Bolstering IIoT Resilience: The Synergy of Blockchain and CapBAC

Argiro Anagnostopoulou[1][a], Eleni Kehrioti[1], Ioannis Mavridis[2][b] and Dimitris Gritzalis[1][c]
[1]*Department of Informatics, Athens University of Economics and Business, Patision 76 Ave, Athens, Greece*
[2]*Department of Applied Informatics, University of Macedonia, 156 Egnatia St, Thessaloniki, Greece*

Keywords: Access Control, Capability-Based Access Control (CapBAC), Blockchain, Industrial Internet of Things (IIoT), Industry 4.0.

Abstract: The growing integration of Internet of Things (IoT) into industrial environments highlights the need for adequate security and privacy maintenance. While traditional access control methods fall short in addressing the rising challenges of such environments, the combination of capability-based access control (CapBAC) models with blockchain technology emerges as a promising alternative. In this paper, we conduct a comprehensive analysis and comparison of approaches that integrate these two concepts. The evaluation of each approach is based on twelve criteria, including scalability, performance, efficiency, latency, throughput, degree of decentralization, consensus mechanism, smart contracts adoption, complexity, interoperability, security guarantees, and privacy. The aim of our analysis is to examine whether the combination of CapBAC and Blockchain brings a new era of secure industrial IoT (IIoT) operations. In order to identify the strengths and the areas for improvement, we provide four types of comparison to further assess these approaches based on IIoT requirements. Finally, we thoroughly discuss our findings, indicating directions for future research in order to enhance the adoption of such innovative mechanisms across broader industrial landscapes.

1 INTRODUCTION

The adoption of IoT concept traces back to the foundational periods of the internet, when researchers envisioned the connection between devices and machines, in order to support a better human interaction, monitoring, and control. In 1999, Kevin Ashton named this concept "IoT," marking an important shift toward embedding intelligence in physical objects so they could communicate over networks (Jaidka et al., 2020). The evolution of Internet technologies and advancements in wireless communication have helped make this vision a reality, gaining interest in the technology sector and driving to a quite fast growth. The low cost of these devices, in combination with advancements in internet connectivity (such as higher speeds) paving the way for their ubiquitous adoption.

Industrial Internet of Things (IIoT) has emerged as a result of the broad use of IoT technologies, which has attracted both consumers' interest and industries' recognition for its potential benefits. By incorporating smart technologies to industrial processes, their automation and efficiency are increased. IIoT involves a wide range of inexpensive, networked devices, such as actuators, sensors, and PLCs (programmable logic controllers). However, in order to protect the availability, confidentiality, and integrity of industrial systems, the integration of these technologies necessitates stricter security measures. Conventional security models frequently fail in the context of IIoT systems because such environments need a scalable and decentralized architecture. Blockchain technology is recognized for its decentralized architecture and its attributes of anonymity, transparency, and immutability. Consequently, there is a growing interest in exploring the integration of traditional access control schemes with blockchain technology. Given the dynamic nature of IIoT environments, robust access control methods are essential, in order to ensure that only authorized entities can interact with the data and services. One effective approach is CapBAC which efficiently manages access rights through the use of capability tokens. In this paper, we thoroughly assess the synergy of blockchain technology with CapBAC models.

[a] https://orcid.org/0000-0003-4199-6257
[b] https://orcid.org/0000-0001-8724-6801
[c] https://orcid.org/0000-0002-7793-6128

Anagnostopoulou, A., Kehrioti, E., Mavridis, I. and Gritzalis, D.
Bolstering IIoT Resilience: The Synergy of Blockchain and CapBAC.
DOI: 10.5220/0013513800003979
In *Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT 2025)*, pages 120-131
ISBN: 978-989-758-760-3; ISSN: 2184-7711

1.1 Motivation

The rapid growth of IIoT has transformed industrial operations to enable real-time monitoring and automation. However, this introduces a great number of security and privacy risks. Traditional access control methods, such as RBAC and ABAC, struggle to address the dynamic and distributed nature of IIoT systems, leaving them vulnerable to cyberattacks. CapBAC offers dynamic and fine-grained access management but relies on centralized systems prone to failure and limited transparency. Integrating CapBAC with blockchain technology provides a decentralized and secure framework, that can address these weaknesses and enhance transparency and traceability. This paper seeks to evaluate existing approaches that combine CapBAC and blockchain. Authors define several key criteria, in order to identify both the benefits and the limitations in order research community to build more secure industrial systems.

1.2 Structure

The remainder of this paper is structured as follows. Section 2 presents the algorithm that we used (i.e. the PRISMA statement) for the selection of the papers that we compare in this work. Section 3 briefly introduces the key concepts of our work. In Section 4, we present ten approaches that integrate blockchain technology with CapBAC. In Section 5, we establish twelve evaluation criteria and we comprehensively compare the aforementioned approaches. Finally, in Section 6 we discuss our findings and future research that may motivate research community to improve existing frameworks.

2 RESEARCH METHODOLOGY

In order to conduct a transparent and reproducible systematic literature review of the approaches that integrate the concepts of CapBaC and blockchain technology, we utilized the PRISMA statement (Page et al., 2021). The four steps that define PRISMA are: (1) plan and define the scope, (2) identify papers based on targeted keywords, (3) assess the selected papers, and (4) extract data, and present the findings.

2.1 Research Objectives and Strategy

The first and most important step was to define a set of research questions that we aimed to answer through this manuscript. The research questions, along with their corresponding goals, are presented in Table 1.

Table 1: Overview of the research questions and their goals.

