OT networks with centralized architectures have several drawbacks, including a single point of failure, high costs for transmission and computing, and data loss. In addition, given that multiple devices may be associated with each user, IoT/IT/OT systems need to guarantee that data ownership is maintained. This will allow users to have full control over the shared data. There may be extra security vulnerabilities associated with the IoT/IT/OT since it uses open standards and protocols, as well as the cohabitation and cooperation of multiple technologies. Despite the variety of IoT devices, the inherent computational power restrictions of IoT devices, and the massive size of the IoT network, there is a growing interest in autonomic computing for device management. This implies that each device is given the authority to make critical choices without the approval of the others. In this scenario, sensors and devices must interact with one another in a manner that is dispersed. This, in turn, results in a multitude of design issues, some of which include restricted scalability and considerable delay.

These issues can be overcome by designing a secure and supervised distributed architecture. Such an architecture would include a security platform intelligently distributing the processing load across the nodes of the network [4]. DLT, such as the blockchain, is suitable for implementing a decentralized secure architecture [6]. Blockchain can enhance security by providing a decentralized and tamper-proof ledger for transactions and data exchanges. This technology can be used to secure communications, verify device integrity, and ensure the authenticity of data in IoT ecosystems.

The blockchain records transactions in blocks and connects each new block with a cryptographic hash of the previous blocks. Blockchain guarantees data integrity by using Merkle trees. Thus, all transactions within each block are reduced to a single hash value, thus one can easily verify whether the contents of the block have been changed. Merkle trees are also used for zero-knowledge proof verification allowing one party to prove to another party that it has certain information without revealing its confidential content. In the process, Merkle trees can be used to verify the existence and accuracy of a particular piece of a data set without revealing the entire data set [31].

DLT transactions could be validated by trust-free consensus algorithms that allow every node to participate in the consensus. This may increase the robustness and reliability of transactions as well as scalability and reliability compared to absolute consensus algorithms. Additionally, transitioning from a centralized IoT architecture to a distributed one could enhance the effectiveness of CI by enabling decentralized data analysis and decision-making. This improves network security through diverse, real-time threat detection and response [4]. DLT may be used to ensure data security and integrity as an immutable and secure database of CI systems enabling transparent collaboration and trust between decentralized organizations [3].

DLT may enhance the verification of the integrity of training data for ML models and serve as a safeguard against model poisoning by maintaining an immutable and transparent record of each data point and modification. Consensus algorithms used by the DLTs, such as Proof of Work and Proof of Stake, may be employed to authenticate transactions and maintain integrity inside distributed ledgers. It also allows reaching a consensus among all network members about a singular version of the truth in collaborative decision-making contexts [32].

Unlike in conventional IoT/IT/OT systems, where a central authority often governs trust, DLT establishes a decentralized ledger that facilitates safe, decentralized, and trustless interactions and integration among IoT devices. The decentralized and immutable character of DLT can be leveraged to improve whitelisting and blacklisting, where whitelists and blacklists are recorded on a distributed ledger. This ensures that all entries are transparent, secure against tampering, and can be verified by all participants in the network. Due to this strategy, there is no need for a central authority to handle the lists. As a result, the risk of having a single point of failure is reduced, and participants' confidence in one another is increased. Furthermore, the use of smart contracts can automate the process of updating and enforcing these lists, therefore guaranteeing compliance in real-time and lowering the amount of administrative work required [33]. This is essential for scalability in IoT systems and can mitigate potential vulnerabilities and bottlenecks.

The main advantages of DLT can be summarized as [7]:

- Decentralized Trust: Devices may engage in consensus-driven decision-making independent of a central authority, augmenting system resilience.
- Immutable Records: Transactions and interactions are kept permanently, guaranteeing accountability and traceability. This is essential for CI applications requiring autonomous device collaboration.
- Automation with Smart Contracts: These self-executing agreements may automate interactions among IoT devices, facilitating smooth coordination in CI networks, including automated device onboarding, service payment, and resource sharing.

The capacity of DLT to guarantee transparency, security, and trust is essential for supply chain oversight, smart cities, and other IoT applications requiring autonomous device collaboration.

