ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στην ΑΝΑΠΤΥΞΗ & ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"Αξιοποίηση της Τεχνολογίας Blockchain για την Παροχή Κινήτρων στις Ροές Πληροφορίας με Χρήση Ασαφούς Λογικής"

Κωνσταντίνος Καρλής

f3312403

ΑΘΗΝΑ, ΙΑΝΟΥΑΡΙΟΣ 2026

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

DEPARTMENT OF INFORMATICS

M.Sc.

in DEVELOPMENT AND SECURITY OF INFORMATION SYSTEMS

DIPLOMA THESIS

“Blockchain-Based Incentivization of Information Flows using Fuzzy Logic”

Konstantinos Karlis

f3312403

ATHENS, JANUARY 2026

Περίληψη

Η ραγδαία εξάπλωση του Βιομηχανικού Διαδικτύου των Πραγμάτων (Industrial Internet of Things) έχει μετασχηματίσει τα σύγχρονα βιομηχανικά περιβάλλοντα, οδηγώντας σε αυξημένη διασυνδεσιμότητα, αυτοματοποίηση και ανταλλαγή δεδομένων σε πραγματικό χρόνο. Παρά τα σημαντικά λειτουργικά οφέλη, η πολυπλοκότητα και η δυναμική φύση των IIoT υποδομών δημιουργούν σοβαρές προκλήσεις ασφάλειας, ιδιαίτερα όσον αφορά την παράνομη ή επικίνδυνη ροή πληροφοριών. Οι παραδοσιακοί μηχανισμοί ελέγχου πρόσβασης συχνά αδυνατούν να εντοπίσουν έμμεσες εξαρτήσεις και αλυσιδωτές επιπτώσεις, καθιστώντας αναγκαία την υιοθέτηση πιο προσαρμοστικών και βασισμένων στον κίνδυνο προσεγγίσεων.

Η παρούσα διπλωματική εργασία εξετάζει το πρόβλημα της διαχείρισης της ροής πληροφοριών σε περιβάλλοντα IIoT και εστιάζει στην ανάλυση του κινδύνου που προκύπτει από παράνομες ή ύποπτες ροές δεδομένων. Αρχικά, παρουσιάζεται το θεωρητικό υπόβαθρο των IIoT συστημάτων, των μηχανισμών ελέγχου πρόσβασης και ελέγχου ροής πληροφοριών, καθώς και των τεχνολογιών blockchain. Ιδιαίτερη έμφαση δίνεται στις ιδιαιτερότητες των βιομηχανικών υποδομών, όπως οι αυξημένες απαιτήσεις αξιοπιστίας, διαθεσιμότητας και ανθεκτικότητας σε επιθέσεις.

Στη συνέχεια, αναλύεται η μεθοδολογία INFFLOW-RT, η οποία παρέχει ανάλυση σε πραγματικό χρόνο της επικινδυνότητας παράνομων ροών πληροφορίας σε IIoT περιβάλλοντα. Η μεθοδολογία βασίζεται στη μοντελοποίηση των συστημάτων ως γράφων εξαρτήσεων και αξιοποιεί χαρακτηριστικά συναλλαγών, όπως η σοβαρότητα των δεδομένων, το είδος της λειτουργίας και τη νομιμότητα. Παράλληλα, εξετάζεται η διάδοση του κινδύνου μέσω εξαρτήσεων πολλαπλών τάξεων και η δομική σημασία των κόμβων, επιτρέποντας την εκτίμηση τόσο τοπικών όσο και συστημικών επιπτώσεων.

Βασιζόμενη στην ανάλυση αυτή, η εργασία προτείνει το INFFLOW-RT+, ένα προσαρμοστικό πλαίσιο κινήτρων που συνδέει την εκτίμηση κινδύνου της ροής πληροφοριών με αναλογικές ενέργειες επιβράβευσης και επιβολής. Το πλαίσιο αξιοποιεί ασαφή λογική για τη διαχείριση της αβεβαιότητας και των σταδιακών αλλαγών συμπεριφοράς, ενώ ενσωματώνει τεχνολογίες blockchain και έξυπνα συμβόλαια για αποκεντρωμένη, διαφανή και αδιάβλητη επιβολή κινήτρων και ποινών. Με τον τρόπο αυτό, η ασφαλής συμπεριφορά καθίσταται η πλέον ωφέλιμη στρατηγική για τους συμμετέχοντες κόμβους.

Τέλος, αν και το προτεινόμενο πλαίσιο δεν έχει εφαρμοστεί ή αξιολογηθεί σε πραγματικό βιομηχανικό περιβάλλον, παρουσιάζονται ενδεικτικά σενάρια λειτουργίας που αναδεικνύουν τη δυναμική του. Τα σενάρια αυτά δείχνουν πώς η σύνδεση της ανάλυσης κινδύνου με μηχανισμούς κινήτρων μπορεί να ενισχύσει τη συμμόρφωση, την αυτορρύθμιση και τη μακροπρόθεσμη ανθεκτικότητα των IIoT υποδομών. Συνολικά, η εργασία συμβάλλει στη μελέτη της διαχείρισης της ασφάλειας σε IIoT συστήματα, προτείνοντας μια ενοποιημένη, προσαρμοστική και βασισμένη στον κίνδυνο προσέγγιση.

Abstract

The rapid growth of the Industrial Internet of Things (IIoT) has significantly changed modern industrial environments by enabling increased connectivity, automation and real-time data exchange. Despite the substantial operational benefits, the complexity and dynamic nature of IIoT infrastructures introduce critical security challenges, particularly related to illegal or risky information flows. Traditional access control mechanisms often fail to capture indirect dependencies and cascading effects, highlighting the need for adaptive and risk-based security approaches.

This thesis addresses the problem of information flow management in IIoT environments, focusing on the assessment of risks arising from illegal or suspicious data exchanges. Initially, the theoretical background of IIoT systems, access control mechanisms, information flow control principles and blockchain technologies is presented. Special emphasis is placed on the unique characteristics of industrial infrastructures, including strict requirements for reliability, availability and resilience against cyber threats.

Subsequently, the INFFLOW-RT methodology is examined as a real-time risk-based approach for detecting illegal information flows in IIoT systems. The methodology models industrial environments as dependency graphs and evaluates transactions using descriptors such as data severity, operation type and legality. In addition, it considers risk propagation across multi-order dependencies and the structural importance of nodes, enabling both localized and system-wide risk assessment.

Building upon this analysis, the thesis introduces INFFLOW-RT+, a risk-adaptive incentive framework that translates information flow risk assessments into proportional incentive and enforcement actions. The framework employs fuzzy logic to manage uncertainty and gradual behavioral changes, while leveraging blockchain technology and smart contracts to ensure decentralized, transparent and tamper-resistant enforcement. Through this design, secure behavior becomes the most beneficial long-term strategy for participating nodes.

Although the proposed framework has not been deployed or experimentally evaluated in real industrial environments, illustrative scenarios are presented to demonstrate its potential effectiveness. These scenarios highlight how linking risk analysis with incentive mechanisms can promote compliance, self-regulation and long-term resilience in IIoT infrastructures. Overall, this thesis contributes to risk-aware and incentive-driven security management in IIoT systems by proposing an integrated and adaptive approach.

Acknowledgements

With the completion of this thesis, I would like to thank all those who supported me throughout its preparation.

First of all, I would like to thank my supervisor, Professor Dimitris Gritzalis, for the trust he showed in me by assigning this thesis and for his continuous guidance and support during its development. I am also grateful for the knowledge he provided throughout my studies in the postgraduate program Development and Security of Information Systems.

I would also like to thank the PhD candidate Argyro Anagnostopoulou for our excellent collaboration, her valuable assistance and her willingness to guide me at every stage of this thesis.

Finally, I would like to thank my family for their support and understanding during my studies.

List of Figures

List of Tables

Table of Contents

1.Introduction

The rapid adoption of the Industrial Internet of Things (IIoT) has changed modern industrial environments. It allows for large-scale connections between sensors, controllers, machines and software services. Industrial systems increasingly depend on continuous data exchange to support automation, real-time monitoring, predictive maintenance and intelligent decision-making. However, this high level of connectivity brings new security challenges because information flows through various components, administrative domains and communication layers. In these environments, failures or malicious actions can lead to serious operational, financial and safety issues.

One of the biggest challenges in IIoT environments is managing information flows securely. Traditional access control mechanisms focus mainly on granting or denying access to specific resources. However, they often fail to capture how information is transmitted through indirect dependency chains after access is granted. This can lead to illegal or risky information flows even when local access policies are followed. Furthermore, security monitoring and risk assessment techniques often work passively. They provide alerts or risk indicators without directly influencing system behavior. This thesis addresses these issues by focusing on risk-aware information flow management. It proposes mechanisms that turn risk assessment results into clear, automated and incentive-driven behavioral regulation in IIoT systems.

1.1 Research Contribution

The main contribution of this thesis is the design and analysis of a risk-adaptive incentive framework for managing information flows in Industrial Internet of Things (IIoT) environments. This approach builds on a risk-based real-time information flow analysis methodology and extends it by linking illegal or risky information flow behavior to automated, proportional incentive and enforcement actions.

In modern industrial infrastructures, where information moves through complex dependency chains and indirect interactions, this work addresses the limitations of traditional access control and monitoring-focused security models. Instead of treating risk assessment as a passive analysis, the proposed framework turns risk indicators into actionable system responses that actively influence node behavior over time.

By combining information flow risk analysis, fuzzy logic decision-making and blockchain-enabled decentralized enforcement, this research offers a systematic way to evaluate both the likelihood of illegal information flows and their systemic impact. The framework focuses on behavioral regulation through incentives, making secure information handling the most beneficial long-term strategy for participating nodes. Through conceptual modeling, methodological synthesis and illustrative scenarios, this thesis contributes to the ongoing discussion about risk-aware security management and incentive-driven compliance in IIoT ecosystems.

1.2 Research Objectives

Aligned with the above contribution, this thesis sets specific objectives to guide the research toward measurable outcomes. These objectives are:

- To examine the characteristics and security challenges of Industrial Internet of Things environments, focusing on access control, information flow control and risk propagation based on dependencies.
- To analyze existing methods in blockchain-based access control, risk assessment, fuzzy logic modeling and incentive mechanisms, identifying their limitations when applied independently.
- To study and apply a risk-based real-time method for detecting illegal information flows in IIoT systems, focusing on dynamic risk estimation and multi-order dependency analysis.
- To design a risk-adaptive incentive mechanism that changes information flow risk assessments into proportional reputation updates, economic incentives and enforcement actions.
- To incorporate fuzzy logic to address uncertainty, gradual behavior changes and context-dependent decision-making, instead of strict threshold-based reactions.
- To use blockchain and smart contracts for clear, tamper-resistant and decentralized enforcement of incentives and penalties.
- To show how risk-aware incentives can affect resource allocation and long-term behavior, improving resilience and self-regulation in IIoT infrastructures.

These objectives aim to close the gap between identifying security risks and applying practical automated behavior regulation in distributed industrial systems.

1.3 Thesis Structure

The rest of this thesis is organized as follows. Chapter 2 presents the theoretical background required for the study. It introduces the Industrial Internet of Things and its layered architecture. The chapter highlights the key differences between IoT and IIoT environments in terms of security, reliability and operational limits. It also looks into access control methods and information flow control principles, highlighting their importance in managing data flow in distributed systems. Additionally, it discusses security dependencies, blockchain fundamentals and blockchain-based security approaches. These concepts establish the foundation for risk-aware and decentralized enforcement in IIoT infrastructures.

Chapter 3 reviews related work in blockchain-based access control, secure data exchange, fuzzy logic–based risk assessment and incentive-driven security mechanisms. The chapter critically reviews existing strategies and how they address authorization, risk assessment and behavioral regulation in IIoT environments. Through this review, it identifies key limitations in current solutions. In particular, it highlights the absence of integrated frameworks that directly connect information flow risk to automated incentives and long-term behavior management.

Chapter 4 introduces the INFFLOW-RT methodology for risk-based real-time analysis of illegal information flows in IIoT environments. It presents a system modeling approach based on dependency graphs and the transaction descriptors that describe security-relevant events. The chapter also explains the process of estimating dynamic risk. Furthermore, it discusses how risk propagates across multi-order dependencies and how the system's structural features, like node centrality, affect the overall security posture of industrial infrastructures.

Chapter 5 explores incentive mechanisms in cybersecurity and IIoT systems, offering an overview of their theoretical foundations and practical implications. It looks at a wide range of incentive mechanisms, which include game-theoretic, reputation-based, token-based, auction-based and learning-based approaches. The chapter discusses how these mechanisms influence cooperation, discourage malicious behavior and promote scalability and sustainability in distributed industrial environments.

Chapter 6 gives a comparative discussion of different incentive mechanism using a set of evaluation attributes tailored to IIoT requirements. It analyzes similarities, differences and complementary characteristics of the approaches reviewed. The discussion focuses on coordination costs, fairness, security strength, scalability and adaptivity. The chapter also shows how different incentive types can be combined into hybrid architectures. These combinations aim to balance efficiency, resilience and operational limits in industrial systems.

Chapter 7 presents the risk-adaptive incentive framework, INFFLOW-RT+. The chapter describes the overall architecture of the framework and explains how real-time information flow risk evaluations are turned into proportional incentive and enforcement decisions. It details the role of fuzzy logic in reputation assessment and the use of blockchain smart contracts for decentralized enforcement. Additionally, it explains how incentive results are integrated into resource allocation processes. Examples are provided to illustrate how the mechanism operates as a closed feedback loop. This loop promotes self-regulation and long-term compliance in IIoT environments.

Finally, the concluding chapter summarizes the main findings of the thesis and discusses their implications for secure information flow management in Industrial Internet of Things systems. It outlines the limitations of the proposed approach and identifies directions for future research. The discussion focuses on scalability, real-world deployment and the evolution of risk-adaptive and incentive-driven security mechanisms.

2.Theoretical Background

2.1 Industrial Internet of Things (IIoT)

A common used architectural model for IIoT systems is the four-layer architecture, which consists of the perception, network, middleware and application layers [1]. Each layer performs specific functions and introduces different operational and security challenges. As a result, security management in IIoT environments must follow a complete and layered approach rather than relying on isolated protection mechanisms.

The perception layer, also known as the sensing or device layer, is the foundation of the architecture. It contains physical devices like sensors, actuators, RFID tags, cameras and programmable logic controllers (PLCs). Its main job is to collect raw data from the physical world, like temperature, vibration, pressure or light and convert them into electrical or optical signals for higher-level systems to read. Because these devices often work in open or remote industrial areas, they are especially vulnerable to physical and logical attacks. These include node capturing, where an attacker replaces or manipulates a legitimate node and malicious code injection, which can disrupt normal operations. In addition, sleep-deprivation attacks can exhaust the limited energy of edge devices, stopping data collection and transmission [1].

The network layer supports communication within IIoT ecosystems. It makes sure that data can transmit securely between devices and higher layers using various wired and wireless technologies such as Ethernet, 5G, Wi-Fi, LPWAN and industrial communication protocols like MQTT or OPC UA. At this level, data packets are routed and authenticated, while encryption mechanisms protect them from unauthorized interception. Due to its connectivity role, this layer is highly vulnerable to Denial-of-Service (DoS/DDoS) attacks, which flood the network with malicious traffic, as well as routing attacks, such as sinkhole and wormhole, that redirect data to compromised nodes. Phishing and spoofing attacks can also target poorly setup gateways or access policies, stealing credentials and giving unauthorized access to industrial control networks [1].

The middleware layer is responsible for processing and managing services. It handles data aggregation, computation and storage. It provides the infrastructure for cloud computing, big-data analytics and machine learning. This allows raw sensor readings to become meaningful insights and digital representations of physical processes. However, because it often depends on centralized cloud platforms and third-party APIs, it can become a primary target for attacks like SQL injection, man-in-the-middle and cloud-malware injection. These could damage data integrity or confidentiality. To counteract this, strong encryption, access control and continuous monitoring of data transactions are necessary [1].

At the top, the application layer connects industrial services with end users. It enables intelligent functions, such as production monitoring, predictive maintenance, inventory optimization and decision-making based on data. Security at this level focuses on access control, data protection and application-level integrity. Common threats include account breaches, data thefts, cross-site scripting (XSS) and unauthorized reprogramming of industrial devices. Such issues could seriously disrupt industrial systems. Therefore, advanced authentication, data isolation and end-to-end encryption are needed to maintain confidentiality and trust across the entire IIoT ecosystem [1].

The four-layer IIoT architecture is essential for designing, analyzing and securing industrial environments. Each layer provides unique functions and introduces different vulnerabilities that must be addressed together. Understanding these layers is essential for creating advanced protection systems, decentralized trust management models like blockchain and risk-based incentive frameworks, which will be discussed in the following chapters.