Research Question	Goal
RQ1. How does CapBAC model operate in IIoT? What are its key security vulnerabilities?	This RQ explores the key vulnerabilities and challenges of CapBAC model, including scalability and unauthorized data access.
RQ2. How integrating blockchain into CapBAC enhances security in IIoT environments?	This RQ investigates how blockchain enhances the security of CapBAC models in IoT environments.
RQ3. What are the key challenges and limitations of using blockchain in CapBAC for IIoT?	This RQ identifies practical limitations of implementing blockchain in CapBAC, such as scalability, and energy consumption.
RQ4. Which models have researchers proposed to address the main vulnerabilities?	This RQ examines CapBAC and architectures proposed to address IoT vulnerabilities, highlighting innovative approaches.
RQ5. What performance evaluation metrics used for the developed models?	This RQ explores the key metrics for evaluating the performance and effectiveness of CapBAC models.
RQ6. How are these schemes and models validated?	This RQ investigates the validation methodologies for these CapBAC models.

Based on these questions, we constructed a comprehensive keyword string that employed in the search engines in order to retrieve relevant works (see Table 2). We used several widely known academic search systems in order to retrieve relevant work, including Google Scholar, Scopus, and Web of Science. The systematic literature search was carried out from September to December 2024.

Table 2: Keyword Query that used at search.

(“Capability-Based Access Control” OR “CapBAC”) AND (“Industrial Internet of Things” OR “IIoT”) AND (“blockchain” OR “blockchain integration” OR “blockchain for security”) AND ((“vulnerabilities” OR “access control weaknesses”) OR (“challenges” OR “limitations”) OR (“Models” OR “Schemes”) OR (“performance” OR “evaluation criteria” OR “evaluation”) OR “validation”)

The search query resulted in the significant number of 447 publications. For the evaluation of all these publications we established and applied the following sets of inclusion and exclusion criteria. The inclusion

criteria include: (a) relevance of title, (b) evaluation of the gathered material based on abstract and introduction, and (c) full-text reading of each article and publication.

The exclusion criteria include: (i) research papers, book chapters, and scientific articles without peer-review processes, (ii) articles or papers not written in English, (iii) publications missing abstracts and introduction as these sections are crucial for preliminary evaluation of relevance, (iv) irrelevant articles that initially seemed to be in context, but after closer review they were out-of-scope, (v) articles and publications from organizations without a valid national or international status, and (vi) unreferenced publications or unknown authors that were not members of relevant scientific communities. Criterion vi refers to publications not published in any scientific venue and are not referenced, cited, or otherwise validated from other technical whitepapers, reports, or research publications. It is important to clarify that this does not depend on whether a publication is included in paid venues; it just eliminates the possibility of fake or plagiarized content.

2.2 Selection of Studies and Analysis

We introduce Figure 1, which shows the PRISMA flow diagram, as a visual representation of the research selection procedure. The number of studies found, screened, included, and excluded at each review stage is depicted in this diagram. First, we eliminated 20 documents that were written in languages other than English. Next, we eliminated the 137 documents that were duplicates. From the remaining 290 documents, we eliminated a significant number of documents (222 documents) based on their titles and abstracts. Finally, we excluded 49 documents after conducting full-text reading. In the end, we selected 19 papers for our review. Ten of them examine blockchain-enabled CapBAC approaches. The remaining nine papers played an important role in shaping our evaluation criteria. We also used additional literature for peripheral information of our work. However, we did not take them into account to the number of included files as they were not directly associated with our research questions.

3 THEORETICAL BACKGROUND

This section provides the theoretical foundation, emphasizing on the core concepts of capability-based access control and blockchain technology.

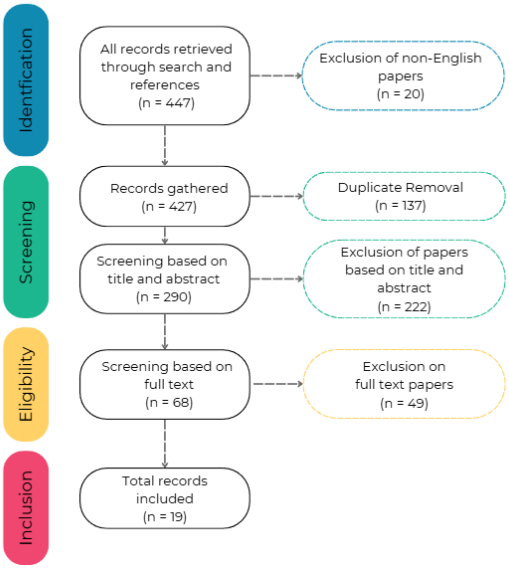

Figure 1: PRISMA Flowchart.

3.1 Capability-Based Access Control

CapBAC model has emerged as a promising approach for managing access rights in distributed systems, particularly suited for the IoT environment. Unlike traditional access control models that rely on centralized access control lists (ACLs), CapBAC distributes access rights directly to subjects in the form of capability tokens (Hernández-Ramos et al., 2013), (Nakamura et al., 2021). A capability token is a set of access rights granted to a subject. Each access right is typically represented as a pair (device, operation), indicating that the subject is allowed to perform a specified operation on the given device. In IoT, operations are most likely actions like GET, PUT, POST, and DELETE (Nakamura et al., 2021).

The key components of the CapBAC model are subjects (users, applications, or other entities that request access to resources), objects (resources or devices), capability tokens (sets that encapsulate access rights), and device owners. Firstly, the device owner issues a capability token for the device to a subject. Then the subject sends an access request to the device with the capability token that recieved from the owner. The device then validates the capability token and informs the subject whether the request was denied or approved (Nakamura et al., 2021).