3.5.1 Decentralized Device Management and Access Control using DLT

Challenges regarding a client integration scenario can be addressed using DLT and ZTA as follows. A blockchain-based architecture can be used to allow blockchain nodes to perform regular checks for distributed blacklisting, whitelisting, and registration of IoT clients. Blockchain-based distributed blacklisting is an advanced security approach that enhances IoT network resilience by leveraging blockchain technology for secure and transparent blacklist management. This method uses real-time threat intelligence and ML algorithms to continuously update and share blacklists across decentralized nodes, such as edge and fog computing devices. By analysing device behaviour and network traffic patterns, the system can swiftly identify and isolate rogue devices, minimizing the risk of false positives and ensuring uninterrupted service. Blockchain technology ensures that blacklist data is tamper-proof and transparently synchronized across all nodes, providing a robust mechanism for maintaining device trustworthiness. This adaptive strategy not only improves the accuracy of threat detection but also reduces administrative overhead, making it an effective solution for securing dynamic and distributed network environments [3].

Registered malicious IoT clients can be prevented from detecting the network topology by listening to the signalling traffic and adding new malicious IoT clients with the following business flow (see Figure 5):

1. Client A requests to connect to a registered neighbouring IoT client B.
2. Client B checks whether the IoT client A is blacklisted or registered to the IoT network against the blockchain ledger.
    a. If client A is blacklisted, client B terminates the connection.
    b. If client A is already registered, client B connects and interacts with it.
    c. If client A is neither blacklisted nor registered to the IoT network, client B forwards the request to the AI-blockchain node. An AI-blockchain node, functioning within the IoT network as a blockchain node, executes anomaly detection and serves as a gateway.
3. After receiving the registration request from the registered client B, the AI-blockchain node initiates the registration process for client A. Firstly it performs a blacklist and registration check.
    a. If client A is neither blacklisted nor registered, it performs a whitelist check.
    b. If client A passes the device whitelist check, it adds client A to the IoT network by assigning a public key pair and updating the device registry.
4. The AI-blockchain node shares the key pair with client A and completes the registration process. After registration is completed, client A can access the IoT network.

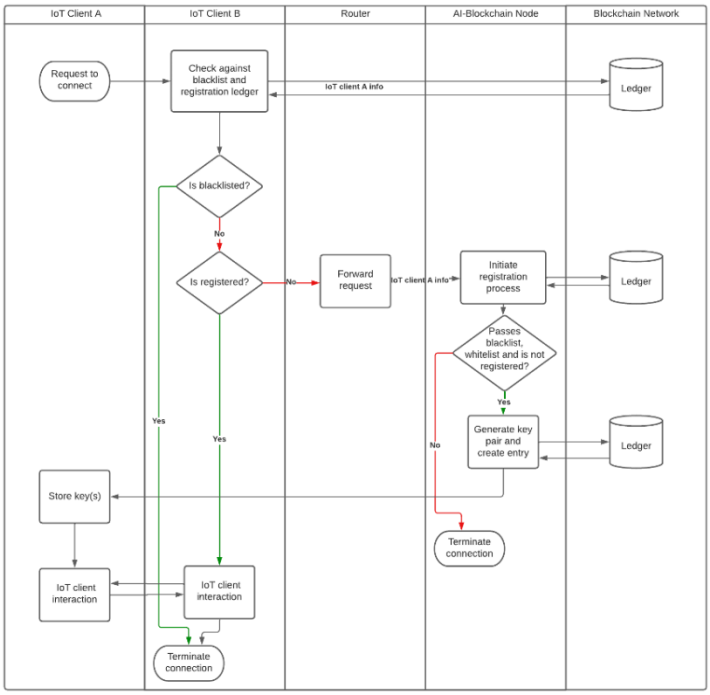

Figure 5. Sequence diagram of IoT client interaction *[3]*

Once the IoT client is registered, it is continuously monitored by AI-blockchain nodes, and anomaly detection is performed. If anomalous behaviour is detected by any of the AI-blockchain nodes in the network, it publishes its findings via the blockchain network. The blockchain network jointly decides in real-time whether to blacklist the IoT client by individually performing anomaly detection, using a voting mechanism such as majority voting, OR rule, AND rule, etc. If and when AI-blockchain nodes have consensus on anomalous behaviour, then the malicious IoT client is added to the blacklist via the blockchain network using a blockchain consensus algorithm [33]. If AI-blockchain nodes identify an IoT client as offline for a specified duration, such as owing to a physical assault or battery depletion, it is then included in the list of compromised clients. Therefore, clients are required to inform about their presence in the network and approaching battery depletion.