2.2 Differences between IoT and IIoT

As mentioned earlier, the Industrial Internet of Things (IIoT) is the advancement of the Internet of Things (IoT) in industrial environments. It integrates new sensing, communication and data analytics technologies into critical infrastructures and production systems. To better understand its role in Industry 4.0, it is important to highlight the key differences between IoT and IIoT based on their goals, architecture and operational needs.

The IoT mainly focuses on consumer applications designed to improve convenience, efficiency and personalization in everyday life. Examples include smart homes, wearable devices and smart city systems. In contrast, the IIoT targets mission-critical industrial settings where reliability, security and real-time operation are fundamental [2]. Its applications include manufacturing plants, energy grids, transportation systems and healthcare infrastructures, where even small failures can result in severe operational, financial or safety-related consequences [3].

One significant difference lies is how Information Technology (IT) and Operational Technology (OT) systems are integrated. While IoT mainly operates within IT infrastructures, relying on cloud-based communication and software, IIoT bridges IT with OT. This includes systems like PLCs, SCADA and Distributed Control Systems (DCS), forming a unified industrial ecosystem [4]. This integration makes the IIoT more complex and demanding because it requires synchronization between digital and physical processes with minimal delay or tolerance for error.

The technical characteristics of IoT and IIoT devices also differ significantly. IoT devices are usually low-cost, low-power and lightweight. They are made for non-critical applications with limited processing power and shorter operational lifespans. In contrast, IIoT devices are designed for high durability and reliability, capable of operating in harsh industrial environments with extreme temperatures, vibration and electromagnetic interference. IIoT deployments require a higher level of system availability, as industrial systems require continuous operation with minimal downtime [3].

Communication technologies provide further distinctions between IoT and IIoT. IoT networks typically use protocols such as Wi-Fi, Zigbee or Bluetooth Low Energy, which work well for short-range wireless communication and energy efficiency. IIoT networks use industrial Ethernet, 5G with ultra-low latency and strong protocols like MQTT and OPC UA to guarantee real-time data transmission and reliable Quality of Service (QoS) [1], [3]. In addition, IIoT setups often rely on wired or hybrid communication networks to ensure steady connectivity and minimize interference among thousands of connected devices.

The two approaches also differ in data processing and analysis. In the IoT, data is usually sent to the cloud for analysis focused on user-centric improvements. In the IIoT, however, edge and fog computing architectures process data closer to where it is generated, reducing latency and supporting real-time decision making [4]. In IIoT systems, data are often handled through Artificial Intelligence (AI) and Machine Learning (ML) models that enable predictive maintenance, quality control and autonomous process optimization.

Furthermore, the IIoT reaches beyond traditional industrial domains, finding applications in healthcare, defense and logistics. In these areas, reliability and real-time responses are critical since system failures can affect human safety or threaten national and infrastructural security [4]. This broad range of applications shows that IIoT is not just a technological upgrade of IoT but a complete framework that integrates intelligent systems across various industrial and societal sectors.

Despite their differences, IoT and IIoT share common technological and security challenges. Vulnerabilities present in IoT ecosystems, such as weak encryption, outdated firmware or insufficient authentication, also exist in IIoT environments. But they are often more severe and impactful due to the critical nature of industrial operations [1], [4]. Understanding these shared risks is essential for addressing access control and information flow security in IIoT systems.

2.3 Access Control Mechanisms in IIoT

Managing access in the Industrial Internet of Things (IIoT) is crucial for industrial cybersecurity. It ensures that only authorized users, devices and processes can interact with important assets. Unlike traditional IT infrastructures, which rely on centralized and mostly static policies, IIoT networks are diverse, distributed and dynamic. They include sensors, actuators, controllers and hybrid devices that operate across different administrative domains. This complexity makes access control more than just a policy issue. It’s also a challenge of context awareness, scalability and information integrity [5], [6].

Early IIoT deployments mostly used centralized access control setups. In these systems, one authority defined and enforced all access policies. While this approach simplified management, it led to bottlenecks, communication delays and a critical single point of failure. The need for flexibility caused the creation of hybrid architectures. Here, central servers maintained policy authority while edge devices participated in context-aware decision making. However, even these models had difficulty to meet the low-latency and high-availability requirements of industrial environments. As a result, research has moved toward distributed and decentralized access control systems, where endpoint devices autonomously exchange and confirm permissions based on local policies or delegated capabilities [5].

The modern understanding of access control in IIoT is structured around three key phases: identification, authentication and authorization. During identification, a subject such as a user, machine or process declares its identity to the system. Next, authentication verifies that identity using cryptographic keys, credentials or trusted hardware. Lastly, authorization determines what actions the authenticated subject is allowed to perform, based on pre-defined or dynamically generated rules. According to Kokila and Reddy (2025) [6], these phases must work together to maintain the CIA triad (confidentiality, integrity and availability), while adapting to the limitations of low-power and real-time IIoT devices.

To enable flexible and detailed decision making, IIoT systems often use policy-based access control architectures compliant with standards like XACML 3.0 and Next Generation Access Control (NGAC). In these architectures, authorization is achieved through modular components. The Policy Administration Point (PAP) defines rules and updates them dynamically. The Policy Decision Point (PDP) evaluates access requests. The Policy Enforcement Point (PEP) implements authorization decisions at the device level. Additional parts, such as the Policy Information Point (PIP) and Policy Refinement Point (PRP), collect contextual information and adapt policies in real time using artificial intelligence or analytics. Together, these modules create a scalable framework that supports context-awareness and collaboration in complex IIoT ecosystems [5].

Several access control models have developed to address the specific needs of IIoT. Traditional frameworks like Discretionary Access Control (DAC) and Mandatory Access Control (MAC) established the foundation for modern authorization systems but tend to be too rigid or centralized for distributed industrial operations. Role-Based Access Control (RBAC) introduced the idea of assigning permissions to roles instead of individuals, which suits hierarchical industrial structures and SCADA systems. Despite its efficiency, RBAC struggles with real-time changes and cross-domain interactions. Attribute-Based Access Control (ABAC) offers more flexibility by basing decisions on attributes describing users, devices, resources and environmental factors. ABAC supports detailed, context-aware policies, but its need for continuous policy evaluation can put pressure on resource-limited IIoT nodes .

To address these issues, researchers have suggested more decentralized models, most notably the Capability-Based Access Control (CapBAC) model. In CapBAC, the owner of a device issues a capability token, a cryptographically protected object that contains the rights granted to a subject. A subject can only interact with a device if it shows a valid token specifying the allowed operation and the corresponding resource [5]. Unlike RBAC or ABAC, CapBAC does not require a centralized decision point. This feature makes it especially suited for distributed IIoT environments, where each node can independently validate capabilities. However, as demonstrated in the work of Nakamura et al. (2020) [7], improper capability delegation can create illegal information flows between devices. For example, a subject allowed to access sensor data through an intermediary device might unintentionally allow another subject to retrieve that data without explicit authorization.

To prevent such violations, Nakamura and colleagues proposed the Operation Interruption (OI) protocol. This protocol adds an extra layer of monitoring for data paths. It defines relationships between devices in terms of legal and illegal information flows. A legal flow happens when a subject is authorized to access all upstream data sources from which the requested information originates. An illegal flow emerges when data travels through devices or subjects not included in the authorized access chain. The OI protocol stops any operation that would cause such a flow, effectively blocking the transaction before the data breach occurs. This mechanism adds an information-flow control layer to access control, connecting traditional authorization with data-centric security enforcement [7].

Building on these advancements, blockchain-based CapBAC systems have been developed to eliminate trust issues in distributed environments. By recording capability tokens and access transactions on an unchangeable ledger, blockchain increases transparency, traceability and accountability while preventing single points of failure [6]. Additionally, risk-based access control mechanisms have emerged to adjust permissions dynamically based on the assessed trustworthiness or behavior of each device. This approach is particularly useful in IIoT scenarios where operational conditions and security levels continuously change [5].

The progress in access control in IIoT shows a shift from static and hierarchical architectures to flexible, decentralized and information-driven models. Combining CapBAC with technologies such as blockchain, artificial intelligence and the OI protocol represents a significant step toward self-managing authorization frameworks that can secure industrial operations on a large scale. The next step in this discussion concerns Information Flow Control (IFC), which extends access control by regulating how data move and are protected across interconnected industrial systems.

2.4 Information Flow Control (IFC) and Security Dependencies

In IIoT, security is not only concerned with who has permission to access data or take actions but also with how information travels once access has been granted. This aspect of security is known as Information Flow Control (IFC), focuses on supervising and constraining data propagation between entities. While access control ensures that a subject has authorization to interact with a specific object, IFC ensures that the resulting data flows remain within proper limits. This concept is crucial in IIoT environments where physical and cyber systems coexist, and data from sensors, actuators, and controllers constantly flows through various industrial subsystems [8], [9].

Traditional access control models are static and object-centric, offering no protection once a transaction has been authorized. In contrast, IFC introduces a data-centric view. Each piece of information is assigned a security label that defines the level of sensitivity, confidentiality, or trust associated with it. Information flows are allowed or denied based on set flow policies that evaluate whether data can legally move from one entity to another. A flow is defined as legal if it follows these security labels and illegal if it violates them. Through this framework, IFC enforces the principle of non-interference, ensuring that information from a high-security domain cannot influence the behavior or state of a lower domain [8].

In IIoT, data transmission is multi-hop and dynamic, involving devices that frequently change roles between data producers and consumers. This variability requires IFC mechanisms capable of tracking flows across distributed nodes. Modern IFC architectures use graph-based representations to describe how data move through networks. In these models, devices and services are represented as nodes, and directed edges indicate dependencies or data exchanges. Each edge can include parameters such as latency, criticality, or trust level. This approach allows security engineers to formally define which flows are acceptable and automatically detect paths that violate security policies [10], [11].

A practical realization of information flow control in IIoT can be seen in capability-based access control models that incorporate information flow restrictions into their operational logic. Building on the CapBAC model, these designs improve traditional access control by embedding flow rules directly into capability tokens. Each capability not only defines which operations a device is allowed to perform but also specifies the permitted directions of data exchange, such as from which sources data can be collected and to which destinations it may be transmitted. In this way, every operation carries flow constraints that dictate how data propagate through the network. For instance, a control device may be authorized to collect measurements from sensor A and forward the results only to a specific supervisory system B. These built-in flow definitions transform capabilities from static authorization credentials into active mechanisms that enforce compliance with established flow policies during runtime [8].

Despite their efficiency, capability-based access control mechanisms can still lead to unintended information flow in complex IIoT layouts. Hybrid devices that act simultaneously as sensors and actuators may unintentionally become channels for data transfer between otherwise unrelated subsystems, creating illegal information flows. To mitigate this issue, enhanced capability-based frameworks integrate runtime monitoring mechanisms capable of detecting and interrupting unauthorized transmissions. One such mechanism is the Operation Interruption (OI) protocol, which continuously evaluates data transfer operations (such as read, write, or transmit) against the system's dependency graph. If an operation would generate an unauthorized flow, the OI protocol immediately halts execution before any data leave the originating node. This proactive validation process is crucial in latency-sensitive IIoT environments, where even brief illegal flows may compromise operational integrity or data confidentiality [8].

While IFC initially focused on enforcement between individual devices, recent developments have extended its application to larger industrial infrastructures through risk-based analysis. In these approaches, IIoT systems are modeled as dependency graphs, where nodes represent assets and edges represent the direction and strength of information or control dependencies. Each edge is evaluated based on factors such as probability of misuse, potential impact, and dependency criticality. The result of this assessment produces an illegal flow risk metric, which identifies network areas with high vulnerability to unauthorized propagation [10].

By quantifying risk in this manner, IFC becomes a predictive instrument that helps administrators allocate resources efficiently and revise flow policies dynamically.

An important contribution to this field is the modeling of multi-order dependencies, which consider indirect or transitive relationships between IIoT components that can increase risk. In large industrial networks, a compromise in one subsystem can affect several others through chains of dependent interactions. Graph-theoretical methods, such as centrality and connectivity analysis, are used to measure the influence of each node in the propagation of information. Nodes with high centrality values (like gateways, edge servers, or control aggregators) represent critical points where an illegal flow could lead to severe consequences for the entire system. Identifying these components allows for more targeted mitigation strategies, reducing the probability of cascading failures [11].

At a higher conceptual level, IFC also involves studying security dependencies, which describe the logical and operational relationships among assets that rely on each other to maintain secure operations. In IIoT systems, dependencies extend beyond direct data exchange. They include trust relationships, shared configurations, and synchronized operations. For example, a manufacturing execution system may rely on accurate readings from sensors in upstream stages, while those sensors depend on consistent control signals from programmable logic controllers (PLCs). A failure or compromise in any of these links can disrupt the flow of trustworthy information, propagating insecurity across the entire production chain [11], [12].

To manage such dependencies effectively, IFC frameworks incorporate trust management and dependency-aware modeling, where each device or subsystem maintains a dynamic trust score based on its operational history, reliability, and compliance with policies. This allows the system to adjust flow permissions according to the current trustworthiness of nodes, creating a self-regulating defense mechanism. Dataflow management frameworks further extend this capability by integrating sensing, control, and feedback mechanisms that continuously assess how information moves and how dependencies change over time. This combination of IFC and dataflow management principles establishes the foundation for resilient and adaptive IIoT architectures capable of maintaining secure operation despite dynamic conditions [9], [12].

In summary, Information Flow Control transforms IIoT security into a continuous, data-centric process where the legality, trust, and risk of every information exchange are evaluated dynamically. By combining micro-level enforcement through protocols such as OI with macro-level risk and dependency modeling, IFC provides a comprehensive theoretical framework that safeguards industrial systems against unauthorized propagation of data and cascading security failures. This holistic approach naturally leads toward the integration of blockchain-based mechanisms for immutable logging and trust verification, which represent the next step in achieving traceable and tamper-resistant information governance, as explored in the following section.

2.5 Blockchain Fundamentals

Blockchain technology is one of the most significant developments in distributed computing. It offers a decentralized and tamper-resistant method for recording and verifying digital transactions. At its core, a blockchain is a distributed ledger that keeps a growing list of ordered records, known as blocks, which are linked together using cryptographic techniques. Each block contains a cryptographic hash of the previous block, a timestamp, and a set of validated transactions. This structure ensures immutability, as any modification to a block would change its hash, making all following blocks invalid and alerting the network to potential tampering [13].

The operation of a blockchain depends on the peer-to-peer (P2P) network model. In this model, each node has a copy of the ledger and participates in the validation of new transactions. This decentralization eliminates the need for a central authority and distributes trust across all participants in the network. Every transaction is verified collectively through mathematical consensus, ensuring that all nodes agree on the current state of the ledger. This mechanism guarantees transparency, auditability, and non-repudiation, as every participant can trace the origin and history of recorded data [13], [14].

2.5.1 Blockchain Architecture and Structure

From a structural viewpoint, blockchain systems are typically organized in layers: the data layer that stores blocks and transactions, the network layer responsible for communication between nodes, the consensus layer where agreement on the ledger's state happens and the application layer that supports decentralized applications and smart contracts. Each block is divided into two primary components: the block header, which has metadata like the previous hash and timestamp, and the block body, which list the confirmed transactions. These transactions are organized in a Merkle Tree, a binary hash tree structure that allows for efficient verification of data integrity. The root of the Merkle Tree is in the block header, allowing nodes to verify a transaction's inclusion without accessing the entire dataset, thus improving efficiency and scalability [13].

The combination of hashing, timestamping, and Merkle trees establishes the core properties of integrity and immutability in blockchain. Since every block references the hash of its predecessor, any attempt to change data in a previous block would change all subsequent hashes, making tampering computationally infeasible. In distributed operation, simultaneous block proposals may temporarily create forks or competing branches of the ledger. Canonicality is restored using the longest-chain rule, where nodes adopt the branch with the greatest accumulated work (or stake/weight, depending on the consensus). Orphaned blocks are discarded during this process. This cryptographic linkage and eventual consistency create a continuous chain of trust, where each addition to the ledger is verifiable and permanent [13], [14].

2.5.2 Cryptographic and Security Foundations

The strength of blockchain comes from using asymmetric cryptography, especially public–private key pairs and digital signatures. Each participant has a private key to sign transactions and a public key for others to verify their authenticity. In practice, transactions link public-key addresses to signed transfer or state-update messages: a participant produces a signature over the transaction payload with the private key, and peers validate it with the matching public key. Addresses are derived from public keys through cryptographic hashing, enabling verifiable ownership without revealing real-world identities. Additionally, hash functions like SHA-256 provide one-way cryptographic transformations that generate unique outputs for given inputs, ensuring data integrity and preventing forgery [14].

Blockchain security also depends on the concept of distributed consensus, which prevents malicious actors from manipulating the ledger. Unlike traditional centralized systems that trust a single authority, blockchain distributes verification power across multiple nodes. Even if some nodes act dishonestly, the system maintains integrity as long as the majority follow the agreed rules. This decentralization of verification is the foundation of trustless trust, where participants can rely on the system's mathematical guarantees rather than on institutional intermediaries [13].