3.2 Blockchain

Blockchain uses cryptographic algorithms, public key infrastructure, and decentralized consensus to synchronize distributed databases. It operates as a distributed ledger, where all nodes in a peer-to-peer net-

work maintain identical copies of the ledger. Transactions are integrated into the network through a consensus process, ensuring consistent updates across nodes (Kumar et al., 2022), (Latif et al., 2021). A blockchain consists of three components: blocks, the chain, and the network. Blocks consist of a header and a body containing cryptographically signed transactions. The header includes the previous block's hash, a timestamp, a nonce, and a Merkle root. Blocks are linked sequentially, starting from the genesis block, with each block's identifier derived from its hash (Latif et al., 2021), (Wang et al., 2020), (Lesavre et al., 2020). The key characteristics of blockchain technology are summarized below:

- **Immutability.** This guarantees data integrity by linking each block to its predecessor via cryptographic hashes, rendering the blockchain tamper-proof. Alterations in any block disrupt the consistency of the entire chain (Latif et al., 2021).
- **Decentralization.** By employing consensus algorithms and smart contracts, the distribution of data processing across nodes reduces costs and eliminates single points of failure (Kumar et al., 2022).
- **Transparency.** All information should be available to everyone. The transactions are stored in the ledger and can be traced by users with access to the blockchain (de Haro-Olmo et al., 2020).
- **Non-repudiation.** Signatures and private keys verify the repudiation by the corresponding public key. Cryptographically signed transactions are irreversible (Latif et al., 2021).
- **Traceability.** Timestamps facilitate the tracking of transactions and the path of digital assets (Kumar et al., 2022), (Latif et al., 2021).
- **Pseudonymity and Anonymity.** While information of the transactions are public, identities are shielded, offering users privacy through the use of public keys and cryptographic techniques (de Haro-Olmo et al., 2020), (Kumar et al., 2022).
- **Persistency.** Once transactions are verified and added to the blockchain, they become immutable and cannot be modified (Kumar et al., 2022).
- **Auditability.** Once a transaction is stored in the blockchain, its status is changed, making the transactions traceable (Kumar et al., 2022).
- **Interoperability.** Nodes can interact with physical resources and transmit data within the IIoT equipment (Kumar et al., 2022).
- **Reliability.** Blockchain uses cryptographic techniques (e.g. hash signature generation) to ensure reliability (Kumar et al., 2022).

4 BLOCKCHAIN-ENABLED CapBAC MODELS FOR IIoT

This section introduces ten approaches that combine CapBAC with blockchain technology to improve security and efficiency in IIoT systems.

4.1 CapBAC (Using Public Ethereum)

Liu et al. (Liu et al., 2021) proposed a decentralized CapBAC model for IoT devices using blockchain technology and decentralized identifiers (DIDs). Each participant (human or IoT device) has at least one unique DID, and access control is managed through capability tokens and credentials. The system consists of three modules: (i) identifier, (ii) ownership, and (iii) capability management, each interacting with on-chain smart contracts. The DID Registry links DIDs to DID Documents (DDOs) which are stored on-chain enabling registration, resolution, updates, revocation, and recovery. Device owners create ownership tokens and credentials stored in a Device Ownership Credential Registry, ensuring only authorised devices interact with requesters. The capability tokens and credentials manage access rights. Requesters send capability tokens to edge servers for verification, which then grant or deny access. The model is evaluated using an IoT device rental use case on a university campus. Authors implemented a proof-of-concept prototype using Node.js and the Parity consortium blockchain, with smart contracts written in Solidity. Security evaluation demonstrates protection against unauthorized access, data manipulation, and system recovery issues. Performance evaluation shows blockchain operations take around 10 seconds, while non-blockchain operations are faster. The model eliminates single points of failure, prevents device tracking, and provides a scalable, lightweight solution for IoT access control. Its comprehensive architecture and detailed system interaction address gaps in existing blockchain-based access control solutions.

4.2 CapBAC (Using Private Ethereum)

Nakamura et al. (Nakamura et al., 2019) proposed a CapBAC scheme for IoT that uses Ethereum smart contracts to provide decentralized and reliable access control. The model employs capability tokens linked to specific actions (e.g., read, write, execute) for each subject-object pair. Smart contracts manage token creation, delegation, revocation, and verification. When a subject requests access, the smart contract verifies the token's validity and access rights. Unlike

hierarchical delegation trees, this scheme uses a delegation graph, offering more flexibility in transferring access rights dynamically among subjects to adapt to changing needs. Authors evaluated the model by implementing it on a private Ethereum network and analyzing its gas consumption compared to BlendCAC. Gas costs were measured for key functions under different scenarios. They conluded that the proposed scheme consumed less gas for most operations. Token creation had a constant gas cost, unlike BlendCAC's linear increase. Delegation costs were similar to BlendCAC, while revoking a single child's token consumed less gas. However, revocation from all descendants required more gas due to the granular token structure. The evaluation indicated that the proposed model provides more flexible and fine-grained access control at similar or lower computational costs. Limitations include low privacy due to the absence of encryption and a lack of real-world IoT scenario testing.

4.3 CapChain

Le and Mutka (Le and Mutka, 2018) proposed CapChain, a blockchain-based access control framework for IoT environments. Device owners generate and encrypt capabilities, which are transferred through anonymous transactions on a public blockchain. This framework allows users to share and delegate access rights while protecting privacy. CapChain employs techniques from anonymous cryptocurrency systems, such as ring signatures and capability commitments, to hide user identities and capability details. Key features include automatic capability expiration, revocation of delegated rights, and management of multiple capabilities through a single master account. CapChain also implements a deterministic sub-address system to supports anonymous transactions while ensuring traceability for the original delegator. Authors employ a similar approach to FairAccess in order to transfer authorisation tokens through transactions. However, CapChain avoids embedding access control policies in token transactions, preserving privacy by keeping sensitive device and user information off the public blockchain. A proof-of-concept testbed demonstrates its ability to securely manage access rights while maintaining privacy. CapChain addresses resource limitations in IoT devices by allowing them to rely on a local proxy for blockchain queries. It enhances privacy by obfuscating user identities, capability details, and transaction depths, solving key privacy challenges in public blockchains. Moreover, this approach enables scalability by allowing users to manage capabilities across multiple domains through a single account. Authors evaluated CapChain under an adapted proof-of-work consensus from Monero. They integrated techniques from anonymous cryptocurrencies, and prove that CapChain provides a privacy-preserving access control solution for IoT environments.