3.5.2 Secure Distributed Logging using DLT

Utilizing blockchain technology for distributed secure logging provides a formidable approach to improving the security and integrity of log files. Utilizing the decentralized and immutable characteristics of blockchain, log entries may be safely documented and preserved across numerous nodes, thwarting illegal modifications and guaranteeing transparency. Every log entry is cryptographically connected to its predecessor, forming a tamper-evident sequence of entries. This method safeguards against nefarious alterations while enabling instantaneous auditing and verification of logs independent of a central authority. Furthermore, blockchain-based logging enhances compliance with regulatory standards by providing an immutable audit trail, making it an ideal solution for environments where data integrity and security are paramount.

3.6 Advanced Threat Intelligence

Threat intelligence involves collecting and analyzing information about current and emerging threats. By leveraging advanced analytics and threat intelligence platforms, organizations can gain insights into attackers' tactics, techniques, and procedures, enabling them to preemptively strengthen their defenses.

Collaboration and information sharing among organizations, governments, and cybersecurity vendors are crucial for effective cyber risk management. Sharing threat intelligence, best practices, and resources can help build a collective defense against cyber threats. Initiatives like Information Sharing and Analysis Centers (ISAC) play a pivotal role in this collaborative approach.

3.7 Dynamic Isomorphism

A significant problem in CI-enabled IoT networks is the coordination, distribution, and synchronization of intelligence across varied, resource-limited, and dynamic settings. Dynamic isomorphism can be used to address these issues. Dynamic isomorphism refers to the ability of software systems to adapt and transition across different computational contexts without necessitating substantial alterations to their architecture or code. Dynamic isomorphism implementations frequently depend on uniform programming technologies and frameworks, including containerization, WebAssembly, or platform-agnostic runtimes, to facilitate the dynamic deployment and migration of software components across diverse platforms [34]. This facilitates the **redistribution of computational workloads**, allowing jobs to be transferred from resource-limited edge devices to more powerful cloud servers when demanding processing is necessary. Conversely, jobs may be transferred to the edge to diminish latency and enhance responsiveness, particularly for time-critical applications. This adaptability improves system performance by facilitating intelligent load balancing, alleviating bottlenecks, and averting resource inefficiencies, so guaranteeing that each activity is performed in the most appropriate environment. Furthermore, dynamic isomorphism facilitates the **adaptive scaling of resources**, enabling systems to effectively adjust to varying workloads and sustain high efficiency under changing conditions. It enables real-time data processing and decision-making at the edge, minimizing latency and improving responsiveness. It concurrently ensures the efficient dissemination of updates and intelligence throughout the network, synchronizes devices, and maintains operations with current information. Consequently, dynamic isomorphism serves as a fundamental principle for constructing adaptive, efficient, and intelligent IoT networks.

Conventional AI models frequently encounter challenges stemming from their rigid designs, restricted adaptability, and ineffectiveness in managing real-time, distributed decision-making processes. Therefore, there is a need to automate the design of neural network architectures to facilitate scalable and efficient AI solutions. Dynamic isomorphism can improve AI implementations over the cloud-edge continuum, facilitating calculations near the data source or offloading them to the cloud as required. This methodology addresses critical challenges in traditional approaches, including inefficiencies in designing large, dispersed systems like IoT networks. It facilitates the deployment and distribution of AI models or updates across the network. A singular iteration of a software component can be disseminated and run across all devices, including low-powered edge devices, gateways, or cloud servers, hence eliminating the necessity for extensive reconfiguration or recompilation [35]. This capacity enhances the dissemination of intelligence and guarantees that all nodes stay synchronized with the most recent updates. It enhances synchronization by enabling real-time data and model sharing among IoT devices through compatibility and seamless functionality. Devices can dynamically relocate jobs or exchange intelligence based on resource availability, as their same software assures seamless transitions without errors or delays. This is particularly crucial in dynamic contexts, where resource availability and operational demands fluctuate swiftly.