2.5.3 Consensus Mechanisms

Consensus mechanisms define how nodes in a distributed blockchain network agree on the validity of transactions and the order of blocks. The earliest and most well-known protocol is the Proof of Work (PoW) mechanism, in which participants, called miners, compete to solve complex cryptographic puzzles. In PoW systems, miners change a nonce (a one-time number in the block header) to find a hash digest below a difficulty target. Adjusting this target controls the block production rate and security, while verification remains computationally inexpensive. Although PoW provides strong security through computational difficulty, it uses a lot of energy and can be slow due to its heavy resource demands [13].

To address these issues, alternative consensus mechanisms such as Proof of Stake (PoS) were developed. In PoS, validation power is based on the amount of cryptocurrency or stake held by a participant, using economic commitment instead of energy consumption to build trust. PoS offers better energy efficiency and transaction throughput while reducing the risk of centralization associated with mining-based systems. A further development, Delegated Proof of Stake (DPoS), adds a democratic voting process. Token holders elect a limited number of trusted validators who produce and verify blocks for the network. This method improves performance and governance flexibility while maintaining security and decentralization [13].

Recent blockchain systems also use Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) algorithms, especially in permissioned or consortium networks. These consensus schemes focus on speed and reliability over full decentralization, making them suitable for enterprise and industrial environments where participants are known and partially trusted [14].

Each consensus protocol represents a trade-off between scalability, energy efficiency, security, and the level of decentralization. This balance is an essential area of research domain in blockchain theory.

2.5.4 Smart Contracts and Programmable Logic

A major evolution in blockchain systems came with the introduction of smart contracts, self-executing programs that automatically enforce rules and conditions encoded within the blockchain. These contracts are stored and executed on the distributed ledger, ensuring that once conditions are met, the specified actions occur without human involvement. Smart contracts extend blockchain functionality from simple transaction recording to programmable logic. They enable the automation of agreements, workflows and system governance. Their deterministic execution provides transparency and trust while reducing the need for third-party enforcement [14].

Smart contracts constitute the foundation of Blockchain 2.0 and beyond. They transform blockchains from passive data registries into autonomous computing infrastructures. They provide the flexibility to embed business logic directly into the blockchain, paving the way for decentralized applications (DApps) and token-based ecosystems. As blockchain architectures continue to change, new concepts like Blockchain 3.0 emphasize interoperability, scalability and integration with new technologies, including AI and edge computing. These advancements aim to achieve seamless coordination among distributed systems while keeping the blockchain's key qualities of integrity and transparency [14].

2.5.5 Advantages and Limitations

The main benefits of blockchain technology come from its ability to guarantee immutability, transparency, traceability and decentralized trust. Every transaction recorded on the ledger is cryptographically secured and permanently auditable. The distributed architecture eliminates single points of failure and enhances resilience against internal and external attacks. Additionally, blockchain promotes accountability by keeping a complete, chronological record of all network activities [13], [14].

However, blockchain has its limitations. Consensus algorithms such as PoW face scalability and energy efficiency challenges. PoS and DPoS require mechanisms to prevent validator collusion or stake centralization. The storage requirements grow as the ledger expands over time, creating challenges for devices with limited resources. Additionally, delays caused by consensus processes can interrupt real-time operations. These issues continue to drive research into lightweight, scalable, and hybrid blockchain architectures, seeking to balance performance, decentralization and security [13].

2.5.6 Blockchain Types

Blockchains are commonly categorized as permissionless, permissioned and consortium systems. In permissionless networks, anyone can read and propose blocks, and open consensus (e.g., PoW/PoS) secures the ledger against adversarial conditions. Permissioned systems restrict writers to verified members and often employ Byzantine-fault-tolerant consensus (e.g., PBFT, PoA) to achieve low latency and predictable finality. Consortium chains are managed by multiple organizations, combining selective participation with shared auditability and collaborative governance. Each model has different trust assumptions, performance characteristics and governance properties that shape the ledger's security and operational profile [14].

2.6 Blockchain Applications in IIoT Security

The integration of blockchain technology into the Industrial Internet of Things (IIoT) represents a significant change in how security, trust, and data integrity are achieved in industrial systems. As an extension of the principles discussed previously, blockchain offers a decentralized and tamper-resistant framework that protects data, manages access and maintains accountability among different industrial entities. Through its unchangeable ledger and consensus-based validation mechanisms, blockchain removes the need for centralized authorities and enables autonomous cooperation among IIoT devices.This ensures transparency, integrity and resilience in crucial environments [15].

In IIoT infrastructures, data security requirements extend beyond encryption to include real-time integrity checks, traceability and dynamic access control. Blockchain satisfies these requirements by validating and permanently recording every data exchange or operational event through cryptographic methods. This unchangeable record guarantees the source and authenticity of data, making it possible to verify the sensor data and control commands at any time. Furthermore, decentralized consensus protocols prevent unauthorized modification or deletion of records, reducing the single points of failure that traditionally characterize centralized architectures [15], [16].

A key application of blockchain in IIoT is its role in distributed access control and authentication. Traditional Role-Based or Attribute-Based Access Control mechanisms depend on central servers that process authentication requests. This can lead to delays or vulnerabilities. In contrast, blockchain enables policy enforcement through smart contracts, which automatically carry out authorization rules on the ledger. Access permissions, revocation conditions and context-aware constraints are included in these contracts, offering a secure and verifiable way for managing trust relationships. This decentralized approach boosts security while improving transparency and operational efficiency, as every action is verifiable across the network [17].

Blockchain also significantly helps with data integrity and privacy preservation. By storing cryptographic hashes of sensor outputs and event logs, it quickly identifies any unauthorized changes. Even when large data sets are stored off-chain for scalability, on-chain verification keeps data consistent and authentic. Combining blockchain with Zero Trust security models and AI-driven anomaly detection improves the ability of IIoT systems to identify and respond to threats such as Distributed Denial of Service (DDoS) and data manipulation attacks in real time. This combination creates a security framework that protects information and adjusts to new threats as they arise [15].

Another critical advantage is traceability and accountability throughout the industrial lifecycle. Each step, from raw material sourcing to production and distribution, can be logged as a chain of immutable transactions. This allows stakeholders to trace every asset’s history, verify compliance, and ensure transparency in manufacturing and logistics. Blockchain-based traceability minimizes counterfeiting, improves regulatory adherence and reinforces trust among supply-chain participants [16].

Emerging IIoT architectures are increasingly incorporating blockchain into edge and cognitive networks, especially in 6G-enabled environments. In these systems, blockchain acts as the core trust and coordination layer, managing device authentication, spectrum access and communication security. Through consensus-driven synchronization, devices can negotiate resource allocation and maintain secure connections, even in highly dynamic environments. This shows how blockchain can extend its capabilities beyond data protection to support independent and adaptable trust management in next-generation industrial networks [16].

Despite its potential, blockchain implementation in IIoT still faces challenges related to computational load, latency, and scalability. Consensus algorithms such as Proof of Work or certain Proof of Stake variants require considerable energy and processing power, often more than what industrial edge devices can handle. To overcome these challenges, research emphasizes lightweight, permissioned and consortium blockchain architectures optimized for IIoT environments. Such systems work with known participants and use efficient consensus methods like Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA), which reduce overhead while preserving trust and transparency. Combining blockchain with edge computing and off-chain processing further improves throughput and responsiveness, making blockchain a practical foundation for real-time industrial operations [15], [17].

In summary, blockchain establishes the structure and operations needed for secure, transparent and decentralized IIoT ecosystems. Its distributed nature ensures tamper-proof data integrity, independent access control and verifiable accountability across all industrial layers. As IIoT infrastructures advance toward greater autonomy and interconnectivity, blockchain emerges as a key technology that enables trustworthy collaboration among machines, networks and humans. The merging of blockchain with artificial intelligence, Zero Trust models and edge computing establishes the theoretical groundwork for self-securing, adaptive and resilient IIoT systems that define the future of Industry 4.0 and beyond [15], [16], [17].

3. Related work

Industrial Internet of Things (IIoT) environments need secure and reliable ways to control data access and manage information exchange between connected devices and systems. The distributed and dynamic nature of industrial infrastructures makes traditional centralized access control methods and static security policies insufficient. Recent research has explored blockchain-based access control, secure data exchange mechanisms, fuzzy logic–based risk assessment and incentive-driven approaches in order to improve security, trust and cooperation in IIoT systems.

A representative blockchain-based access control solution was proposed by Usman et al., who introduced a scalable domain access control framework for IIoT environments [18]. Their approach uses Hyperledger Fabric to implement a permissioned Role-Based Access Control (RBAC) model. In this model, devices, roles and access policies are registered and enforced through smart contracts. By dividing the IIoT system into multiple policy domains, the framework improves scalability, decentralization and traceability compared to centralized options. Experimental results showed less computational overhead than Attribute-Based Access Control (ABAC). However, the framework mostly focuses on authorization management and does not account for the risks of dynamic information flow or the long-term adaptation of device behavior.

In addition to access control, blockchain has been used for secure data exchange in IIoT environments. Liu et al. proposed a blockchain-based data exchange method to prevent data leakage, tampering and unauthorized access [19]. Their framework combines Public-Key Encryption with Keyword Search (PEKS) to allow encrypted data retrieval. It utilizes Zero-Knowledge Proof of Knowledge and Pedersen commitments to protect privacy during authorization. Smart contracts manage access rights and enable auditing. While this approach strengthens confidentiality and decentralized trust, it does not analyze how information flows move through interconnected components or how repeated risky behavior affects system security over time.

To address uncertainty in security assessment, several studies have applied fuzzy logic to IIoT risk analysis. Kerimkhulle et al. introduced a fuzzy logic model for assessing information security risks by combining the likelihood of threats with their potential impact [20]. Their approach considers asset importance, existing security controls, previous incidents and possible financial or reputational damage. This allows for more flexible risk estimation than traditional quantitative models. While effective in managing uncertainty, the model emphasizes on risk evaluation and does not define automated enforcement or incentive mechanisms.

Similarly, Atlam et al. suggested an adaptive risk-based access control model that merges fuzzy logic with expert judgment to dynamically evaluate access requests in IoT environments [21]. The model evaluates contextual parameters such as location, time, data sensitivity, action severity and user behavior history to generate real-time risk scores. Smart contracts monitor behavior during access sessions. While the model is adaptive and context-aware, it mainly supports access decision-making and does not address information flow dependencies or continuous behavior regulation.

In addition to risk-aware access control, incentive-based methods have been proposed to promote secure and cooperative behavior in IIoT data-sharing scenarios. Sohail et al. presented a blockchain-enabled incentive-driven framework that combines cryptographic methods with game-theoretic incentive distribution to support fair and secure industrial data sharing [22]. Smart contracts automate participant registration, authentication and reward distribution, encouraging participants to contribute high-quality data. Despite its success in promoting cooperation, security risk is treated as an implicit factor and is not directly derived from information flow analysis.

Another relevant research area combines blockchain with federated learning for secure analytics in IIoT environments. Zhang et al. proposed a blockchain-based federated learning framework for device failure detection. This allows industrial participants to collaboratively train models without sharing raw data [23]. Blockchain commitment ensures data integrity and auditability, while smart contracts provide incentives based on data input. Although this approach supports privacy-preserving collaboration, it focuses on machine learning processes rather than on enforcing information flow security policies.

Overall, the existing literature shows that there has been significant progress in blockchain-based access control, secure data exchange, fuzzy risk assessment and incentive mechanisms for IIoT systems. However, most approaches examine these elements separately. Risk assessment is often treated as a monitoring activity, access control decisions are usually static or transaction-based and incentive mechanisms are usually not directly linked to security-related behavior. Consequently, identified security risks do not always lead to clear or consistent consequences for system components.

The approach followed in this work addresses this gap by connecting information flow risk directly to system behavior in a simple and structured way. Instead of analyzing security events in isolation, the method continuously considers how information moves between nodes and how risky this behavior is over time. Fuzzy logic helps analyze these risk indicators gradually, avoiding strict yes-or-no decisions. Based on this interpretation, nodes receive proportional rewards or penalties that affect their future participation in system operations. Enforcement and incentive actions are applied automatically through a decentralized mechanism, ensuring transparency and consistency. This approach combines security assessment, decision-making and enforcement into one process that encourages safer behavior, gradual adaptation and long-term compliance in Industrial Internet of Things environments.

4. INFFLOW-RT: Risk-Based Real-Time Analysis of Illegal Information Flows in IIoT

This chapter presents the INFFLOW-RT methodology, which was originally proposed in [24], and provides an explanatory and structured description adapted to the context of this thesis.

4.1 Overview and System Modeling

Industrial Internet of Things (IIoT) environments involve continuous interaction between various components, such as sensors, controllers, gateways and software services. Access control mechanisms determine if an entity can perform a specific operation, but they do not fully address how information spreads once access is granted. In complex industrial systems, information can travel through multiple components through indirect paths, creating security risks that are difficult to detect with traditional authorization models. INFFLOW-RT addresses this issue by offering a risk-based and real-time methodology for analyzing illegal information flows and their propagation across interconnected IIoT systems.

INFFLOW-RT models an IIoT environment as a directed dependency graph. The nodes in the graph represent system objects like devices or services, while the directed edges show how information flows between these objects. A key aspect of this methodology is the distinction between information flows and transactions. An information flow represents a logical data dependency between two objects. On the other hand, a transaction refers to a specific event of data exchange, such as a read or write operation. This distinction helps the methodology capture both the structural properties of the system and the dynamic behavior observed during operation.

An important feature of the model is that it explicitly considers dependencies. First-order dependencies describe direct information exchanges between objects. However, in real IIoT infrastructures, information often moves through chains of intermediate components. These higher-order dependencies are essential for understanding risk propagation, as illegal behavior at an upstream node can indirectly affect downstream components that do not directly interact with the original source. By modeling these multi-order dependencies, INFFLOW-RT enables system-wide analysis of how illegal information flows might spread across processes and services.

4.2 Transaction-Based Risk Estimation and Real-Time Updating

To measure the security implications of information flows, INFFLOW-RT uses a small set of transaction descriptors that capture the context and potential impact of each data exchange. These descriptors work together to provide structured input for the risk estimation process. By assigning simple numerical values to qualitative security properties, the methodology allows for consistent comparisons between various transactions without adding unnecessary complexity.

Table 1 summarizes the three core descriptors used to characterize transactions: severity, operation factor and legality. Each descriptor captures a different aspect of security relevance. Severity shows the importance of the data involved. The operation factor expresses the potential impact of the action performed and legality shows the compliance with the defined access and flow policies. Together, these metrics allow INFFLOW-RT to tell the difference between low-impact routine operations and events that might pose a serious threat to system integrity.

Metric	Description
Severity	Sensitivity or importance of the data involved
Operation factor	Impact of the performed operation
Legality	Level of compliance with security policies

Table 1: Transaction metrics used in INFFLOW-RT

Severity values are based on the category of data being exchanged. As shown in Table 2, data that directly affect system configuration or control logic are viewed as more critical than auxiliary or informational data. This distinction is important because unauthorized access to configuration data can cause cascading failures, while exposing non-critical data typically has limited impact. The exact numeric values are illustrative and can be adjusted to fit the deployment scenario, but the ordering reflects increasing security sensitivity.

Data category	Severity
Acknowledgement data	1
Customer data	2
Billing & pricing data	3
Sensor data	4
Configuration data	5

Table 2: Severity values based on data category

In addition to data sensitivity, the type of operation performed also affects risk. Table 3 shows the difference between read and write operations by assigning a higher operation factor to write actions. This reflects that write operations can change system's state and affect downstream components, while read operations mainly provide information without altering behavior. By including this distinction, INFFLOW-RT assigns higher potential impact to transactions that can actively change the system.

Operation Type	Factor
Read	2
Write	3

Table 3: Operation factor values

The legality descriptor captures whether a transaction follows the defined policies and information flow rules. As shown in Table 4, transactions are classified into categories ranging from fully legal to clearly illegal or impossible. Higher legality values correspond to more serious violations. This classification allows the methodology to treat repeated illegal writes as stronger evidence of risky behavior compared to occasional suspicious reads. Importantly, legality values do not enforce decisions directly. Instead, they serve as probabilistic signals used in risk estimation.

Transaction class	Legality value
Legal read/write	1
Illegal read	2
Illegal write	3
Suspicious read	4

Transaction class	Legality value
Impossible write	5

Table 4: Transaction legality classes

These three descriptors serve as input to the real-time risk estimation process. Instead of producing a binary decision, INFFLOW-RT combines them with probabilistic updating to estimate how likely it is that a given information flow displays illegal behavior. This estimation changes over time as new transactions are observed.

The real-time aspect of INFFLOW-RT is achieved through Bayesian updating, which allows the likelihood of illegal information flow to be revised dynamically. An initial probability derived from historical data is updated whenever new evidence appears. To ensure stability in cases where data are sparse or illegal events are rare, Laplace smoothing is applied to prevent probability values from dropping to zero or one too quickly. This design allows for gradual adjustments to behavioral changes instead of abrupt risk fluctuations.