4.4 CB2FAC

Chen et al. (Sun et al., 2019) proposed CB2FAC, a fine-grained and flexible capability-based access control model using blockchain. CB2FAC supports dynamic authorization and fast revocation through a new capability token structure and strict authorization rules. The model uses an authorization tree and a capability revocation list for efficient privilege management, encrypts tokens with AES for secure transmission, and employs a strict verification process. CB2FAC is built on the Hyperledger Fabric blockchain platform and consists of three main components: (i) a Service Domain for policy enforcement, (ii) an Application Domain for subject-object interactions, and (iii) smart contracts for managing subjects, resources, and capabilities. Smart contracts mediate between users and the blockchain, handling tasks such as subject registration, resource management, and token manipulation. This architecture ensures fine-grained access control and fast privilege revocation, while it reduces revocation time through the capability revocation list. To evaluate CB2FAC, authors conducted simulation experiments on a virtual machine setup with Hyperledger Fabric. Tests included granting, revoking, and verifying capability tokens, focusing on latency and throughput under various transaction request rates. Results indicated that CB2FAC achieved high throughput and low latency in large request scenarios while maintaining secure and reliable access control. Authors concluded that CB2FAC is suitable for practical applications and suggested that there is need to improve the encryption algorithm to enhance security.

4.5 IoT-CCAC

Bouras et al. (Bouras et al., 2021) proposed IoT-CCAC, a blockchain-based access control model for IoT consortium networks. IoT-CCAC organizes access control data into assets (physical devices), services (collaborative applications), and profiles (asset representations within services) to improve flexibility and granularity. It introduces statements as documents defining access permissions, which can be granted as capability tokens to individuals or groups. The model supports group capability tokens and provides a membership service with varying permissions.

It also integrates a blockchain-based database that combines blockchain security with the performance of traditional databases. This approach aims to address the scalability and growth needs of IoT. To evaluate the model, authors implemented a proof-of-concept prototype simulating a waste management scenario in a smart city. The prototype was built using Python, Flask, JWT Crypto Library, and BigchainDB. Authors chose Tendermint as the consensus protocol. The evaluation measured communication and computation costs for creating assets, profiles, services, and statements, as well as scalability through bulk transaction tests. Results indicated that IoT-CCAC performed well in security and scalability. Finally, they achieved faster authentication by efficient database querying.

4.6 BlendCAC

Xu et al. (Xu et al., 2018) proposed a blockchain-enabled decentralized capability-based access control model for IoT systems. BlendCAC is designed to provide a scalable, and lightweight access control solution. The Identity-based capability tokens specify which subjects have access to specific objects. The smart contracts handle token generation, validation, and revocation. BlendCAC also incorporates a federated delegation mechanism, enabling access rights delegation across different security domains. When a subject requests access, the service provider retrieves the token from the smart contract and validates access locally, allowing fine-grained, context-aware decisions. Authors evaluated BlendCAC through a proof-of-concept prototype on a private Ethereum blockchain. Miners acted as cloud servers, fog nodes, and edge nodes. The evaluation focused on the effectiveness in preventing unauthorized access, managing delegation and revocation, computational overhead, and network latency. Results indicated that BlendCAC effectively blocked unauthorized access and efficiently handled delegation and revocation processes. Overall, BlendCAC provides a decentralized and scalable solution to access management challenges in dynamic and heterogeneous IoT environments, while blockchain enhances security and transparency.

4.7 CapBlock

Truong et al. (Truong et al., 2022) proposed CapBlock, an IoT access control model integrating distributed CapBAC (DCapBAC) with blockchain. CapBlock uses two smart contracts on a permissioned blockchain: a policy contract for managing and evaluating access control policies and a capability contract for generating and managing tokens. It employs the XACML standard for defining policies and the DCapBAC approach for specifying tokens. When a user requests access, the system authenticates them, evaluates policies, and generates a capability token if approved, with all actions recorded on the blockchain for auditability. Authors implemented CapBlock using Hyperledger Fabric and evaluated its performance under various configurations, including different network and block sizes. They assessed latency, throughput, and the efficiency of policy registration, evaluation, and token generation. Results indicated that CapBlock improves security and provides efficiency comparable to non-blockchain DCapBAC solutions.

4.8 DTSAC

Liao and Wu (Liao and Wu, 2023) proposed DTSAC, a Dynamic Trust and Smart Contract-based Access Control model, to overcome the limitations of traditional access control. DTSAC uses smart contracts to automate capability token generation, delegation, and verification. The model employs a delegation tree system, with a root tree and subtrees representing delegator-delegatee relationships. This structure simplifies access control management, allowing quick permission revocation and reducing complexity. When a data user (DU) requests access, the smart contract verifies the token and assesses the DU's trust value based on predefined thresholds. Trust is categorized into normal, frequent, and malicious access. DTSAC updates trust values dynamically across multiple trees using both direct trust (on-chain history) and indirect trust (tree relationships), enhancing flexibility and efficiency. Authors implemented DTSAC on the Sepolia Ethereum testnet and evaluated its performance for security, scalability, and dynamic access management. Results indicated that DTSAC improves flexibility in granting and revoking capabilities and strengthens security through two-way dynamic trust evaluation. The model addresses IoT challenges like single points of failure and limited adaptability, providing a scalable and robust solution for distributed environments.