Evolutionary algorithms have arisen as effective instruments for this objective, emulating natural selection to progressively enhance network designs according to performance measures. Frameworks such as the Synthesis of Tailored Architectures (STAR) [36] and principles in Evolutionary Neural Architecture Search (ENAS) [37] illustrate this by utilizing continuous learning and resource-aware optimization to develop models tailored for varied and dynamic contexts. These systems dynamically adjust their structures in reaction to real-time input and environmental changes by incorporating principles inspired by neuroplasticity. This methodology not only improves the adaptability and efficiency of AI models but also lays the groundwork for developing intelligent ecosystems that can jointly and effectively tackle complicated issues. Progress in this field illustrates the capacity to generalize automated design ideas across diverse applications, ranging from IoT networks to extensive, decentralized AI systems. These architectures are engineered to utilize streaming data, adjust to fluctuating resource availability, and autonomously rearrange to manage diverse data complexities. This may enable seamless intelligence coordination across IoT devices, efficient load distribution, and real-time collaborative decision-making, transforming IoT networks into cohesive, intelligent ecosystems adept at collectively and effectively resolving difficult challenges.

3.8 Knowledge Graphs and Ontologies

Knowledge graphs and ontologies are essential for facilitating coordination and comprehension in CI-enabled IoT networks. A knowledge graph systematically organizes and depicts data as interrelated entities and their relationships, offering a structured, semantic foundation for devices to analyze and communicate information efficiently. Ontologies establish a common lexicon and framework that standardizes how devices articulate and comprehend data, ensuring uniformity

across diverse systems. Collectively, these techniques enable IoT devices to attain a cohesive perspective of the environment, promoting interoperability and collaborative reasoning. As an example, in a smart city, knowledge graphs can define the interconnections among traffic sensors, public transit systems, and emergency services, whereas ontologies provide uniform interpretations of terms such as "traffic congestion" and "incident severity" across all devices. This semantic framework facilitates real-time decision-making, adaptive learning, and collaborative problem-solving, enhancing the intelligence and responsiveness of IoT networks to dynamic settings.

3.9 Digital Twin Frameworks

Digital twin (DT) frameworks provide a revolutionary method for collaborative activities in IoT networks by generating virtual clones of actual items, systems, or entire networks. These digital replicas consistently synchronize with their physical counterparts, facilitating real-time monitoring, analysis, and modeling of system activities. In CI-enabled IoT networks, DT can serve as a cohesive platform for devices to engage electronically, predict outcomes, enhance resource distribution, and coordinate operations. In a smart manufacturing setting, the DT of machinery and processes can replicate production situations, forecast potential bottlenecks, and provide dynamic coordination among interconnected devices to sustain efficiency. DT frameworks boost decision-making accuracy, improve fault tolerance, and promote the seamless integration of new devices or systems by offering a real-time, data-driven model of the network, hence making IoT networks more flexible and robust [38].

4 Conclusions

This report investigates the efficient cyber risk management of IoT and OT ecosystems, including the architectural issues and solutions. The integration of IT, OT, and IoT ecosystems presents a double-edged sword, offering both enhanced capabilities and new security challenges.

Utilizing CI via data sharing and collaborative problem-solving has recently become an important technique for enhancing threat detection and response. This strategy improves networks' potential to tackle existing security issues and establishes a robust defense against future attacks. However, distributed algorithms and load-balancing strategies used in CI have their own risks and architectural challenges and require risk and impact analysis.

Solutions to multi-faceted architectural challenges in CI-enabled heterogeneous systems include decentralization, trust management, scalable network architectures, multilayered security, resilience, data integrity, authentication, advanced threat intelligence, AI/ML, distributed ledger technology, trust scoring, and ZTA. Recent advances in science, technology, and cyber risk management practices provide a robust foundation, while the evolving threat landscape necessitates continuous innovation and adaptation. By embracing these solutions, organizations can enhance their cyber resilience and secure their interconnected ecosystems against emerging threats.