The result of this process is a Dynamic Risk value associated with each information flow. In the INFFLOW-RT methodology, the Dynamic Risk of a flow from object x to object y is defined as the product of the flow's total transaction impact and the dynamically updated likelihood of illegal information flow occurrence. Specifically, the Dynamic Risk is computed as:

$$R_{dyn}(x \to y) = TTI_{x\to y} \cdot D\_IIFL_{x\to y}$$

where $TTI_{x\to y}$ denotes the Total Transaction Impact derived from the transaction descriptors (severity, operation factor and legality) and scaled to the range [0,10], while $D\_IIFL_{x\to y}$ represents the Bayesian-updated posterior probability of illegal information flow occurrence.

For interpretation, continuous Dynamic Risk values are mapped to qualitative levels, as shown in Table 5. These levels do not represent strict thresholds for enforcement but provide a human-readable representation that supports monitoring, comparison and subsequent decision-making processes.

Risk range	Interpretation
[0,2)	Very low
[2,4)	Low
[4,6)	Medium
[6,8)	High
[8,10]	Very high

Table 5: Dynamic risk levels

By structuring transaction characteristics in this way and interpreting risk through gradual levels, INFFLOW-RT offers a balanced approach between analytical rigor and practical usability. The methodology allows security analysts to understand why a flow is considered risky and how this assessment evolves over time, rather than relying on opaque or static security indicators.

4.3 Risk Propagation and Structural Importance in IIoT Dependency Graphs

While transaction-level risk estimation provides useful insights into individual information flows, security risks in IIoT environments rarely remain isolated. In practice, information flows are part of larger operational processes where multiple components depend on each other for coordinated tasks. Therefore, INFFLOW-RT expands its analysis beyond direct interactions and evaluates how risk propagates through chains of dependencies. This perspective allows the methodology to capture system-level exposure rather than focusing on isolated events.

The concept of cumulative dependency risk comes from noticing that a component may become risky not because of its own actions. Instead, it can become risky because it relies on upstream information flows that repeatedly violate security or information flow control policies. As information passes through multiple nodes along a dependency path, the effects of illegal or suspicious transactions can build up. This increases the overall vulnerability of the dependent process. To model this behavior, INFFLOW-RT analyzes multi-order dependencies, which means it explicitly considers indirect relationships between system objects.

Let's define an information flow chain as $IF_0 \to IF_1 \to \cdots \to IF_n$, where each information flow depends on the previous one. According to the INFFLOW-RT methodology, the dependency risk of an illegal information flow chain is calculated by combining the likelihood of illegal information flows along the dependency path with the impact of the final transaction in the chain. The dependency risk of a chain of information flows is defined as:

$$Ch\_R_{IF_0,\ldots,IF_n} = D\_IIFL_{IF_0,\ldots,IF_n} \times TTI_{IF_{n-1},IF_n} = \left(\prod_{i=1}^{n} D\_IIFL_{IF_{i-1},IF_i}\right) \times TTI_{IF_{n-1},IF_n}$$

where $D_IIFL_{IF_0,\ldots,IF_n}$represents the combined likelihood of illegal information flows along the dependency chain and TTI_{IF_{n-1},IF_n} captures the impact of the final transaction between the last two objects.

In addition to dependency chains, the methodology also considers the structural importance of nodes in the information flow graph. Not all components contribute equally to risk propagation. Some nodes, such as gateways, aggregators or central controllers, hold key positions that many information flows pass through. Even moderate-risk behavior at these points can have a disproportionate impact on the system as a whole. INFFLOW-RT captures this aspect through graph-based centrality analysis, which identifies nodes whose position makes them critical for the propagation of information and consequently, for the spread of risk.

Specifically, the methodology uses normalized closeness centrality and Bonacich (eigenvector) centrality to evaluate node importance. Normalized closeness centrality measures how close a node is to all other nodes in the graph based on shortest-path distances. This helps identify nodes that can rapidly influence the rest of the system. Bonacich (eigenvector) centrality evaluates a node's influence by looking at its direct connections and the importance of its neighboring nodes. This makes it suitable for finding nodes involved in multiple high-risk dependency chains.

To add a security context, INFFLOW-RT introduces a risk-weighted graph centrality metric that combines structural importance with transaction-related risk. The risk-weighted centrality is defined as:

$$Risk - weighted\ centrality = Centrality \times TRiF$$

where *Centrality* corresponds to either normalized closeness or Bonacich (eigenvector) centrality and *TRiF* reflects the transaction risk factor derived from the type of transaction and the likelihood of illegal information flows.

By combining cumulative dependency risk with centrality-based indicators, INFFLOW-RT enables a system-oriented understanding of security risk in IIoT environments. This combined view supports prioritization by identifying not only which flows are risky, but also which components are most influential in amplifying or containing that risk. While these insights significantly enhance situational awareness and analytical depth, the methodology remains focused on assessment.

5. Incentive Mechanisms

5.1 Incentive Mechanisms in Cybersecurity and IIoT

In decentralized and large-scale environments such as the Industrial Internet of Things (IIoT), ensuring secure and cooperative behavior among different devices requires more than traditional cryptographic or policy-based security controls. Previous sections discussed how blockchain promotes integrity, transparency and decentralized trust, but these guarantees alone cannot motivate rational industrial entities to participate honestly in distributed security tasks. This issue leads to the concept of incentive mechanisms, which are designed to align the self-interest of autonomous nodes with the network's collective security goals. By embedding economic and reputation-based incentives into blockchain-enabled IIoT architectures, systems can encourage continuous cooperation, data sharing and compliance without relying on centralized enforcement [25].

Incentive mechanisms come from economic and game-theoretic principles that analyze how rational participants respond to rewards and penalties. In IIoT networks, devices and gateways act as autonomous agents with limited resources and potentially conflicting goals. Blockchain-based incentives create a self-regulating environment where each participant wants to contribute to the network's security and reliability. These mechanisms can be monetary, rewarding nodes with digital tokens for valid actions like data validation, intrusion reporting or threat detection. They can also be non-monetary, offering higher reputation scores, trust levels or priority access in industrial operations. Hybrid models combine both approaches, ensuring that resource-constrained devices can still be rewarded through lightweight reputation-based benefits [25].

The theoretical base of incentive mechanisms lies in game theory, which models strategic interactions among rational agents. Here, the goal is to design a system where all participants are better off cooperating rather than acting maliciously or selfishly. For example, mechanisms based on evolutionary game theory use adaptive reward and penalty structures that guide the system toward an evolutionary stable strategy (ESS), where cooperation becomes the leading behavior. In IIoT ecosystems, such models ensure that nodes involved in threat detection, data sharing or maintenance operations are continuously rewarded, while free-riders and non-cooperative nodes face penalties or exclusion from the network [26].

Blockchain plays a central role in the implementation of these mechanisms since it provides a transparent, tamper-proof and automated platform for incentive distribution. Smart contracts can define and execute incentive rules automatically, removing the need for trusted third parties. The blockchain ledger records every action (like data submission, verification or anomaly reporting), allowing fair and verifiable reward allocation. Smart contracts can also adjust incentive parameters based on network conditions, security performance or device reliability, ensuring that rewards match the levels of contribution. This adaptability is crucial in IIoT environments where resource availability, network load, and operational priorities are constantly changing [26].

Another emerging direction involves reputation-based incentive frameworks, where blockchain keeps unchangeable records of each node’s performance history. Reputation scores come from the quality and reliability of contributions and nodes with higher reputation receive priority in access to industrial services or higher reward rates. These systems strengthen trust and accountability while discouraging dishonest behavior. Inmore advanced setups, reputation and incentive models are combined with federated learning frameworks, allowing distributed devices to work together to train machine learning models for security analytics without exposing raw data. Nodes that provide accurate or energy-efficient updates are rewarded, while low-quality contributions reduce the participant’s reputation and future incentives. This method promotes security, privacy and efficiency which are essential for sustainable IIoT networks [27].

Incentive mechanisms also address important issues related to sustainability and scalability in industrial cybersecurity. Traditional centralized security management often suffers from low participation, high communication costs and limited motivation for continuous engagement. By introducing self-enforcing incentive structures, blockchain-driven IIoT systems turn passive devices into active participants in network defense and monitoring. Moreover, these mechanisms help balance resource use and performance. Participants invest computational or communication resources only when rewarded appropriately, creating a more energy-efficient and fair system.

Incentives thus bridge technical security assurance and behavioral compliance, enabling a defense model that aligns economic and operational motivations [25], [26], [27].

However, designing effective incentive mechanisms for IIoT security remains a challenge both theoretically and practically. Issues such as reward fairness, privacy preservation, collusion resistance and long-term sustainability require careful planning. Token-based systems must avoid inflation or centralization of power, while reputation-based systems must guard against false reporting and Sybil attacks. Additionally, incentive distribution has to be lightweight enough for limited industrial devices. Ongoing research explores hybrid approaches that merge monetary, trust and collaborative incentives, aiming for a balanced framework where cooperation, security and efficiency support each other.

In summary, incentive mechanisms are crucial for secure and trustworthy IIoT ecosystems. By merging blockchain transparency, game-theoretic reasoning and automated enforcement through smart contracts, these mechanisms turn security from a static policy into a dynamic, self-sustaining process. As IIoT networks move toward greater autonomy and interconnectivity, collaboration driven by incentives will become essential for maintaining resilient, adaptive and economically sustainable cybersecurity infrastructures [25], [26], [27].

5.2 Incentive Mechanisms methodologies

5.2.1 Game-Theoretic Incentive Mechanisms

Game-theoretic incentive mechanisms offer a strong framework for understanding strategic behavior among autonomous entities in decentralized IIoT environments. Unlike static incentive structures, these mechanisms show how nodes including sensors, edge devices, or validators react to rewards and penalties based on their logical decisions. By treating interactions as games, the system can predict how changes in incentive parameters affect individual strategies and overall network performance. This enables the design of incentive-compatible policies that promote cooperation, discourage free-riding and stabilize group behavior, even when devices have conflicting goals or different resource limitations. Within this wider range of methods, different game formulations including hierarchical, non-cooperative, evolutionary, or cooperative models, address specific IIoT requirements, offering flexible tools for connecting local decisions with global system goals.

5.2.1.1 Stackelberg Incentive Mechanisms

Stackelberg incentive mechanisms represent a hierarchical game-theoretic approach in which a key leader first sets an incentive policy, followed by rational followers choosing their strategies in response. This sequential decision structure works well with the operational patterns of IIoT environments, where coordination typically comes from industrial controllers, consortium operators or blockchain policy designers toward heterogeneous and resource-limited devices. In these situations, the leader announces reward rates, penalties or resource-allocation rules, while followers, usually sensors, edge nodes, validators or data contributors, optimize their utility based on factors like computational cost, energy use, storage needs or communication delays. The resulting equilibrium comes from backward induction, ensuring that the leader predicts follower reactions and selects incentive parameters that generate stable and system-optimal behavior [28].

A key advantage of the Stackelberg framework is its ability to account for external effects created by decentralized IIoT agents. In industrial networks, actions taken by a single device, such as generating too much data, creating network congestion or storage issues, impact overall system performance. Stackelberg-based incentive design allows the leader to incorporate pricing or reward changes that mitigate these external effects, guiding the network toward socially efficient outcomes. Typical hierarchical formulations have a multi-stage structure: the leader selects incentive rates, IIoT devices choose their participation levels or data generation behaviors and distributed processing or validation nodes allocate resources accordingly. The equilibrium of these systems usually corresponds to a subgame-perfect solution, where no participant benefits from acting alone, guaranteeing predictable and cooperative operation across the IIoT ecosystem [28].

Stackelberg incentives are also highly relevant in collaborative analytics and security-enhanced IIoT workflows. In these architectures, a coordinating entity, as the leader, sets incentive payments for devices that contribute security-related data, model updates or anomaly-detection features. Followers then evaluate whether participation is worthwhile, weighing energy limits, privacy issues, and local workloads against the offered rewards. The leader shapes this incentive mechanism as a bi-level optimization problem that considers learning accuracy, latency and resource efficiency, while followers adopt best-response strategies that reflect their local utility. This structure promotes ongoing participation from a wide range of IIoT nodes, improving the quality of distributed detection and enhancing the resilience of industrial processes [29].

Beyond learning-driven applications, Stackelberg formulations apply broadly to IIoT operations that depend on hierarchical decision making. Controllers or edge servers can set reward or pricing policies for activities like distributed sensing, data reporting, resource allocation or computation offloading, while devices respond based on their resource limits and operational priorities. By anticipating follower behavior, the leader can set incentive rules that achieve resource utilization, reduced energy consumption and ensure stable cooperation across devices with heterogeneous objectives and capabilities. Furthermore, when Stackelberg incentives combine with blockchain-based smart contracts, these mechanisms provide clear, tamper-proof and verifiable enforcement, boosting trust and operational strength within IIoT networks [28] [29].

5.2.1.2 Cooperative Incentive Mechanisms

Cooperative incentive mechanisms model IIoT devices as participants that can form alliances or coalitions to achieve benefits for all. In contrast to non-cooperative settings—where each device acts independently to maximize its own payoff, cooperative game-theoretic models allow devices to coordinate actions, share resources, and collectively improve the efficiency or security of the system. These mechanisms especially important in IIoT environments where nodes may benefit from joint sensing, collaborative anomaly detection, shared computation or coordinated security actions. By focusing on coalition formation, the system encourages devices to act in ways that increase overall benefits for the group rather than just individual rewards [30].

A key idea in cooperative incentive design is the formation of coalitions, where multiple nodes work together to complete tasks more efficiently. The total benefit of a coalition is based on the combined contributions of its members, and the incentive mechanism must define a fair method for distributing this payoff among participants. Methods like utility-based coalition evaluation and contribution-based reward sharing ensure that each device gets a share of the group reward that reflects its value. These processes support coalition stability by making sure that no subgroup has a stronger reason to leave the coalition, which keeps a stable collaborative framework that benefits the overall IIoT system [30].

Cooperative mechanisms often use fair allocation rules to distribute coalition benefits. A common example is the principle of rewarding members based on their marginal contribution to the coalition's total benefit. This maintains fairness and prevents free-riding behaviors, as devices that contribute more to performance, reliability or security receive higher rewards accordingly. When integrated with blockchain, these allocations can be automatically managed through smart contracts, ensuring that coalition rewards and penalties remain clear, verifiable and secure. Blockchain also guarantees the integrity of coalition decisions, enabling trust among devices that may belong to different administrative domains [30].

In summary, cooperative incentive mechanisms empower IIoT systems to take advantage of group coordination by linking rewards to shared goals. Through coalition formation, fair reward distribution and guarantee transparency with blockchain support, these mechanisms encourage stable and effective collaboration among diverse devices while boosting the reliability and resilience of industrial networks.

5.2.1.3 Non-Cooperative Incentive Mechanisms

Non-cooperative incentive mechanisms view IIoT devices as autonomous, self-serving agents that make decisions alone to maximize their individual payoff. In contrast to cooperative setups, where nodes form coalitions or share common objectives, non-cooperative methods assume that each device evaluates the cost and benefit of its actions in isolation. This view is especially relevant in large-scale IIoT networks with various nodes having different trust levels, resource limitations and operational priorities. Under these circumstanced, mismatched incentives can lead to selfish or malicious actions and the role of incentive design is to guide rational agents toward strategies that support the system's security and performance needs [31].

In non-cooperative game models, each IIoT node chooses between strategies like honest participation, partial compliance or malicious deviation. The interaction among nodes is represented as a strategic game where each participant's payoff depends on its own action and those of others. The system reaches a Nash equilibrium when no node can benefit by changing its strategy on its own. This feature is particularly useful for IIoT security, as it creates a stable behavioral state where honest participation is the most logical choice for self-interested entities. Therefore, incentive mechanisms are designed to modify payoff structures, either through rewards or penalties, so that honest actions are always preferable to harmful ones. By adjusting costs and benefits accordingly, the system encourages devices to remain compliant, even when they are not directly collaborating with others [31].

A fundamental component of non-cooperative incentive mechanisms is the use of penalty–reward structures that discourage harmful actions while encouraging positive behavior. In this model, nodes earn payoff based on the quality and reliability of their contributions. Honest nodes receive positive rewards, while nodes involved in deceptive or malicious activity face penalties that reduce their expected utility. This design makes malicious actions economically irrational. The mechanism evaluates each node's interaction history using a trust-based scoring system, which updates the perceived reliability of the node over time. Nodes with falling trust scores face penalties, reducing their motivation to participate dishonestly. Over repeated interactions, rational agents tend to adopt honest strategies because deviating results in lower rewards than following the rules [31].