4.9 CDDAC

Li et al. (Li et al., 2021) proposed CDDAC, a blockchain-based IoT Cross-Domain Delegation Access Control Method, to enhance interoperability and security in IoT cross-domain access control. CDDAC uses single-layer capability tokens to represent access rights, reducing size and processing overhead compared to traditional nested tokens. This design sim-

plifies integration with blockchain systems and reduces token complexity. When access is requested, the domain manager verifies the token against policies and creates a delegation topology stored as a hash in a Delegation Trajectory Database (DTDB) on the blockchain. This approach ensures reliability without frequent policy updates on-chain, though smart contract redeployment adds overhead. Cross-domain access requests are handled through inter-domain communication based on the aggregated delegation data. Authors evaluated CDDAC on the Ropsten test network, whith their focus on delegation verification speed and decision-making efficiency. The results showed that CDDAC outperformed CapBAC and BlendCAC, achieving faster token verification speeds. The model enhances scalability and usability, providing a robust solution for cross-domain IoT access control and improving security management.

4.10 DCACI

Pinjala and Sivalingam (Pinjala and Sivalingam, 2019) proposed a Decentralized Lightweight Capability-Based Access Control Framework using IOTA. DCACI make use of IOTA's fee-less distributed ledger and Directed Acyclic Graph (DAG) structure, known as the Tangle, in order to enable efficient and secure transactions. Most transactions occur on the Tangle, enhancing scalability and usability. The framework uses the Winternitz signature scheme for stronger transaction security and IOTA's Masked Authenticated Messaging (MAM) for privacy and integrity of capability tokens, which encapsulate user permissions for accessing resources. Domain owners manage capability tokens on the Tangle and use IOTA seeds to generate private keys and addresses for transactions. When users request tokens, they should specify the resource and action. This request will be evaluated by domain owners. The approved tokens are context-aware, since they embed information like time or location for access. Users without an IOTA seed can participate but need one to delegate access rights. Authors evaluated DCACI through a proof-of-concept implementation on resource-constrained devices. The performance metrics indicated that the framework supports access control for millions of IoT devices with low latency and high transaction throughput. Its fee-less nature makes it ideal for environments with frequent device interactions.

5 COMPARISON OF APPROACHES

5.1 Comparison Criteria

This manuscript explores CapBAC models that integrate blockchain technologies to address IIoT challenges. We inspired from other fields that use clear, multi-criteria comparisons. For example, Pipyros et al. (Pipyros et al., 2018) combined legal, technical, and measurable factors to assess cyber-attacks under international law. Even though their focus is on legal thresholds like the "use of force", we follow a similar mindset by using specific IIoT-related criteria to compare access control models. We define 12 criteria, grouped into four categories. For each criterion we provide a description and its relevance to IIoT security.

5.1.1 Group 1: Performance Metrics

This group evaluates the performance aspects of a model regarding scalability, efficiency, and reliability in high workloads. It ensures that a model can operate effectively in real-world industrial scenarios.

Scalability. Refers to model's ability to efficiently handle a growing number of devices, users, and requests in IIoT environments (Pal and Jadidi, 2021).

Performance. In Industry 4.0, real-time operations are crucial since they rely on fast-paced data transmission and processing. Any delay or performance issue may significantly impact productivity and efficiency (Ahmed et al., 2023).

Efficiency. Measures the computational and communication overhead of a model. It evaluates the processing power, memory, and bandwidth needed, aiming to minimize resource use and make it suitable for resource-limited IIoT devices (Ahmed et al., 2023).

Latency. Captures the time needed by the system to process an access request and provide a response. Low latency is critical in industrial environments where timely responses ensure system reliability and avoid delays that may disrupt operations (Kumar et al., 2022).

Throughput. Evaluates whether a model can handle a great volume of access requests per unit of time. High throughput indicates that the model can efficiently support concurrent access in IIoT systems without bottlenecks (Kumar et al., 2022).

5.1.2 Group 2: Blockchain Features

This group examines blockchain-specific features that improve CapBAC models, including decentralization,

Table 3: Definition of values for the model scoring criteria.

Criterion	Low	Medium	High
Group 1: Performance Metrics			
Scalability	Limited ability to scale and thus not suitable for IIoT.	Moderate increase in devices and users.	Great increase in devices and users without performance degradation.
Performance	Poor performance, with frequent errors, delays, and instability.	Acceptable performance, with occasional errors or delays.	Excellent performance, with high accuracy, and responsiveness.
Efficiency	Intensive resource requirements, not for resource-constrained environments.	Moderate resource requirements, but can be optimized for better efficiency.	low computational overhead, minimizing resource consumption.
Latency	Low response times, ideal for real-time applications.	Moderate response times, ideal for IIoT use cases.	High response times, which impacts real-time cases.
Throughput	Low throughput, limited handling of large workloads.	Handling of moderate volume of requests.	Handling of high volume of requests, ensuring system responsiveness.
Group 2: Blockchain Features			
Degree of Decentralization	Centralized system with the blockchain as a minor role (e.g. private blockchains).	Consortium blockchain, a few approved participants manage the system.	Decentralized public blockchain, anyone can participate (max. transparency).
Consensus Mechanism	Lightweight mechanisms designed for smaller, private networks with fewer participants (e.g. Raft).	Mechanisms for moderate scalability that require enough resources (e.g. PoW, PoA, PoET).	Mechanisms which offer strong security, efficiency, and scalability (e.g. PBFT, PoS).
Smart Contracts Adoption	Use of smart contracts only for basic tasks, not central to how the system works.	Use of smart contracts for partial automation and advanced tasks.	Heavily use of smart contracts to automate operations and enforce rules.
Group 3: Complexity and Implementation Effort			
Complexity	Simple and easy to implement and maintain.	Moderate complexity, requiring technical expertise.	Increased complexity, need for expertise and resources for maintenance.
Interoperability	Low interoperability, limiting its compatibility with other systems.	Moderate interoperability, requiring some integration efforts.	High interoperability with existing IIoT infrastructure and standards.
Group 4: Security and Privacy			
Security Guarantees	Weak security features and susceptible to attacks.	Moderate security features, but vulnerable to attacks.	Strong security features, robust cryptography and key management.
Privacy Protection	Weak protection and may expose user data to privacy risks.	Moderate protection, but may not fully protect sensitive data.	Strong protection of user data from unauthorized access.

consensus mechanisms, and smart contracts. These are the key elements for secure, efficient, and autonomous access control systems.