Security analysis is crucial for identifying potential cyber risks and vulnerabilities, implementing effective threat mitigation techniques, and protecting the integrity and confidentiality of data, code, systems, and infrastructures. For this purpose, security analysis of selected CISSAN solutions has been carried out in detail (provided in the confidential annexes).

The development of global standards and regulations for the security of CI-enabled IoT networks is vital for addressing the problems encountered by these technologies, including coordinated responses to cyberattacks.

References

[1] G. BB and Q. M., "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols.," *Concurrency Computation Practice and Experience,* 2020.

[2] A. Tanveer, R. Sinha and S. G. MacDonell, "On Design-time Security in IEC 61499 Systems: Conceptualisation, Implementation, and Feasibility," in *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, Porto, Portugal, 2018.

[3] T. Frantti and I. Şafak, "An Architecture for Enabling Collective Intelligence in IoT Networks," in *International Conference on Computational Collective Intelligence (ICCCI) 2023. Lecture Notes in Computer Science (LNCS)*, 2023.

[4] T. Q. Y. H. R. e. a. Alsboui, "Distributed Intelligence in the Internet of Things: Challenges and Opportunities," *SN Computer Science,* vol. 2, no. 277 , 2021.

[5] Q. Arshad, W. Khan, F. ,. M. K. K. Azam, H. Yu and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems,* vol. 9, p. 6155–6176, 2023.

[6] Y. Maleh, S. Lakkineni, L. Tawalbeh and A. AbdEl-Latif, "Blockchain for Cyber-Physical Systems: Challenges and Applications," in *Advances in Blockchain Technology for Cyber Physical Systems*, Y. Maleh, L. Tawalbeh, S. Motahhir and A. Hafid, Eds., Springer Cham, 2022, p. 11–59.

[7] B. Farahani, F. Firouzi and M. Luecking, "The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions," *Journal of Network and Computer Applications,* vol. 177, no. 102936, 2021.

[8] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," *IEEE Access,* vol. 9, pp. 59353-59377, 2021.

[9] C. A. Baykara, I. Şafak and K. Kalkan, "SHAPEIoT: secure handshake protocol for autonomous IoT device discovery and blacklisting using physical unclonable functions and machine learning," in *13th International Conference on Network and Communications Security (NCS 2021)*, 2021.

[10] G. Fortino, L. Fotia, F. Messina, D. Rosaci and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," *IEEE Access,* vol. 8, pp. 60117-60125, 2020.

[11] C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT," *Wireless Personal Communications,* vol. 112, p. 1383–1429, 2020.

[12] C. Berger, P. Eichhammer, H. P. Reiser, J. Domaschka, F. J. Hauck and G. Habiger, "A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms," *ACM Computing Surveys,* vol. 54, no. 7, 2021.

[13] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah and P. Djukic, "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats," *ACM Computing Surveys,* vol. 55, no. 5, p. 37, 2022.

[14] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology (NIST), 202.

[15] V. K. R. Vangoor, S. M. Yellepeddi, C. S. Ravi, A. K. P. Venkata and P. Katari, "Zero Trust Architecture: Implementing Microsegmentation in Enterprise Networks," *Journal of Artificial Intelligence Research and Applications,* vol. 4, no. 1, 2024.

[16] Y. He, D. Huang, L. Chen, Y. Ni and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing,* p. 13, 2022.

[17] R. Freter, "Department of Defence (DoD) Zero Trust Reference Architecture, Version 2.0.," *Proceedings of the Defense Information Systems Agency (DISA) and National Security Agency (NSA),* 2022.

[18] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access,* vol. 10, pp. 57143-57179, 2022.

[19] C. Bast and K.-H. Yeh, "Emerging Authentication Technologies for Zero Trust on the Internet of Things," *Symmetry,* vol. 16, no. 8, 2024.

[20] National Institute of Standards and Technology (NIST), “The NIST Cybersecurity Framework (CSF) 2.0,” 2024.

[21] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), “ISO/IEC 27001:2022 Information security management systems — Requirements,” ISO/IEC, 2022.