Non-cooperative incentive models also provide a structured way to mitigate attacks in IIoT environments, such as data falsification, misreporting or resource exhaustion. Since nodes work independently, an attacker may try to maximize its own gain by exploiting vulnerabilities, sending false information or impersonating multiple identities. To address these actions, the incentive mechanism includes features like misbehavior detection, trust score adjustments and punishment coefficients. These elements ensure that repeated malicious actions rapidly reduce the attacker's rewards while honest nodes continue to be rewarded for reliable interactions. As the system progresses, malicious nodes become economically sidelined, reducing their impact and discouraging ongoing adversarial behavior [31].

The non-cooperative framework is particularly effective when integrated with blockchain-based enforcement. Blockchain guarantees transparency, immutability and verifiable execution of the incentive rules, making it impossible for nodes to manipulate payoff values or fake trust levels. Smart contracts enable penalty and reward adjustments ensuring that every strategic decision is reflected accurately in the node's payoff. This prevents centralized manipulation and guarantees that each agent responds only to the actual incentive structure of the game. Within IIoT systems, this leads to a self-stabilizing environment where rational behavior naturally aligns with security goals, even without cooperative effort among devices [31].

Overall, non-cooperative incentive mechanisms provide a mathematically grounded and behaviorally realistic approach for shaping how nodes behave in IIoT environments. By treating devices as independent, self-interested entities and creating payoff structures that reward reliable actions while penalizing malicious behavior, these mechanisms ensure stable and secure operation in varied and challenging environments. Their combination with blockchain technology strengthens trust and accountability, enabling IIoT networks to maintain resilient and self-regulating security features.

5.2.1.4 Evolutionary Incentive Mechanisms

Evolutionary incentive mechanisms use evolutionary game theory to understand how the collective behavior of IIoT entities changes over time due to shifting incentive structures, perceived risks, and past experiences. Unlike static or fully logical approaches, evolutionary models suggest that agents adjust their strategies gradually based on the payoffs they observe compared to the rest of the group. Through repeated interactions, strategies that lead to higher utility gain traction, while less effective behaviors fade. These dynamics are typically outlined through replicator equations, which describe how the proportion of agents adopting each strategy evolves according to payoff differences. As the process continues, the system may settle into an Evolutionarily Stable Strategy (ESS), a state that cannot be invaded by alternative behaviors and thus remains stable in the long run [32].

A significant advantage of evolutionary incentive mechanisms is their ability to model different IIoT environments where devices and operators differ in capabilities, goals and risk sensitivities. In these conditions, the success of a given incentive does not depend solely on its immediate payoff but also on how individual nodes perceive risk and evaluate trade-offs between cooperation and self-interest. Evolutionary frameworks capture these behavioral complexities by allowing agents to update their strategies based expected rewards, subjective risk assessments and limited rationality. As cooperation or non-cooperation becomes more or less advantageous relative to others, the prevalence of these behaviors adapts accordingly. Incentive mechanisms can thus be designed to influence these dynamics, increasing the relative payoff of desirable actions, like secure data sharing, anomaly reporting or participation in security analytics, until cooperative behavior becomes dominant [32].

These adaptive dynamics make evolutionary mechanisms particularly suitable for large-scale IIoT deployments. In these networks, devices frequently join and leave, environmental conditions change and threat landscapes change continuously. Rather than depending on fixed incentive parameters, evolutionary models support dynamic adjustment: rewards can be increased when cooperative behavior declines and penalties can be increased when non-compliance becomes more frequent. This feedback process continuously guides the population toward stable and cooperative behavior, enabling robust security even in highly dynamic industrial environments. The combination of replicator-based adaptation and incentive-driven payoff shaping ensures that the network eventually aligns with a stable cooperative equilibrium that promotes secure information flow and resilient system operation.

When paired with blockchain-based governance mechanisms, evolutionary incentive structures gain additional advantages. Blockchain enables tamper-proof tracking of behavior, verifiable reward distribution and clear enforcement of penalties, ensuring that the payoff structure guiding evolutionary dynamics remains trustworthy and consistent. This collaboration allows IIoT ecosystems to maintain long-term cooperative strategies grounded in both behavioral adaptation and secure incentive enforcement, creating a self-sustaining security model that remains effective as network conditions change [32].

5.2.2 Reputation-Based Incentive Mechanisms

Reputation-based incentive mechanisms are approaches where each device or node builds a dynamic reputation score. This score shows the quality, reliability and consistency of its past behavior. Unlike reward system based strictly on game theory or tokens, reputation-based systems focus on how trust evolves over time. They help IIoT infrastructures show the difference between cooperative, honest nodes and those that behave maliciously or opportunistically. These mechanisms are particularly effective in decentralized environments where devices share sensing data, participate in distributed learning or support security analytics and where a central authority is absent. This absence requires ongoing checks of each node's credibility. By linking rewards directly to reputation, the system encourages long-term honest participation and discourages short-term exploitation or free-riding [27].

A core element of reputation-based mechanisms is the use of a multi-factor reputation evaluation model. This model combines various behavioral indicators into one score. Typically, it considers factors like message accuracy, reporting frequency, communication reliability and the historical validity of the data from each node. Reputation values are updated dynamically based on local observations and aggregated feedback. This allows the system to account for recent actions while still considering long-term performance. To ensure resilience, reputation systems may use decay functions that gradually reduce the weight of outdated behavior. They can also use weighting schemes that balance the importance of different metrics like trustworthiness, stability, and the quality of past contributions [27]. In IIoT environments, where devices might change behavior due to resource limitations or external conditions, these flexible models offer a more realistic view of trust than static evaluation methods.

Reputation scores act as indicators of trust and influence incentive allocation. Nodes with high reputation levels are usually earn higher rewards, get priority for participation or enjoy reduce operational costs. On the other hand, nodes with low reputation may face penalties or get excluded from sensitive tasks. This creates a loop where honest, accurate, and efficient behavior is rewarded over time. In distributed learning and security analytics, reputation values can decide if a device is selected for model training, how its contributions are weighted in the aggregation process or whether its data is dependable for detecting anomalies. By linking reputation to real incentives, the system encourages devices to maintain high-quality contributions, improving accuracy, robustness and stability in IIoT security processes [27].

One notable advantage of reputation-based incentives is their ability to detect and reduce malicious or incorrect behavior without requiring significant computational overhead. Devices that frequently submit inaccurate, noisy or malicious inputs will see their reputation scores drop.

Consequently, their impact on critical processes decreases, protecting the network from attacks that could poison it or spread misinformation. Reputation mechanisms also help mitigate Sybil attacks since newly created identities cannot easily gain a long-term reputation. When combined with blockchain infrastructures, reputation updates gain additional integrity. Tamper-proof logs prevent manipulation of reputation scores, while smart contracts handle reward distribution and penalty enforcement automatically [27]. This combination boosts transparency, fairness and auditability, allowing reputation-based incentives to function reliably even in untrustworthy IIoT environments.

Through continuous evaluation, historical integration and rewards based on reputation, these incentive mechanisms promote sustainable cooperation and encourage trustworthy behavior across IIoT ecosystems. Their flexibility with different device characteristics and fit with decentralized architectures make them essential for long-term security in modern industrial networks. By encouraging accurate reporting, reliable participation and consistent compliance with security protocols, reputation systems significantly strengthen the resilience and integrity of IIoT infrastructures [27].

5.2.3 Token-Based Incentive Mechanisms

Token-based incentive mechanisms are a strong type of decentralized reward system where digital tokens serve as the primary economic driver. They motivate participation, ensure resource availability and maintain cooperative behavior across distributed infrastructures. In IIoT environments, where nodes vary widely in computational capacity, sensing accuracy, availability and energy resources, token incentives offer a flexible way to reward devices based on their contributions. Unlike reputation-based incentives, which emphasize behavioral trust, token mechanisms give clear and measurable value for activities like computation, data provision, anomaly detection or secure storage. This setup allows IIoT systems to create transparent and auditable reward frameworks that can scale across large networks without relying on centralized trust authorities [33].

In a token-based mechanism, nodes earn tokens by completing verifiable tasks that improve network’s reliability, security or performance. The underlying framework describes a comprehensive token-based economic model developed for decentralized storage systems providing a baseline for IIoT applications. In this model, devices receive token rewards based on the quantity and quality of resources they contribute, mainly storage capacity, uptime and the successful retrieval of stored objects. Rewards are calculated according to set smart-contract rules and adjusted for device availability, resource commitment and compliance with service-level expectations. This structure ensures that nodes with higher reliability or more consistent operations earn more tokens, encouraging stable and long-term participation [33].

A key aspect of token-based incentive mechanisms is dynamic reward scaling. This adjusts token payouts according to network demand, resource scarcity or service quality. In the model, reward rates change based on factors such as bandwidth use, data retrieval success or the current supply–demand balance of storage resources. These approach, often managed by exponential moving averages (EMAs) or similar adaptive pricing methods, prevents the oversupply of rewards and encourage participation where the network needs more resources. When applied to IIoT networks, this mechanism can be focus contributions during peak load conditions, emergency situations or periods when critical security tasks require extra computing power. In these cases, the elastic nature of token incentives allows the system to respond automatically to changing operational needs, keeping a balance between resource availability and network performance.

Another important part of token-based mechanisms is stake-based commitment. In this system, nodes must lock a specific amount of tokens as collateral before participating in specific operations. This reduces the chance of malicious actions since nodes risk losing a portion of their stake if they break service rules, submit false data or act against network policies. Penalties such as token slashing or forfeiture ensure economic disincentives against attacks like data withholding, inaccurate anomaly reporting or unreliable participation. In IIoT environments, where devices might differ widely in reliability and trustworthiness, staking creates a baseline of economic accountability, strengthening critical processes like sensor data collection or collaborative machine learning [33].

Token-based incentives also support quality-based reward differentiation. In the reference framework, nodes with higher uptime, faster response rates, or more accurate retrieval proofs receive extra reward bonuses. These "service-quality multipliers" can be applied directly into IIoT scenarios by providing higher rewards to devices that consistently offer availability, high-quality sensing or low-latency processing. In critical IIoT applications like industrial automation, fault detection and real-time monitoring, differentiating rewards ensures that devices providing the most valuable or urgent services are compensated appropriately, enhancing system-wide reliability and resilience.

The integration of token-based incentives with blockchain infrastructure improves transparency, auditability and security. Smart contracts automatically manage reward distribution, enforce penalties and maintain tamper-proof records of contributions and violations. This automation reduces the need for centralized management, mitigates conflicts and ensures that nodes cannot manipulate reward calculations or hide poor performance. For IIoT networks working across multiple administrative domains, where trust boundaries may be ambiguous, tokenized mechanisms create a universal economic layer that aligns incentives, reduces coordination friction and guarantees that all participating entities follow verifiable performance standards [33].

Collectively, token-based incentive mechanisms offer a flexible, economically grounded and cryptographically secure way to promote cooperation and efficiency in IIoT environments. By linking rewards to measurable contributions, dynamically adjusting token flows and using blockchain for enforcement, these mechanisms ensure sustainable participation and strong service delivery. Their adaptable design allows IIoT ecosystems to create differentiated and flexible economic policies, making token-driven incentive frameworks a key part of modern decentralized industrial architectures [33].

5.2.4 Auction-Based Incentive Mechanisms

Auction-based incentive mechanisms use competitive bidding processes to allocate tasks and resources efficiently in distributed IIoT environments. Unlike fixed-price or reputation-driven schemes, auction-based approaches determine rewards and assignments based on market dynamics. Here, devices show their willingness to participate by submitting economic bids. This approach works well for IIoT systems with different devices that vary in energy availability, computing power, sensing accuracy or communication quality. Auctions can adapt reward levels based on real-time supply and demand, providing a flexible method for incentivizing resource contribution, ensuring fairness and achieving efficient task distribution in dynamic operational conditions [34].

A common used model in these mechanisms is the double auction model. Devices submit a bid (bid value) representing the maximum cost they are willing to incur to complete a task, while the coordinating authority publishes an ask (ask value), defining the minimum reward offered. During the auction, bids are typically ranked from lowest to highest and asks from highest to lowest. A match happens when a bid value meets or exceeds an ask value. After this, a clearing price is set and the task goes to the device with the winning bid. This matching process ensures that tasks are assigned to devices capable of completing them efficiently, while the price reflects the real-time balance between available resources and network demand. Each node participates voluntarily only when the expected incentive is greater than their operational cost [34].

Auction-based mechanisms also focus on incentive compatibility, making sure that devices have no reason to misrepresent their capabilities or costs. Truthful bidding is encouraged through pricing rules inspired by second-price auctions or verification methods that check the feasibility of submitted bids. These rules prevent strategic manipulation like inflating bids for higher rewards or underbidding to win tasks that a device cannot perform reliably. In IIoT networks, where devices may have asymmetric or uncertain knowledge of each other’s capabilities these mechanisms help avoid task misallocation and promote strong cooperation. Devices that fail to fulfill awarded tasks may face penalties, such as reduced participation opportunities or enforced sanctions, strengthening system resilience [34].

A notable advantage of auction-based incentives is their fit for dynamic and real-time IIoT environments. Workloads and network conditions change often due to device mobility, intermittent connectivity or operational variability. Auction cycles can be executed periodically, allowing the system to update task assignments and reward structures based on current conditions rather than static or long-term assumptions. As device availability, energy reserves or sensing quality change, clearing prices and winning bids adjust automatically. This keeps the system adaptive and efficient across heterogeneous and evolving environments. It provides scalability and robustness without requiring centralized optimization or detailed knowledge of specific device constraints.

Combining auction-based mechanisms with blockchain technology enhances fairness, transparency and trust in IIoT settings. Smart contracts can automate the entire auction workflow, from bid submission and ranking to price clearing, reward distribution and penalty enforcement. This ensures that all participants follow the same verifiable rules. Because blockchain records are permanent, attempts to manipulate auctions or change outcomes are immediately detectable and discouraged. The combination of transparent bid logging and automated settlement promotes accountability, allowing IIoT networks to operate reliably even when participants belong to different organizations or industries [34].

In general, auction-based incentives provide a strong and flexible approach for aligning economic rewards with efficient resource allocation in IIoT ecosystems. Through competitive bidding, dynamic pricing, truthful participation and blockchain-backed enforcement, these mechanisms support fair and efficient coordination among various devices. As a result, auction-driven incentives represent an effective approach for managing cooperation and ensuring operational stability in large-scale, decentralized industrial environments.

5.2.5 Learning-Based Incentive Mechanisms

Learning-based incentive mechanisms are approaches where rewards are allocated based on the measurable learning contribution of each participating node. Instead of relying on static rules, economic bids or behavioral reputation, these mechanisms evaluate how much each device improves a shared machine learning model. This makes them particularly suitable for IIoT environments, where nodes often engage in distributed analytics, anomaly detection and privacy-preserving collaborative learning. By linking incentives to model quality rather than simple participation, learning-based incentive mechanisms encourage IIoT devices to provide meaningful, high-quality updates rather than minimal or noisy data [35].

The core principle of learning-based incentives is measuring each client's contribution through a clear learning contribution metric. This metric usually reflects how much a node's local training improves the global model, considering factors such as the magnitude of weight updates, the divergence between local and global parameters or the relative improvement in model accuracy. Here, contribution is computed using norms that measure how far a local model deviates from the global model before aggregation, resulting in a scalar contribution value for each participant. This allows the incentive mechanism to differentiate between nodes providing informative, high-quality updates and those whose gradients introduce noise or instability. Such a measure is objective, model-driven and difficult to manipulate, as it depends solely on the learning process rather than on self-reported metrics [35].

Smart contracts serve as a natural enforcement layer for learning-based incentives. By recording each node's contribution value on the blockchain, smart contracts can automatically compute rewards, apply penalties and maintain integrity in a secure manner. The reward distribution process becomes clear and auditable, ensuring that each device gets compensation in line with the value it adds to the learning task. Nodes that provide poor-quality updates, contribute malicious gradients or upload insufficient training results may receive reduced compensation or risk being excluded. On the other hand, nodes that consistently improve the global model earn higher rewards over time. The automation of these processes via blockchain removes the need for centralized scoring authorities and prevents fraudulent changes to contribution scores, enabling scalable and trustworthy incentive delivery across large IIoT deployments [35].

An important feature of learning-based incentive mechanisms is their resilience against malicious behavior in distributed learning systems. Since contributions are evaluated based on objective model improvement, devices that inject noise or manipulate gradients obtain low or negative contribution scores. This reduces their incentives and limits their influence on the aggregated model. This creates a natural defense mechanism: malicious nodes gain no economic benefit and have little effect on the learning process. Furthermore, this reward system adjusts to changing device performance or resource availability, as contributions are recalculated in each training round. IIoT devices can then adjust their participation according to their computational budget, while the system rewards them based on their actual impact on the learning process [35].