Degree of Decentralization. Evaluates the degree to which the model reduces reliance on centralized authorities or intermediaries. Decentralization enhances system reliability, fault tolerance, and resistance to single points of failure (Kumar et al., 2022).

Consensus Mechanism. Explores the consensus algorithm used and its suitability for IIoT environments. Efficient consensus mechanisms contribute to security, scalability, and energy efficiency (Lashkari and Musilek, 2021) (Polat and Göcmenoglu, 2022).

- Proof of Work (PoW): high-energy, computationally intensive puzzles, but its slow transaction rates and energy demands make it unsuitable for IIoT.
- Proof of Stake (PoS): low-energy approach where validators create blocks based on their stake, making it suitable for IIoT. Its monetary basis poses implementation challenges.

Table 4: Evaluation of models based on the four groups of predefined criteria.

Criterion	CapBAC (using private Ethereum)	CapBAC (using public Ethereum)	CapChain	CB2FAC	IoT-CCAC	BlendCAC	CapBlock	DTSAC	CDDAC	DCACI
Group 1: Performance Metrics										
Scalability	H	M	H	H	H	H	H	H	H	H
Performance	H	M	M	H	H	H	M	H	H	M
Efficiency	H	H	M	M	H	H	H	H	H	H
Latency	M	L	M	L	M	M	M	-	L	L
Throughput	-	-	-	H	M	-	M	-	H	H
Group 2: Blockchain Features for CapBAC										
Degree of Decentralization	L	M	H	M	M	L	M	-	H	-
Consensus Mechanism	H	M	M	L	H	M	L	M	M	M
Smart Contracts Adoption	M	L	-	M	-	H	H	H	H	-
Group 3: Implementation Effort										
Complexity	L	M	H	H	M	M	H	L	H	H
Interoperability	M	M	-	H	M	M	H	M	M	M
Group 4: Security and Privacy										
Security Guarantees	-	H	-	H	H	M	H	H	H	H
Privacy Protection	L	H	H	-	M	M	H	-	L	H

- Tendermint: Byzantine consensus algorithm that saves energy by eliminating mining. A proposer suggests a block, and validators vote in steps to commit it, making it suitable for IIoT.
- Proof of Authority (PoA): lightweight, high-performance mechanism for permissioned blockchains, relying on a few trusted validators. Its decreased decentralization makes it suitable for private consortiums.
- Raft: simple, leader-based approach suitable for IIoT. Its scalability issues may slow down the consensus process in large-scale systems as nodes increase.

Smart Contracts Adoption. Assesses how smart contracts are used to automate and enforce access control policies, This emphasizes on flexibility, security, and the ability to manage complex conditions without manual intervention (Kumar et al., 2022).

5.1.3 Group 3: Implementation Effort

This group evaluates the aspects of implementing and maintaining the models, including architectural complexity, costs, and compatibility with existing systems.

Complexity. Examines the complexity of the model's architecture, algorithms, and protocols. Simplified models are easier to implement, and maintain, making them appropriate for real-world applications (Ahmed et al., 2023).

Interoperability. Assesses the model's compatibility with existing IIoT protocols, standards, and devices. This ensures smooth integration without major changes to current systems. This is critical where diverse technologies co-exist (Ahmed et al., 2023).

5.1.4 Group 4: Security and Privacy

This group evaluates whether a model can provide security and preserve privacy. These features are vital for access control models, especially in industrial systems where breaches can cause serious issues.

Security Guarantees. Evaluates the robustness of the model's security, including the use of advanced cryptographic methods, secure key management, authentication mechanisms, and resilience against vari-

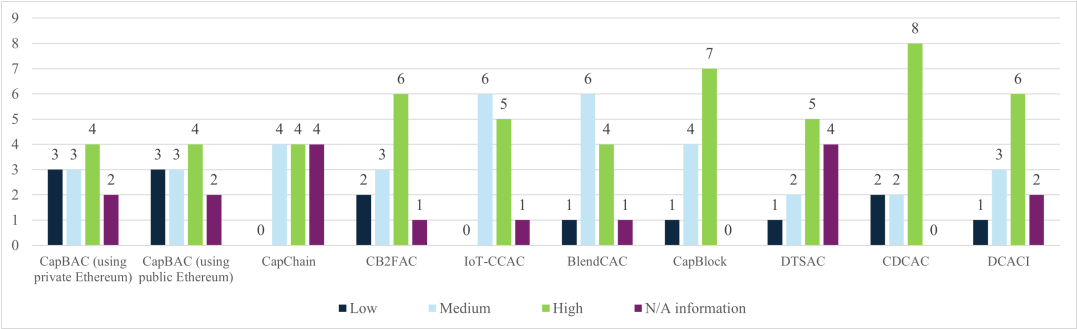

Figure 2: Overall performance per model.

ous cyber-attacks (Pal and Jadidi, 2021).

Privacy Protection. Assesses whether the model can protect user data and maintain confidentiality during communication and storage. It includes mechanisms to prevent unauthorized access to data and comply with privacy regulations (Pal and Jadidi, 2021).