[22] N. A. Tigist Abera, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi and G. Tsudik, "Invited - Things, trouble, trust: on building trust in IoT systems," in *The 53rd Annual Design Automation Conference (DAC '16)*, New York, NY, USA, 2016.

[23] A. Yadav, S. Kumar and J. Singh, "A Review of Physical Unclonable Functions (PUFs) and Its Applications in IoT Environment," in *Ambient Communications and Computer Systems. Lecture Notes in Networks and Systems*, 2022.

[24] I. -R. Chen, J. Guo and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing,* vol. 9, no. 3, pp. 482-495, 2016.

[25] Y. Ge and Q. Zhu, "Trust Threshold Policy for Explainable and Adaptive Zero-Trust Defense in Enterprise Networks,"," in *2022 IEEE Conference on Communications and Network Security (CNS)*, Austin, TX, USA, 2022.

[26] F. Bao, *Dynamic Trust Management for Mobile Networks and Its Applications,* Falls Church, VA, USA: Virginia Polytechnic Institute and State University, 2013.

[27] M. Q. Ali, E. Al-Shaer, H. Khan and S. A. Khayam, "Automated Anomaly Detector Adaptation using Adaptive Threshold Tuning," *ACM Transactions on Information and System Security,* vol. 15, no. 4, p. 30, 2013.

[28] A. Russell-Gilbert, A. Sommers, A. Thompson, L. Cummins, S. Mittal, S. Rahimi, M. Seale, J. Jaboure, T. Arnold and J. Church, "AAD-LLM: Adaptive Anomaly Detection Using Large Language Models," arXiv , 2024.

[29] F. Alotaibi and S. Maffeis, "Mateen: Adaptive Ensemble Learning for Network Anomaly Detection," in *27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID '24)*, New York, NY, USA, 2024.

[30] C. Chai, L. Cao, G. Li, J. Li, Y. Luo and S. Madden, "Human-in-the-loop Outlier Detection," in *The 2020 ACM SIGMOD International Conference on Management of Data (SIGMOD '20)*, New York, NY, USA, 2020.

[31] L. Lantz and D. Cawrey, Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications, O'Reilly Media, 2020.

[32] E. T. M. Beltrán, M. Q. Pérez, P. M. S. Sánchez, S. L. Bernal, G. Bovet and M. G. Pérez, "Decentralized Federated Learning: Fundamentals, State of the Art, Frameworks, Trends, and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 4, pp. 2983-3013, 2023.

[33] O. Tarlan, I. Safak and K. Kalkan, "DiBLIoT: A Distributed Blacklisting Protocol for IoT Device Classification Using the Hashgraph Consensus Algorithm," in *2022 International Conference on Information Networking (ICOIN)*, Jeju-si, Korea, Republic of, 2022.

[34] P. Kotilainen, V. Heikkilä, K. Systä and T. Mikkonen, "Towards Liquid AI in IoT with WebAssembly: A Prototype Implementation," in *Mobile Web and Intelligent Information Systems (MobiWIS 2023). Lecture Notes in Computer Science (LNCS)* , 2023.

[35] K. Systä, C. Pautasso, A. Taivalsaari and T. Mikkonen, "LiquidAI: Towards an Isomorphic AI/ML System Architecture for the Cloud-Edge Continuum," in *International Conference on Web Engineering (ICWE) 2023. Lecture Notes in Computer Science (LNCS)*, 2023.

[36] A. W. Thomas, R. Parnichkun, A. Amini, S. Massaroli and M. Poli, "STAR: Synthesis of Tailored Architectures," arXiv, 2024.

[37] H. Pham, M. Y. Guan, B. Zoph, Q. V. Le and J. Dean, "Efficient Neural Architecture Search via Parameter Sharing," in *The 35th International Conference on Machine Learning*, Stockholm, Sweden, 2018.

[38] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan and Y. Liu, "A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects," *IEEE Internet of Things Journal,* vol. 10 , no. 17, pp. 14965-14987, 2023.

Annex A Security Analysis

The security analysis annexes contain information sensitive for certain CISSAN partners, so those are provided in separate documents with the confidential dissemination level.

A.1 GeoData IoT Platform Security Analysis