Learning-based incentive mechanisms are highly compatible with IIoT environments, where distributed analytics and federated learning are increasingly crucial for tasks like anomaly detection, predictive maintenance and cyber-threat monitoring. By incentivizing high-quality contributions, these mechanisms improve model accuracy, speed up convergence and reduce the burden of centralized data collection. Their integration with blockchain ensures that reward rules are clear, verifiable and resistant to tampering, allowing IIoT systems to coordinate learning across diverse organizational domains. In this way, learning-based incentives enhance other incentive classes, such as token-based, auction-based and reputation-driven schemes, by focusing on the core value of contributed intelligence rather than on external behavioral or economic factors.

In summary, learning-based incentive mechanisms provide a strong and adaptive approach to encourage high-quality participation in distributed IIoT learning tasks. By evaluating contributions directly within the learning process and using blockchain for incentive settlement, these mechanisms promote trustworthy collaboration and improve the effectiveness, resilience and security of industrial analytics systems.

6. Comparative Discussion of Incentive Mechanism Methodologies

6.1 Introduction

The incentive mechanisms presented in the previous chapter provide various strategies for regulating cooperation, discouraging malicious behavior and ensuring stable participation in distributed IIoT environments. Each method is based on different theoretical principles which include hierarchical game-theoretic structures and market-based or learning-driven reward models. Their effectiveness in industrial systems depends on how good they address common issues like scalability, diversity, coordination overhead and security threats.

This chapter offers a structured comparative analysis of these mechanisms. Instead of re-explaining how they work, it focuses on identifying their key similarities, differences and complementary roles in IIoT ecosystems. To achieve this, the analysis introduces a set of unified evaluation criteria that can be used to assess all mechanisms. These criteria create a consistent framework for comparison and highlight the trade-offs involved in choosing one incentive strategy over another.

6.2 Comparative Attributes for Evaluation

To enable a meaningful comparison among the studied incentive mechanisms, it is necessary to establish consistent evaluation attributes. IIoT environments have unique needs, such as low latency, device diversity, industrial safety requirements and high resilience to faults or adversarial actions. These needs impact how well each mechanism performs in practice. The attributes summarized below capture these requirements and serve as the basis for the following comparative analysis.

Attribute	Description
Coordination Overhead	Required communication, negotiation, or synchronization among nodes.
Rationality Assumption	Whether agents act individually, cooperatively, or under hierarchical control.
Fairness	How rewards are allocated and whether mechanisms support equitable distribution.
Security Robustness	Resistance to malicious behavior, manipulation, or strategic deviation.
Scalability	Performance as the network grows in size.
Adaptivity	Ability to respond to dynamic conditions or evolving agent strategies.
Blockchain Compatibility	Ease of on-chain automation and transparency.

Attribute	Description
IIoT Suitability	Fit for industrial workloads, constraints, and real-time requirements.

Table 6: Key Comparative Attributes for Incentive Mechanisms

These dimensions provide a balanced framework that captures both the theoretical and practical elements of incentive mechanisms. They are intentionally broad, reflecting the multidisciplinary nature of IIoT systems, which combine economic, behavioral, computational and security considerations. In the sections to follow, this framework will guide the comparison between methods and allow for the identification of overlapping characteristics, structural differences and potential synergies among the mechanisms.

6.3 Method-Comparison Similarity Mapping

Even though the incentive mechanisms analyzed in the previous chapter come from different theoretical frameworks, many share structural similarities when they are evaluated against the comparative dimensions introduced in Section 4.2. These mechanisms do not exist as isolated categories. They cluster around broader behavioral and operational principles. To illustrate they relate to one another, Figure 1 shows a compact representation of how the main mechanism families regarding their strategic structure, coordination needs and reward logic.

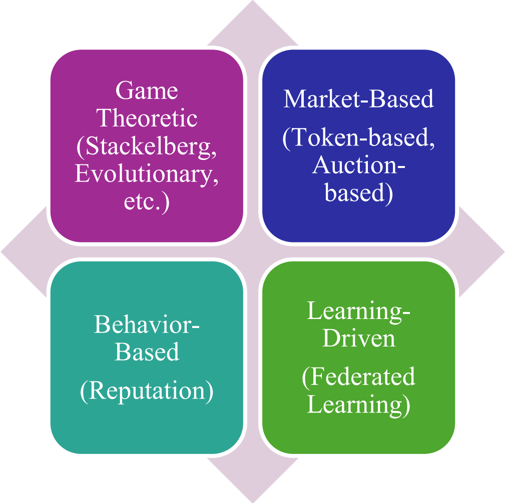
Game Theoretic (Stackelberg, Evolutionary, etc.)
Market-Based (Token-based, Auction-based)
Behavior-Based (Reputation)
Learning-Driven (Federated Learning)

Figure 1: Conceptual Clustering of Incentive Mechanism Families in IIoT

This high-level grouping shows that the game-theoretic mechanisms form a unified cluster based on strategic reasoning and equilibrium concepts. Token-based and auction-driven mechanisms lean towards market-centered incentive design, where behavior is influenced by prices, competition or programmable economic rewards. Reputation-based approaches align with behavioral assessment frameworks, while learning-based incentives occupy a unique position associated with informational contribution and model performance.

A comparison of game-theoretic and economic mechanisms shows that, despite their different origins, both significantly rely on self-interested behavior. In game-theoretic frameworks, this is expressed through strategic optimization, while in economic models it appears through price formation and competitive allocation. They differ in their coordination requirements: cooperative and Stackelberg models often need richer information exchange or explicit negotiation, while market-driven systems usually work through simpler transactions that can be automated by smart contracts. Still, both categories benefit from the transparency and verifiability that blockchain offers, which stabilizes expectations and reduces opportunities for manipulation.

The relationship between cooperative and non-cooperative mechanisms highlights another important contrast. Cooperative methods assume a willingness to align local decisions with collective well-being, leading to higher overall efficiency if participants can coordinate effectively. In contrast, non-cooperative methods assume that each agent acts independently, often under adversarial conditions. Nevertheless, both share a common foundation: they both model decision-making in terms of payoffs, both admit formal equilibrium concepts and both can operate without central authority when integrated into a distributed ledger environment. Their main difference is in robustness and coordination costs. Because non-cooperative mechanisms are generally lightweight and more resilient to misbehavior, while cooperative ones achieve greater efficiency at the price of higher coordination requirements.

Auction-based, token-based and reputation-based schemes share a different kind of connection. All three depend on observable behavior or verifiable contributions to determine rewards. They integrate easily with blockchain systems, which provide secure logging of bids, contributions or reputation scores. However, they differ in what aspect of behavior they prioritize: auctions reward successful bidding strategies, tokens reward participation and resource contribution and reputation mechanisms reward consistent reliability over time. Together, they form a family of mechanisms that are particularly suited for large-scale IIoT environments where transparency, low coordination overhead and scalability are crucial.

Reputation-based and learning-based mechanisms, while distinct, show a strong conceptual overlap. Both rely on behavioral evaluation, one using historical performance and the other using the quality of contributions assessed through model updates. They emphasize long-term accountability and benefit from blockchain-backed logging. Their main difference lies in computational cost: learning-based schemes require more processing power but can differentiating between high and low informational value in a way that reputation scores alone cannot.

Across these comparisons, certain patterns emerge. Strategic, market-based and behavioral mechanisms form three natural clusters, each addressing incentives from a different angle. Blockchain compatibility acts as a unifying feature, though economic and behavioral methods gain the most direct advantage, as their reward processes easily map onto smart-contract execution. Resilience to malicious activity varies greatly, with non-cooperative, reputation-based and learning-based models showing higher resilience than cooperative and market-driven ones.

Ultimately, these relationships show that incentive mechanisms in IIoT do not compete but complement each other. Effective system design often requires combining elements from multiple families to balance robustness, efficiency and scalability.

6.4 Shared Characteristics Across Mechanism Families

Although the incentive methods explored in Chapter 3 differ in theoretical origin and operational structures, several common characteristics emerge when viewed system-wide. These shared traits reflect the essential requirements of IIoT environments, where diversity, decentralization and resilience to misbehavior underlie any incentive-driven architecture. Studying these characteristics provides a unified view of the mechanisms and clarifies why multiple approaches often coexist or are combined in practice.

A first point of convergence is how incentives depend on quantifiable signals of behavior. Whether the mechanism evaluates an agent's payoff in a strategic game, the bid submitted in an auction, the token stake locked in a contract, the historical performance recorded in reputation systems or the accuracy in learning-based methods, the core idea is the same. Rewards must be based on observable, verifiable and preferably tamper-resistant indicators. In all cases, blockchain technology enhances this property by offering secure logging and automated enforcement, meaning that even mechanisms that were not originally designed for decentralization can gain significantly from integration in a ledger-based architecture.

Another shared feature is how these mechanisms deal with uncertainty and diversity, both of which are native to IIoT networks. Whether the uncertainty relates to device reliability, communication quality, task complexity or adversarial disruption, the mechanisms aim to guide individual behavior toward predictable patterns. Strategic models formalize this through equilibrium concepts, economic models through pricing and market clearing, reputation mechanisms through behavioral smoothing over time and learning-based schemes through refined contribution assessments. Despite their differences, all aim to create long-term stability in environments where no central authority can fully dictate behavior.

Additionally, most mechanisms show at least some level of decentralization. Even those that rely on hierarchical control, like Stackelberg formulations, can operate without centralized trust when the leader's policies are transparently recorded and enforced on-chain. Market-driven and behavioral mechanisms naturally fit into distributed settings, as their operations depend on local information and minimal coordination. The level of decentralization may vary, but the trend is similar: each mechanism attempts to reduce reliance on centralized decision-making while ensuring coherent system-wide behavior.

6.5 Consolidated Comparative Summary

The analysis in this chapter demonstrates that incentive mechanisms in IIoT systems differ not only in their mathematical or economic principles but also in the way they balance coordination cost, fairness, robustness and scalability under industrial constraints. While game-theoretic approaches provide structured strategic reasoning, market-based mechanisms provide transparent and scalable resource allocation and behavioral or learning-driven methods deliver detailed control over long-term system reliability. Therefore, these mechanisms forms a complementary set of tools rather than competing alternatives, with their variety reflecting the diverse operational requirements of IIoT environments.

A consolidated comparison of all mechanisms based on the core evaluation dimensions introduced earlier is presented in Table 7. This summary captures not only the main characteristics that set the mechanisms but also the common points that justify their integration into hybrid incentive architectures, especially in settings that require adaptability, transparency and resilience against misbehavior.

Mechanism	Rationality Assumption	Coordination Overhead	Fairness	Security Robustness	Scalability	Adaptivity	Blockchain Compatibility	IIoT Suitability
Stackelberg	Hierarchical leader–follower optimization. Equilibrium driven by anticipation of reactions.	Medium. Depends on leader's role	Leader-defined policies. Predictable allocation	Medium. Vulnerable if leader compromised	Medium. depends on hierarchy size	Low-to-Medium. Limited adaptive behavior	High. Leader's policies easily encoded on-chain	Suitable for hierarchical control loops and gateway–edge relationships
Evolutionary	Strategy evolution based on payoff replication. Convergence toward ESS.	Low. Minimal communication	Emergent fairness via population dynamics.	Medium-to-high. Resilient to noise & irrationality	High. suited for large populations	High. Reacts to environmental changes	Medium. Stochastic dynamics logs are able on-chain	Effective for dynamic and large-scale IIoT environments
Cooperative Game Theory	Coalition formation. Reward sharing based on collective welfare	High. Requires negotiation or coalition agreement	Strong fairness (e.g. Shapley distribution)	Medium. Dependent on coalition stability	Medium. coordination overhead increases with scale	Medium. Stable but less flexible	Medium. Coalition contracts implementable via blockchain	Strong when collaborative sensing or shared tasks exist
Non-Cooperative Game Theory	Independent optimization. Equilibrium through strategic competition	Very low. No negotiation needed	Fairness emerges only from equilibrium.	High. Naturally resistant to misbehavior	High. minimal overhead	Medium. Relies on strategic updates	High. Penalties and utilities enforceable on-chain	Ideal for adversarial IIoT scenarios and security enforcement
Reputation-Based	Long-term behavioral scoring.	Low. Requires	Long-term fairness. Rewards	High. Punishes	High. lightweight	Medium. Reputatio	Very High. Blockchain	Fits multi-domain IIoT

Mechanism	Rationality Assumption	Coordination Overhead	Fairness	Security Robustness	Scalability	Adaptivity	Blockchain Compatibility	IIoT Suitability
	Incentives tied to reliability history.	periodic score updates	consistent behavior.	misbehavior over time	and distributed	n growth supports adaptivity.	offers tamper-proof logs	where trust establishment is critical
Token-Based	Economic incentives based on programmable digital tokens.	Very low. Simple transactional logic	Market fairness. Reward proportional to contribution	Medium. Depends on token.	Very high. extremely scalable	Low-to-Medium. Depending on policy.	Very High. Native blockchain integration	Suitable for resource markets and decentralized task allocation
Auction-Based	Competitive bid–ask matching. Market clearing selects winners	Low-to-Medium Depending on auction frequency	High fairness in well-designed auctions.	Medium. Depends on truthfulness constraints	Very high. suitable for large-scale environments	Medium. Repeats per auction cycle.	Very High. Auctions naturally encoded via smart contracts	Ideal for bandwidth allocation, computation offloading and priority scheduling
Learning-Based	Rewarding based on model contribution quality.	Medium. requires model training cycles	Accuracy-based or contribution-based fairness.	High. Detects poor or malicious contributions	Medium. depends on learning workload	High. Learning adapts to new data patterns.	Very High. Smart contracts verify model contributions	Best for anomaly detection, predictive maintenance and data-driven IIoT

Table 7: Comparative Characteristics of Incentive Mechanisms in IIoT

7. A Risk-Adaptive Incentive Mechanism for Secure Information Flows

7.1 Introduction

Industrial Internet of Things (IIoT) environments are characterized by highly connected components and continuous information exchanges among different entities. Risk-based information flow analysis can help identify suspicious or illegal data transfers in real time. However, its effectiveness is limited when risk assessment is not directly linked to concrete system consequences. In practice, detecting a high-risk information flow does not automatically prevent future violations or encourage nodes to change their behavior actively.

To fix this issue, this chapter introduces INFFLOW-RT+, a risk-adaptive incentive mechanism that extends the INFFLOW-RT methodology by transforming real-time information flow risk assessments into concrete incentive and enforcement actions. It builds on the INFFLOW-RT methodology, which calculates dynamic risk scores for information flows using Bayesian inference and graph-based centrality metrics. Rather than just using these risk scores for manual policy changes, the approach leverages them as direct inputs to an automated incentive and enforcement framework.

The main idea behind this mechanism is simple: nodes that support secure and low-risk information flows get rewards, while nodes that increase systemic risk face economic and operational penalties. By embedding this logic into a decentralized structure supported by blockchain technology, the system ensures transparency, immutability and resistance to manipulation. Using fuzzy logic lets the mechanism to handle uncertainty and avoid strict, binary decisions that may lead to unfair or unstable behavior.

Unlike traditional access control or intrusion detection methods that focus mainly on allow or deny decisions, this incentive mechanism introduces a continuous and adaptable response model. Risk is viewed as a spectrum rather than a yes or no condition. This allows the system to apply proportional rewards or penalties based on both the severity of the detected behavior and the importance of each node within the information flow graph. This is especially important in IIoT systems, where central nodes can amplify the impact of malicious or incorrect actions.

In summary, this chapter is to present a unified framework that combines risk-aware information flow analysis with incentive-driven enforcement. The mechanism seeks to i) discourage malicious or careless behavior, ii) encourage long-term compliance through economic incentives and iii) improve the overall resilience of IIoT infrastructures by allowing self-regulation without continuous human intervention.

7.2 Architectural Overview of the Risk-Adaptive Incentive Framework

INFFLOW-RT+ uses a layered architecture that links real-time risk assessment closely with automated decision-making and decentralized enforcement. The design aims to transform risk-aware information flow analysis into a continuous feedback loop that actively influences node behavior instead of treating security assessment as a passive monitoring process.

At its core, the architecture relies on the Risk-Based Information Flow Control in real time(INFFLOW-RT). This part evaluates information flows and participating nodes. It calculates dynamic risk values that reflect both the likelihood of policy violations and the changing behavior of entities over time. Besides focusing on transaction-level risks, it incorporates graph-based centrality measures to capture the structural importance of nodes within the information flow graph. This dual approach helps ensure that security decisions account not only for the nature of an action but also for its potential impact on the system.

The risk assessment output is then processed by a fuzzy logic–based decision layer. The role of this layer is to interpret quantitative risk indicators flexible and contextually. Instead of relying on strict thresholds that can cause abrupt or unfair reactions, fuzzy inference allows the system to reason about concepts like low, medium or high risk while considering the centrality of the involved node. This mechanism architecture produces proportional and interpretable reputation adjustments that reflect the severity and significance of observed behaviors.