5.2 Comparison Results

We define a three-scale system to compare the presented approaches. We rate each model as low, medium, or high, with some marked as N/A when data are unavailable. Table 3 explains how we assess the values of the criteria based on their context. Table 4 presents the results of our scoring of the models. To gain a greater understanding, we provide four different aspects for comparison: (i) rank models based on their score distribution. (ii) examine how well the models satisfy each individual criterion, (iii) group criteria into broader categories to uncover patterns and common gaps, and (iv) discuss trade-off between security and complexity.

5.2.1 Overall Performance per Model

In this subsection, we evaluate the overall performance of each approach based on the twelve defined criteria. Figure 2 offers this visual summary, helping identify strengths and weaknesses. It presents a bar chart that describes the distribution of high, medium, low, and N/A scores for each model. In order to better evaluate them, we categorized models in three groups. The first group is *highly performing models* and refers to those with the most high scores and thus a great coverage of IIoT challenges. The second group includes *moderately performing models* that refers to those with a balanced mix of low, medium, and high scores. The third group is the *underperforming models* for those that require refinement or more detailed reporting. The approaches of CB2FAC, CapBlock, CDDAC, and DCACI are labeled as highly performing models. As we notice, CDDAC is the leader in high ratings, since it counts 8 highs in a total of 12 criteria. The CapBlock follows with 7 high scores, while the CB2FAC and DCACI count 6 high scores each. The IoT-CCAC, BlendCAC, and DTSAC approaches are labeled as moderately performing models. They balance their performance with high and medium scores. Finally, CapBac using Ethereum Smart Contracts, CapChain, and CapBac using Blockchain belong to the underperforming models. These have split their scores among all the available values, indicating that they do not have strong aspects to focus on.

5.2.2 Evaluation of Criteria Accomplishment

This subsection assesses the scores that each criterion achieved. We defined and used three levels of classification for our evaluation: (i) outstanding criteria, that include those with most evaluations marked as high. (ii) moderate criteria, which refer to the ones with scores that are mostly medium. Such models may need optimization in order to be used in such environments. (iii) criteria with room for improvement, where the scores are splitted between medium and high, with a strong presence of low and N/A values, indicating gaps in their implementation. Figure 3 presents the number of the models that satisfy each criterion. We observe that scalability, efficiency, and security can be characterized as the most outstanding criteria. Moreover, we can classify performance, complexity, latency, consensus mechanism, and interoperability as moderate criteria. Finally, we recommend that models should prioritize their focus on the aspects of throughput, degree of decentralization, smart contract adoption, and privacy.

5.2.3 Satisfaction of Criterion Groups

Here, we assess how well each model meets the four criteria groups. We, again, defined three labels in order to characterize the satisfaction of a model for each criterion group. Specifically, (i) level 1 refers to high

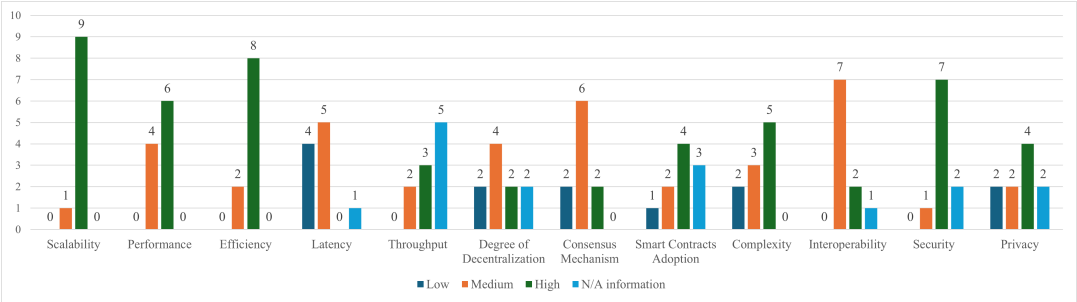

Figure 3: Evaluation of accomplishment of each criterion.

Table 5: Satisfaction of criterion groups.

Model	Group 1	Group 2	Group 3	Group 4
CapBAC (using private Ethereum)	L1	L2	L2	L3
CapBAC (using public Ethereum)	L2	L2	L2	L1
CapChain	L2	L2	L2	L2
CB2FAC	L1	L2	L1	L3
IoT-CCAC	L1	L2	L2	L2
BlendCAC	L1	L2	L2	L2
CapBlock	L2	L2	L1	L1
DTSAC	L2	L2	L2	L2
CDDAC	L1	L2	L2	L2
DCACI	L1	L2	L2	L1

satisfaction, (ii) level 2 refers to partial satisfaction, while (iii) level 3 is for those who needed more attention. Table 5 presents this information. We observe that all models moderately satisfy group 2 and group 3. The criteria of group 1 are almost highly satisfied. However, criteria of group 4 need more attention from researchers.

5.2.4 Trade-Off: Complexity vs Security

It is important to consider the trade-off between the level of security that a model achieves and the complexity of using that model. As all know, the greater the security is considered, the higher the complexity becomes. For this reason we evaluated whether the examined models apply to the above consideration. Table 6 presents the level of each criterion per model. We observe that this claim is verified, since the most models that have scored with high in security, have also scored with medium or high in the complexity. Only the DTSAC has evaluated with low complexity.

Table 6: Trade-off between Complexity and Security.