After deciding on a reputation adjustment, enforcement occurs through a blockchain-based infrastructure. Smart contracts are used to record reputation updates, distribute rewards and apply penalties in a transparent and tamper-resistant way. Nodes in the system have token-based stakes, which lets the enforcement layer to impose economic consequences when necessary. In cases of persistent or severe misconduct, the architecture can automatically restrict or isolate nodes to limit risk spread across the system.

Beyond direct enforcement actions, the architecture also impacts resource allocation. Nodes compete for limited system resources through auction-based processes, where participation conditions and effective bids adjust dynamically based on each node's reputation and risk profile. This design means that security decisions lead to real operational consequences. Nodes that consistently show secure behavior gain better access to resources, while nodes with high risk face costs or reduced opportunities. Importantly, the auction mechanism does not evaluate risk independently, but it reinforces prior assessments, integrating economic incentives into the overall security strategy.

Together, these architectural components create a closed-loop system where risk assessment, decision-making, enforcement and resource allocation continuously align. By merging fuzzy reasoning with decentralized enforcement and market-based incentives, this framework promotes self-regulation and long-term compliance, while staying adaptable to the changing nature of IIoT environments.

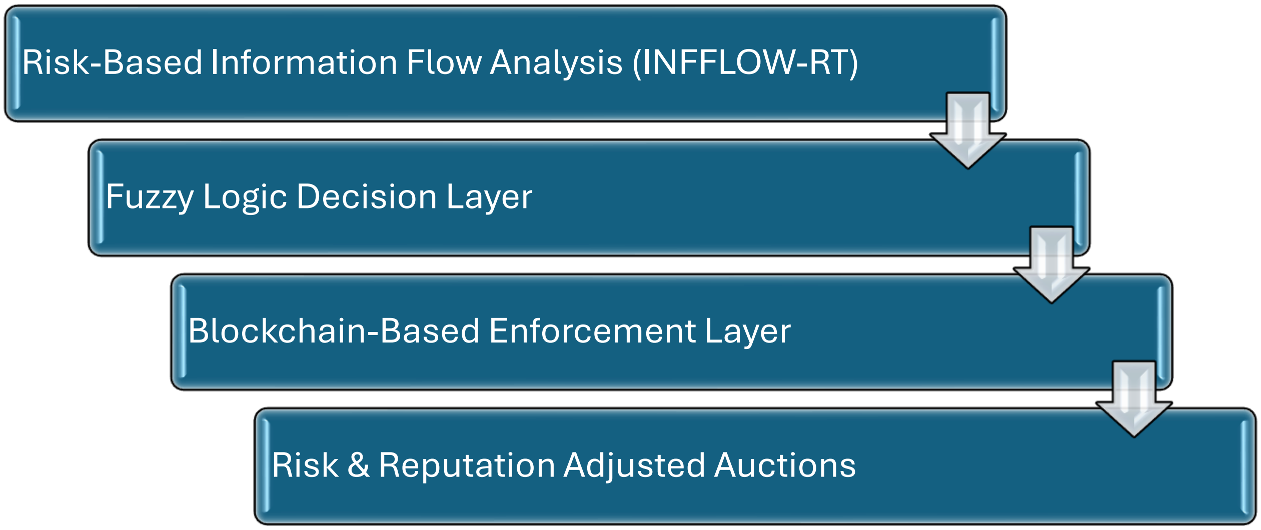
Risk-Based Information Flow Analysis (INFFLOW-RT)
Fuzzy Logic Decision Layer
Blockchain-Based Enforcement Layer
Risk & Reputation Adjusted Auctions

Figure 2: High-level architecture of the proposed risk-adaptive incentive mechanism

7.3 Inputs of the Incentive Mechanism

The effectiveness of INFFLOW-RT+ depends on its ability to observe and interpret significant indicators that reflect both the current security state of the system and the long-term behavior of participating nodes. The mechanism operates on dynamic, runtime-derived inputs from risk-based information flow analysis, rather than on static or manually defined parameters. These inputs are continuously updated as information flows change within the IIoT environment, allowing the mechanism to adjust its decisions over time.

The main inputs of INFFLOW-RT+ are focused on nodes and come directly from the risk-based information flow analysis. The most important of these inputs is the Dynamic Risk value, which represents a probabilistic estimation of the likelihood that an information flow violates security or information flow control policies. INFFLOW-RT produces this estimate using Bayesian updating based on historical data. Alongside risk magnitude, risk-weighted graph centrality metrics reflect the structural importance of each node in the information flow graph. By considering both risk intensity and node centrality, INFFLOW-RT+ evaluates security events in context. This approach recognizes that identical behaviors may have different impact depending on where they occur.

In addition to real-time risk indicators, the mechanism includes historical and state-dependent inputs, specifically the current reputation score of each node and its associated token-related parameters. Reputation reflects the total outcome of past interactions and enforcement actions, enabling the mechanism to differentiate between occasional anomalies and ongoing unsafe behavior patterns. Token-related parameters, such as balance or stake, provide the economic context for implementing proportional incentives. While these parameters do not directly affect risk estimation, they help determine the strength and feasibility of rewards, penalties and participation in resource allocation processes.

Finally, when available, the mechanism may also look at transaction-level attributes, including operation type or data sensitivity categories. These attributes add more context that can refine the interpretation of risk, especially in environments where different types of operations have different security implications. Although optional, these attributes enhance the input space's without changing the fundamental design of the mechanism.

Overall, the input set of the proposed incentive mechanism combines probabilistic risk estimation, structural awareness, historical behavior and economic context into a single decision space. This multi-dimensional perspective enables adaptive, proportional and context-aware incentive enforcement, forming a solid foundation for the methodology described in the next section.

7.4 Methodology of the Proposed Incentive Mechanism

The proposed incentive mechanism, referred to as INFLOW-RT+, follows a structured and flexible approach that turns real-time risk assessments into enforceable incentives and consequences. Instead of depending on static rules or binary decisions, this approach creates a continuous decision-making process. Here, risk is assessed in context, turn into proportional responses and reinforced through economic mechanisms. The primary goal is to make secure behavior the most beneficial strategy for rational nodes in the IIoT environment.

7.4.1 Risk Interpretation and Context Awareness

The methodology starts by interpreting of Dynamic Risk values (R_dyn ∈ [0,10]) from the INFFLOW-RT risk-based information flow analysis. These values provide probability estimates of the likelihood that an information flow will violate security or information flow control policies. However, raw risk magnitude is not enough to decide appropriate responses, since the same risk levels may have different implications based on the role of the node involved.

To solve this issue, INFFLOW-RT+ combines Dynamic Risk with Risk-Weighted centrality metrics from the information flow dependency graph. These metrics capture the importance of nodes and their ability to spread risk across multiple dependency chains. By considering risk magnitude and node centrality together, the system differentiates between localized events and behaviors that can lead to widespread impact. This context-aware approach ensures that violations are evaluated fairly in relation to overall system security goals.

Dynamic Risk values are segmented using the risk levels already defined by INFFLOW-RT, ensuring consistency with the underlying analytical model.

Dynamic Risk (R_dyn)	Risk level
[0,2)	Very low
[2,4)	Low
[4,6)	Medium
[6,8)	High

Dynamic Risk (R_dyn)	Risk level
[8,10]	Very high

Table 8: Dynamic Risk Levels (as defined in INFFLOW-RT)

This segmentation allows continuous Dynamic Risk values to be understood in a clear and straightforward way. By connecting probabilistic risk estimates to specific risk levels, INFFLOW-RT+ can evaluate security events qualitatively while maintaining the numerical basis of the risk analysis. These risk levels provide the main input for subsequent decision-making processes that consider context and uncertainty.

In parallel, risk-weighted centrality values are categorized to enable node-centric decision-making. To support this process, normalized risk-weighted centrality values are grouped into qualitative node roles that show the structural importance of each node in the information flow graph.

Normalized RW Centrality	Node role
< 0.3	Peripheral
0.3 – 0.6	Intermediate
> 0.6	Central

Table 9: Risk-Weighted Node Centrality Classification

This classification helps INFFLOW-RT+ to identify peripheral nodes that have limited impact and central nodes whose behavior can influence multiple dependency chains. By using node roles as qualitative inputs, the system ensures that the same risk levels may lead to different responses based on the potential systemic impact of the involved node. This categorization does not modify the centrality computation performed by INFFLOW-RT, but enables its use as a qualitative decision input within INFFLOW-RT+.

7.4.2 Fuzzy Logic–Based Reputation Assessment

After interpreting risks in context, INFFLOW-RT+ uses a fuzzy logic approach to determine the impact of observed behavior on node reputation. Fuzzy inference helps manage uncertainty, gradual behavioral changes and unclear situations common in dynamic IIoT environments.

Dynamic Risk and node centrality are presented as linguistic variables and evaluated using a predefined rule base.

Input	Linguistic Terms
Dynamic Risk	{Low, Medium, High}
Node Centrality	{Peripheral, Central}
Reputation Adjustment	{Reward, Neutral, Penalty}

Table 10: Linguistic Variables

The linguistic variables defined in Table 10 create the input and output space of the fuzzy inference process. By converting numerical risk indicators and node roles into qualitative terms, INFFLOW-RT+ encourages flexible thinking under uncertainty and avoids strict threshold-based decisions.

The fuzzy decision logic is expressed through IF–THEN rules that capture instinctive security reasoning. These rules combine Dynamic Risk levels with node centrality roles in order to produce proportional reputation effects that represent both behavioral severity and systemic importance.

Rule ID	IF Dynamic Risk	AND Node Centrality	THEN Reputation Effect
R1	Very Low	Any	Reward
R2	Low	Peripheral	Neutral
R3	Low	Central	Penalty (Low)
R4	Medium	Peripheral	Penalty
R5	Medium	Central	Penalty (High)
R6	High/ Very High	Any	Severe Penalty

Table 11: Node-Centric Fuzzy Rule Base

The rule base makes sure that identical risk levels do not always lead to the same reputation outcome, as node centrality explicitly affects the decision. This node-centric reasoning allows INFFLOW-RT+ to penalize high-impact behaviors more strictly, while treating low-risk or peripheral activities more gently.

The output from the fuzzy logic layer is a numerical reputation adjustment value, representing both the direction and magnitude of change to a node's reputation. At this stage, the output is a decision result and not an enforcement action.

7.4.3 Reputation Thresholds and Enforcement Logic

Reputation adjustments are collected over time, creating a global reputation score for each node. This score determines the node's enforcement state based on set thresholds.

Reputation Score	State
> 70	Trusted
40-70	Normal
10-40	At Risk
0-10	Restricted
< 0	Isolated

Table 12: Reputation States

The reputation states defined in Table 12 turn continuous reputation scores into specific trust levels. This approach allows for gradual increases and decreases in enforcement, ensuring that isolated anomalies do not lead to severe penalties, while ongoing negative behavior is systematically addressed over time.

Only when the fuzzy logic rule evaluation produces a non-zero reputation adjustment ($\Delta\text{Rep} \neq 0$) is the enforcement phase triggered. In all other cases, the system maintains the current reputation state.

Enforcement actions associated with each reputation state are implemented through blockchain-based smart contracts. Each reputation state is mapped to a specific set of enforcement actions that determine how the system responds to the node's behavior.

Reputation State	Enforcement Action
Trusted	Token rewards, auction advantages
Normal	No action
At Risk	Monitoring, reduced bidding power
Restricted	Token penalties, access limitations
Isolated	Automatic exclusion via smart contract

Table 13: Enforcement Actions

By requiring nodes to maintain token-based stakes, the system ensures that enforcement actions have real economic consequences. This discourages opportunistic or malicious behavior.

7.4.4 Risk and Reputation-Adjusted Resource Allocation

Beyond direct enforcement, the methodology integrates incentive mechanisms into resource allocation processes through risk and reputation-adjusted auctions. When nodes compete for limited resources, such as bandwidth or service priority, their effective participation conditions are influenced by their current reputation state and risk profile.

Nodes with high reputation and low risk benefit from lower costs or better chances of success, while those with higher risk face higher economic barriers. The auction mechanism does not reassess security risk independently. Instead, it reinforces prior decisions by translating reputation outcomes into long-term operational advantages or disadvantages. This integration ensures that security considerations consistently influence decisions at the system level, aligning economic incentives with desired security behavior.

7.4.5 Adaptive Feedback and Behavioral Regulation

The final aspect of the methodology is a closed feedback loop between enforcement outcomes and future system behavior. Enforcement actions and auction results influence how nodes interact with the system, which in turn affects future information flows and risk assessments.

This feedback mechanism allows the system to adjust dynamically to changing conditions. Nodes are encouraged to alter their behavior proactively in order to maintain a favorable reputation and economic standing, leading to self-regulation and improved overall resilience of the IIoT environment.

7.5 Flow of Operations

The proposed incentive mechanism operates as a continuous, event-driven process that responds to information flow activities in real time. Instead of performing isolated security checks, INFFLOW-RT+ follows a structured sequence of operations that forms a closed feedback loop. This section describes the operational flow of the mechanism, showing how individual system events move through the different components and impact node behavior.

The process starts whenever a new information flow or transaction occurs within the IIoT environment. This event may involve a data read, write or transfer between system components. When this activity is detected, the risk-based information flow analysis module evaluates the transaction and updates the dynamic risk estimates associated with the involved flow and nodes. This evaluation reflects both the immediate characteristics of the transaction and the historical behavior observed over time.

Once updated risk values are ready, the mechanism moves to contextual interpretation. Dynamic risk metrics are combined with structural information, such as node centrality, to assess the potential systemic impact of the observed behavior. This guarantees that risk is understood in relation to the node's role within the information flow graph.

The contextualized risk information is then processed by the fuzzy logic decision layer. Using fuzzy inference rules, the mechanism determines the appropriate reputation adjustment for the involved node. This decision captures both the severity of the observed behavior and its broader implications, producing a proportional outcome rather than a simple yes or no. At this stage, no enforcement action is taken, the system only decides how trust in the node should be updated.

Next, the enforcement phase occurs, where the reputation adjustment decision is implemented through blockchain-based smart contracts. Reputation scores are updated transparently and securely, while token rewards or penalties are applied when needed. If reputation degradation surpasses set thresholds, additional restrictive actions may be triggered automatically, such as limiting access to sensitive interactions. These actions ensure that security decisions have immediate and verifiable results.

Afterward, the updated reputation and risk status of the node influence its participation in resource allocation processes. When nodes compete for shared system resources, their effective participation conditions are adjusted based on their current security status. Nodes with good reputation and low risk are advantaged, while those with high risk face higher costs or limited access. Through this mechanism, security-related behavior directly affects operational capabilities.

The outcomes of enforcement and resource allocation decisions influence future node behavior. Rational nodes adjust their actions in order to maintain or improve their reputation and economic status, leading to new information flow patterns. These patterns are re-evaluated by the risk assessment component, completing the feedback loop and enabling continuous adaptation of the system. Operational flow of the proposed risk-adaptive incentive mechanism.

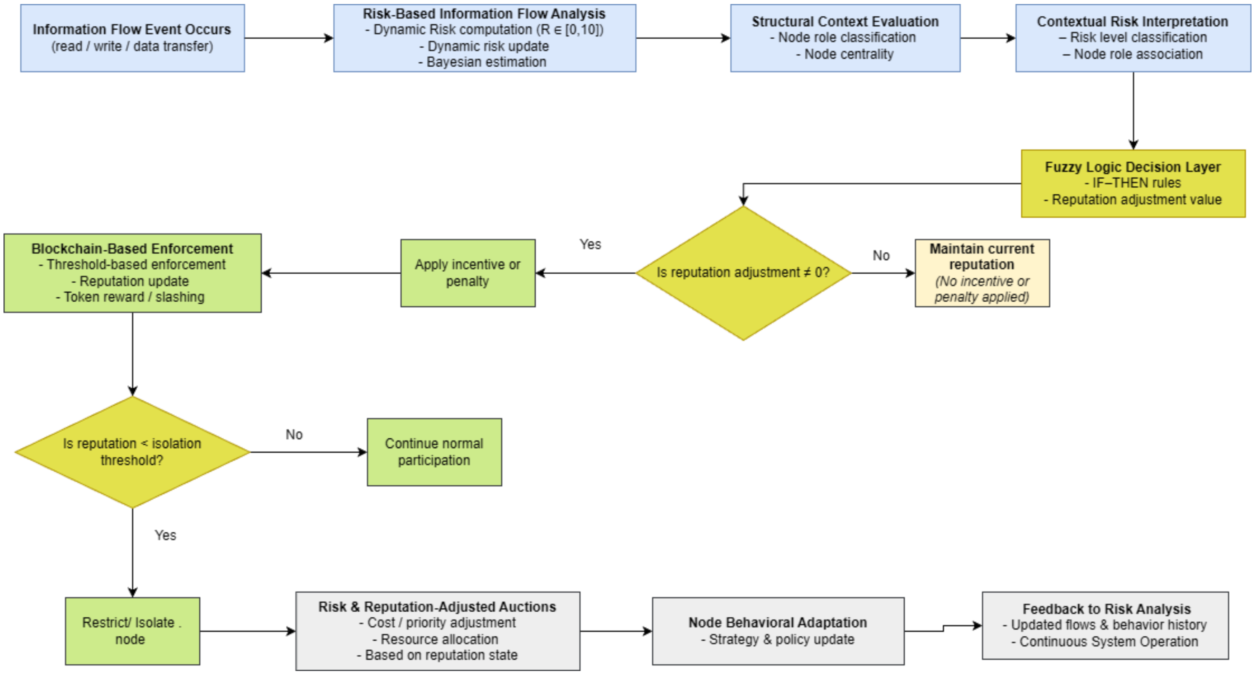
Information Flow Event Occurs
(read / write / data transfer)
Risk-Based Information Flow Analysis
- Dynamic Risk computation (R ∈ [0,10])
- Dynamic risk update
- Bayesian estimation
Structural Context Evaluation
- Node role classification
- Node centrality
Contextual Risk Interpretation
– Risk level classification
– Node role association
Fuzzy Logic Decision Layer
- IF–THEN rules
- Reputation adjustment value
Is reputation adjustment ≠ 0?
No
Maintain current reputation
(No incentive or penalty applied)
Yes
Apply incentive or penalty
Blockchain-Based Enforcement
- Threshold-based enforcement
- Reputation update
- Token reward / slashing
Is reputation < isolation threshold?
No
Continue normal participation
Yes
Restrict/ Isolate . node
Risk & Reputation-Adjusted Auctions
- Cost / priority adjustment
- Resource allocation
- Based on reputation state
Node Behavioral Adaptation
- Strategy & policy update
Feedback to Risk Analysis
- Updated flows & behavior history
- Continuous System Operation

Figure 3: Operational flow of the proposed risk adaptive mechanism

7.6 Illustrative Scenarios

This section presents three examples from a simplified IIoT environment to show how INFFLOW-RT+ operates. It illustrates how risk analysis, fuzzy decision-making, enforcement and incentive mechanisms interact in practice. The aim is to demonstrate how the proposed mechanism translates the risk evolution patterns identified by INFFLOW-RT into specific incentive and enforcement actions.