Model	Complexity	Security
CapBAC (using public Ethereum)	Medium	High
CapBAC (using private Ethereum)	Low	N/A
CapChain	High	N/A
CB2FAC	High	High
IoT-CCAC	Medium	High
BlendCAC	Medium	Medium
CapBlock	High	High
DTSAC	Low	High
CDDAC	High	High
DCACI	High	High

6 CONCLUSIONS

This study explored the integration of blockchain technology with Capability-Based Access Control (CapBAC) models to enhance access control in Industrial Internet of Things (IIoT) environments. By evaluating ten blockchain-enabled CapBAC approaches across twelve key criteria, we identified their strengths, limitations, and potential areas for improvement. Our findings indicate that blockchain-enabled CapBAC models achieve high scalability, which is critical for IIoT environments with a rapidly growing number of interconnected devices. The use of smart contracts is widely adopted, enhancing automation and reducing the need for centralized control. However, most implementations are deployed on private or consortium blockchains, limiting their potential to function as fully decentralized models. Moreover, our comparative analysis revealed that models such as CDDAC, CapBlock, CB2FAC, and DCACI have a strong performance, scoring high across multiple evaluation criteria. In contrast, models like CapBAC (using private Ethereum), CapBAC (using public Ethereum), and CapChain have some limitations that require further improvements to en-

hance efficiency, decentralization, and privacy. Despite their promising capabilities, blockchain-enabled CapBAC models face challenges in throughput, degree of decentralization, smart contract adoption, and privacy. Future research should focus on developing adaptive CapBAC models tailored to dynamic environments, investigate trust mechanisms in decentralized contexts, and propose standardized metrics for evaluating privacy and interoperability.

REFERENCES

Ahmed, S. F., Alam, M. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., Kabir, M., Shafiullah, G., and Muyeen, S. (2023). Industrial internet of things enabled technologies, challenges, and future directions. *Computers and Electrical Engineering*, 110:108847.

Bouras, M. A., Xia, B., Abuassba, A. O., Ning, H., and Lu, Q. (2021). Iot-ccac: a blockchain-based consortium capability access control approach for iot. *PeerJ Computer Science*, 7:e455.

de Haro-Olmo, F. J., Varela-Vaca, Á. J., and Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, 20(24):7171.

Hernández-Ramos, J. L., Jara, A. J., Marin, L., and Skarmeta, A. F. (2013). Distributed capability-based access control for the internet of things. *Journal of Internet Services and Information Security (JISIS)*, 3(3/4):1–16.

Jaidka, H., Sharma, N., and Singh, R. (2020). Evolution of iot to iiot: Applications & challenges. In *Proceedings of the international conference on innovative computing & communications (ICICC)*.

Kumar, R. L., Khan, F., Kadry, S., and Rho, S. (2022). A survey on blockchain for industrial internet of things. *Alexandria Engineering Journal*, 61(8):6001–6022.

Lashkari, B. and Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE access*, 9:43620–43652.

Latif, S., Idrees, Z., e Huma, Z., and Ahmad, J. (2021). 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*, 32(11):e4337.

Le, T. and Mutka, M. W. (2018). Capchain: A privacy preserving access control framework based on blockchain for pervasive environments. In *2018 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 57–64. IEEE.

Lesavre, L., Varin, P., and Yaga, D. (2020). Blockchain networks: Token design and management overview. Technical report, National Institute of Standards and Technology.

Li, C., Li, F., Yin, L., Luo, T., and Wang, B. (2021). A blockchain-based iot cross-domain delegation access control method. *Security and Communication Networks*, 2021(1):3091104.

Liao, J. and Wu, Q. (2023). Dtsac: Smart contract-based access control with delegation and trust management. In *2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 639–644. IEEE.

Liu, Y., Lu, Q., Chen, S., Qu, Q., O'Connor, H., Choo, K.-K. R., and Zhang, H. (2021). Capability-based iot access control using blockchain. *Digital Communications and Networks*, 7(4):463–469.

Nakamura, S., Enokido, T., and Takizawa, M. (2021). Implementation and evaluation of the information flow control for the internet of things. *Concurrency and Computation: Practice and Experience*, 33(19):e6311.

Nakamura, Y., Zhang, Y., Sasabe, M., and Kasahara, S. (2019). Capability-based access control for the internet of things: An ethereum blockchain-based scheme. In *2019 IEEE global communications conference (GLOBECOM)*, pages 1–6. IEEE.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., et al. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *Bmj*, 372.

Pal, S. and Jadidi, Z. (2021). Analysis of security issues and countermeasures for the industrial internet of things. *Applied Sciences*, 11(20):9393.

Pinjala, S. K. and Sivalingam, K. M. (2019). Dcaci: A decentralized lightweight capability based access control framework using iota for internet of things. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 13–18. IEEE.

Pipyros, K., Thraskias, C., Mitrou, L., Gritzalis, D., and Apostolopoulos, T. (2018). A new strategy for improving cyber-attacks evaluation in the context of tallinn manual. *Computers & Security*, 74:371–383.

Polat, B. and Göcmenoglu, I. (2022). Comparison between consensus algorithms in an iiot network: Analysis of proof of work, proof of stake and proof of authentication.

Sun, S., Chen, S., Du, R., Li, W., and Qi, D. (2019). Blockchain based fine-grained and scalable access control for iot security and privacy. In *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, pages 598–603. IEEE.

Truong, H., Hernández-Ramos, J. L., Martinez, J. A., Bernal Bernabe, J., Li, W., Marin Frutos, A., and Skarmeta, A. (2022). [retracted] enabling decentralized and auditable access control for iot through blockchain and smart contracts. *Security and Communication Networks*, 2022(1):1828747.

Wang, Q., Zhu, X., Ni, Y., Gu, L., and Zhu, H. (2020). Blockchain for the iot and industrial iot: A review. *Internet of Things*, 10:100081.

Xu, R., Chen, Y., Blasch, E., and Chen, G. (2018). Blendcac: A blockchain-enabled decentralized capability-based access control for iots. In *2018 IEEE International conference on Internet of Things and IEEE green computing and communications and IEEE cyber, physical and social computing and IEEE Smart Data*, pages 1027–1034. IEEE.