The scenarios are based on the risk evolution behavior observed from the evaluation of INFFLOW-RT. They include reputation-based incentives, blockchain-enforced penalties and risk-aware resource allocation.

7.6.1 Scenario 1: Low-Risk Peripheral Node

Imagine a peripheral IIoT node that performs routine data reading and transferring tasks in full compliance with information flow policies. The Dynamic Risk of these information flows remains consistently low (e.g., Rdyn=1.6), which aligns to the Low risk level defined in Table 8. The node's risk-weighted centrality is also low (e.g., 0.22), classifying it as a Peripheral node according to Table 9.

Based on these inputs, the fuzzy logic decision layer activates a rule for low risk and peripheral role (e.g., Rule R1 or R2 in Table 11). As a result, the system provides a neutral or slightly positive reputation adjustment (ΔRep>0). Since the adjustment is small and positive, the node's reputation stays within the Normal or Trusted state (Table 12).

This decision is logged and enforced using blockchain-based smart contracts, which might lead to a small token reward. When the node later takes part in resource allocation, such as auctions for shared bandwidth, its good reputation allows it to compete under better conditions, encouraging compliant behavior without unnecessary limitations or overhead.

Node	Dynamic Risk	Risk level	RW Centrality	Node role	Activated rule	Reputation Effect
N1	1.6	Low	0.22	Peripheral	R1/R2	Reward/ Neutral

Table 14: N1-Low-Risk Peripheral Node

7.6.2 Scenario 2: Moderate-Risk Central Node

In this scenario, a node occasionally deviates from expected behavior, resulting in moderate Dynamic Risk values (e.g., Rdyn=4.9, classified as Medium risk). Unlike the previous case, this node holds a central position in the information flow graph, with a normalized risk-weighted centrality value of approximately 0.65.

The fuzzy logic decision layer evaluates the combination of medium risk and high centrality, activating a rule that leads to a slight negative reputation adjustment (e.g., ΔRep=−5). This adjustment reflects the increased potential impact of the node's behavior while avoiding overly aggressive enforcement for isolated mistakes.

The blockchain-based enforcement layer applies the reputation update without initiating restrictive actions since the node's reputation remains within the Normal state. However, during later resource allocation processes, the node faces slightly higher costs or decreased bidding effectiveness, indicating that further deviations could lead to stronger penalties.

This gradual response mechanism promotes corrective actions while keeping the system stable and preventing sudden or disproportionate enforcement.

Node	Dynamic Risk	Risk level	RW Centrality	Node role	Activated rule	Reputation Effect
N2	4.9	Medium	0.65	Central	R5	Penalty (Low)

Table 15: N2-Moderate-Risk Central Node

7.6.3 Scenario 3: Repeated High-Risk Central Node

The last scenario considers a highly central node that repeatedly participates in high-risk or policy-violating information flows. Individual events are associated with high Dynamic Risk values (e.g., Rdyn≥7.5, corresponding to High or Very High risk). Each event is analyzed independently by INFFLOW-RT. However, the ongoing nature of the behavior results in lasting high-risk assessments, similar to the bad-biased risk evolution scenario observed in the evaluation of INFFLOW-RT.

For each event, the fuzzy logic decision layer activates rules matching high risk and a central node role, leading to significant negative reputation adjustments (e.g., ΔRep=−15 per event). While no single event directly causes isolation, the cumulative effect of repeated penalties leads to a gradual drop in the node's reputation.

Once the reputation score falls below set tolerance thresholds (Table 12), the blockchain-based enforcement mechanism automatically escalates its response. Token penalties become more severe and restrictive actions like limiting participation in sensitive interactions, are applied. If reputation continues to decline and drops below the isolation threshold, the node gets temporarily isolated from critical information flows to mitigate risk spread.

Importantly, this escalation is not the result of increasingly aggressive decision rules, but rather a logical outcome of consistent high-risk behavior over time.

Node	Dynamic Risk	Risk level	RW Centrality	Node role	Activated rule	Reputation Effect
N3	≥7.5	High/Very High	>0.6	Central	R6	Severe Penalty

Table 16: N3-Repeated High-Risk Central Node

7.6.4 Behavioral Feedback and System Adaptation

Across all scenarios, the outcomes of enforcement and resource allocation decisions influence future node behavior. Rational nodes adapt their strategies to improve reputation and economic position, leading to changed interaction patterns and information flows. These changes are continuously reassessed by the INFFLOW-RT analysis layer, closing the operational feedback loop.

Through this system, nodes are not instantly punished for isolated anomalies, nor allowed to compromise system security without consequence. Instead, INFFLOW-RT+ promotes gradual adaptation and self-regulation, ensuring that secure behavior is the most advantageous long-term strategy. This design improves overall system resilience while minimizing the need for continuous centralized oversight.

8. Conclusion

This thesis examined the problem of regulating information flows in Industrial Internet of Things (IIoT) environments. It focused on the gap between identifying risks and taking actions with system responses. In distributed industrial infrastructures, information propagates across indirect dependency chains. This makes transaction-level access control insufficient for stopping illegal or high-risk information flows. While risk-based analysis of information flows can provide useful real-time insights, its impact is limited when assessment results do not connect directly to consequences for the system participants.

To address this challenge, the thesis proposed a risk-adaptive incentive framework that turns real-time information flow analysis into a continuous behavioral regulation mechanism. Using the INFFLOW-RT methodology, the proposed framework (INFFLOW-RT+) changes dynamic risk indicators into proportional reputation updates and incentive-driven enforcement actions. Fuzzy logic allows gradual and context-aware decision-making, avoiding rigid reactions based on fixed thresholds. Blockchain-based smart contracts offer decentralized, transparent and tamper-resistant enforcement. By linking incentive results to resource allocation processes, the framework promotes long-term compliance and self-regulation within IIoT environments.

The main contribution of this work is methodological and conceptual. The proposed framework has not been implemented in a real or simulated IIoT deployment, and no empirical performance evaluation has been conducted. As a result factors like scalability, latency, computational overhead and behavioral effectiveness in real industrial conditions remain untested. Additionally, the framework assumes that nodes behave adaptively or rationally, relying on expert-defined fuzzy logic rules and reputation thresholds. This, may require careful adjustment to fit the constraints and operational policies of specific industrial domains. Furthermore, the use of blockchain-based enforcement is considered within a permissioned industrial context, without quantitative assessment of its impact on real-time system operation.

Future research should focus on implementing and experimentally evaluating the proposed framework in realistic IIoT testbeds or simulation environments in order to verify its feasibility and effectiveness. Configuration of fuzzy logic parameters and reputation thresholds, possibly supported by learning-based methods, could improve responsiveness and robustness over time. Further studies might look into hybrid incentive architectures that combine reputation-based, token-based and auction-based mechanisms. They could also integrate machine learning techniques for better behavior profiling and anomaly detection. Addressing issues of interoperability, governance and deployment will be crucial for moving the proposed approach from a conceptual design to a practical solution for secure information flow management in industrial environments.

References

[1] S. Latif, Z. Idrees, Z. Huma and J. Ahmad, "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies,* vol. 32, no. 7, p. e4337, 2021.

[2] O. Peter, A. Pradhan and C. Mbohwa, "Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Procedia Computer Science,* vol. 217, pp. 856-865, 2023.

[3] V. G. Trivedi, S. K. Dabhi, V. K. Patel, J. H. Solanki, A. B. Panchal and A. B. Patel, "Assessing the Impact of Industrial IoT on Engineering and Manufacturing: Benefits and Challenges," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 12, pp. 596-605, 2024.

[4] F. Qiu, A. Kumar, J. Hu, P. Sharma, Y. B. Tang, Y. X. Xiang and J. Hong, "A Review on Integrating IoT, IIoT, and Industry 4.0: A Pathway to Smart Manufacturing and," *IET Information Security,* p. Article ID 9275962 (16 pages), 2025.

[5] R. Trabelsi, G. Fersi and M. Jmaiel, "Access control in Internet of Things: A survey," *Computers & Security,* vol. 135, p. 103472, 2023.

[6] M. Kokila and K. S. Reddy, "Authentication, Access Control and Scalability Models in Internet of Things Security – A Review," *Cyber Security and Applications,* vol. 3, p. 100057, 2025.

[7] S. Nakamura, T. Enokido, L. Barolli and M. Takizawa, "Capability-Based Information Flow Control Model in the IoT," in *Advances in Intelligent Systems and Computing*, vol. 994, B. Leonard, Ed., Springer, 2020, p. 63–71.

[8] S. Nakamura, T. Enokido and M. Takizawa, "Implementation and evaluation of the information flow control for the Internet of Things," *Concurrency and Computation: Practice and Experience,* p. e6311, 2021.

[9] G. Kouko, J. Desharnais and N. Tawbi, "Information Flow Control for the Internet of Things," in *Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025)*, 2025.

[10] A. Anagnostopoulou, I. Mavridis and D. Gritzalis, "Risk-Based Illegal Information Flow Detection in the IIoT," in *Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023)*, 2023.

[11] A. Anagnostopoulou, I. Mavridis, M. Athanasopoulos, A. Mylonas and D. Gritzalis, "IIoT's Risk Odyssey: Navigating the Risk Propagation of Illegal Information Flows," *IEEE Access,* vol. 13, p. 59422–59433, 2025.

[12] D. Wei, H. Ning, F. Shi, Y. Wan, J. Xu, S. Yang and L. Zhu, "Dataflow Management in the Internet of Things: Sensing, Control, and Security," *Tsinghua Science and Technology,* vol. 26, no. 6, pp. 918-930, 2021.

[13] S. Rizal and D.-S. Kim, "Enhancing Blockchain Consensus Mechanisms: A Comprehensive Survey on Machine Learning Applications and Optimizations," *Blockchain: Research and Applications,* p. Article 100302, 2025.

[14] R. Lakshmana Kumar, F. Khan, S. Kadry and S. Rho, "A Survey on Blockchain for Industrial Internet of Things," *Alexandria Engineering Journal,* vol. 61, no. 8, pp. 6001-6022, 2022.

[15] M. Essaid and H. Ju, "Blockchain Solutions for Enhancing Security and Privacy in Industrial IoT," *Applied Sciences,* vol. 15, p. Article 6835, 2025.

[16] N. Y. Al-Matari, A. T. Zahary and A. A. Al-Shargabi, "A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks," *Scientific Reports,* vol. 14, p. Article 30990, 2024.

[17] N. Yashaswini and S. R. Sujatha, "Blockchain-Driven Access Control and Data Protection Framework for Industrial IoT Systems," *Mapana – Journal of Sciences,* vol. 24, no. 2, pp. 105-122, 2025.

[18] M. Usman, M. S. Sarfraz, M. U. Aftab, U. Habib and S. Javed, "A Blockchain Based Scalable Domain Access Control Framework for Industrial Internet of Things," *IEEE Access,* vol. 12, pp. 56554-56568, 2024.

[19] Y. Liu, R. Huo, N. Gao, C. Chi and T. Huang, "A Security Data Exchange Mechanism for IIoT Based on Blockchain," in *2025 4th International Conference on Cryptography, Network Security and Communication Technology (CNSCT 2025)*, Zhengzhou, China, 2025.

[20] S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova and A. Salykbayeva, "Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things," *Symmetry,* vol. 15, no. 10, p. 1958, 2023.

[21] H. F. Atlam, R. J. Walters, G. B. Wills and J. Daniel, "Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT," *Mobile Networks and Applications,* vol. 26, pp. 2545-2557, 2021.

[22] M. N. Sohail, A. Anjum, I. A. Saeed, M. H. Syed, A. Jantsch and S. Rehman, "Optimizing Industrial IoT Data Security through Blockchain-Enabled Incentive-Driven Game Theoretic Approach for Data Sharing," *IEEE Access,* vol. 11, 2023.

[23] W. Zhang, Q. Lu, Q. Yu, Z. Li, Y. Liu, S. K. Lo, S. Chen, X. Xu and L. Zhu, "Blockchain-based Federated Learning for Device Failure Detection in Industrial IoT," *arXiv,* vol. abs/2009.02643, 2020.

[24] A. Anagnostopoulou, N. Tsinganos, J. Chatzopoulos, I. Mavridis and D. Gritzalis, "INFFLOW-RT: A real-time, adaptive methodology for risk-based information flow control in IIoT," *International Journal of Information Security,* vol. 25, no. 16, 2026.

[25] T. Hussain, A. Fatima, A. Shaf and M. Iqbal, "How Can Incentive Mechanisms and Blockchain Benefit the Industrial Internet of Things: A Survey and Future Directions," *Computer Networks,* vol. 244, p. Article 110002, 2024.

[26] X. Ma, D. Yu, Y. Du, L. Li, W. Ni and H. Lv, "A Blockchain-Based Incentive Mechanism for Sharing Cyber Threat Intelligence," *Electronings,* vol. 12, no. 11, p. Article 2454, 2023.

[27] Q. Shi, L. Wang, Y. Bao and C. Chen, "Blockchain-Driven Incentive Mechanism and Multi-Level Federated Learning Method for Behavior Detection in the Internet of Vehicles," *Symmetry,* vol. 17, p. Article 669, 2025.

[28] Y. Liu, Z. Fang, M. H. Cheung, W. Cai and J. Huang, "An Incentive Mechanism for Sustainable Blockchain Storage," *arXiv ,* p. arXiv:2103.05866, 2021.

[29] Z. Wang, Q. Hu, R. Li, M. Xu and Z. Xiong, "Incentive Mechanism Design for Joint Resource Allocation in Blockchain-based Federated Learning," *arXiv preprint,* p. arXiv:2202.10938, 2022.

[30] M. Moniruzzaman, A. Yassine and R. Benlamri, "Blockchain and cooperative game theory for peer-to-peer energy trading in smart grids," *International Journal of Electrical Power and Energy Systems,* vol. 151, p. 109111, 2023.

[31] S. Mssassi and A. Abou El Kalam, "Game Theory-Based Incentive Design for Mitigating Malicious Behavior in Blockchain Networks," *Journal of Sensor and Actuator Networks,* vol. 13, no. 1, p. 7, 2024.

[32] J. Wei, X. Yi, X. Yang and Y. Liu, "Blockchain-Based Design of a Government Incentive Mechanism for Manufacturing Supply Chain Data Governance," *Sustainability,* vol. 15, no. 8, p. 6968, 2023.

[33] A. Gupta, "Blockchain-Based Tokenized Storage Incentives: Revolutionizing Decentralized Object Storage," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* vol. 11, no. 1, pp. 854-864, 2025.

[34] Z. Ai, Y. Liu and X. Wang, "ABC: An Auction-Based Blockchain Consensus-Incentive Mechanism," in *2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS)*, Shenyang, China, 2020.

[35] M. R. Behera, S. Upadhyay and S. Shetty, "Federated Learning using Smart Contracts on Blockchain, based on Reward Driven Approach," arXiv, 2022.