electronics

MDPI

Article

Bridge of Trust: Cross Domain Authentication for Industrial Internet of Things (IIoT) Blockchain over Transport Layer Security (TLS)

Fatemeh Stodt * and Christoph Reich *

Institute for Data Science, Cloud Computing and IT Security, Furtwangen University of Applied Sciences, 78120 Furtwangen im Schwarzwald, Germany

* Correspondence: fatemeh.stodt@hs-furtwangen.de (F.S.); christoph.reich@hs-furtwangen.de (C.R.)

Abstract: The Industrial Internet of Things (IIoT) holds significant potential for improving efficiency, quality, and flexibility. In decentralized systems, there are no trust-based centralized authentication techniques, which are unsuitable for distributed networks or subnets, as they have a single point of failure. However, in a decentralized system, more emphasis is needed on trust management, which presents significant challenges in ensuring security and trust in industrial devices and applications. To address these issues, industrial blockchain has the potential to make use of trustless and transparent technologies for devices, applications, and systems. By using a distributed ledger, blockchains can track devices and their data exchanges, improving relationships between trading partners, and proving the supply chain. In this paper, we propose a model for cross-domain authentication between the blockchain-based infrastructure and industrial centralized networks outside the blockchain to ensure secure communication in industrial environments. Our model enables cross authentication for different sub-networks with different protocols or authentication methods while maintaining the transparency provided by the blockchain. The core concept is to build a bridge of trust that enables secure communication between different domains in the IIoT ecosystem. Our proposed model enables devices and applications in different domains to establish secure and trusted communication channels through the use of blockchain technology, providing an efficient and secure way to exchange data within the IIoT ecosystem. Our study presents a decentralized cross-domain authentication mechanism for field devices, which includes enhancements to the standard authentication system. To validate the feasibility of our approach, we developed a prototype and assessed its performance in a real-world industrial scenario. By improving the security and efficiency in industrial settings, this mechanism has the potential to inspire this important area.

Keywords: security; trust management; authorization; authentication; industrial blockchain; IIoT; cross authentication

Citation: Stodt, F.; Reich, C. Bridge of Trust: Cross Domain Authentication for Industrial Internet of Things (IIoT) Blockchain over Transport Layer Security (TLS). *Electronics* **2023**, *12*, 2401. https://doi.org/10.3390/electronics12112401

Academic Editors: Jun-Ho Huh and Yeong-Seok Seo

Received: 5 May 2023
Revised: 23 May 2023
Accepted: 24 May 2023
Published: 25 May 2023

1. Introduction

Industrial communication systems play a crucial role in factory automation, manufacturing, and process control, enabling the exchange of data between controllers, sensors, actuators, input/output devices, and other industrial equipment [1].

As the Industrial Internet of Things (IIoT) continues to evolve, it becomes imperative to establish secure and reliable global connectivity for industrial equipment, ensuring the efficiency, reliability, and safety of industrial processes [2]. This requires the implementation of robust cyber security measures, such as access controls, encryption, intrusion detection and prevention, and security monitoring, to safeguard against potential cyber threats and attacks. Additionally, it is important to ensure that all stakeholders in the IIoT ecosystem, including equipment manufacturers, system integrators, and end users, have a shared understanding of the security risks and challenges associated with IIoT [3], and are committed to following best practices and standards to address them. Ultimately,

a comprehensive and proactive approach to IIoT security is essential to enable the full potential of this transformative technology while minimizing the risk of cyber incidents and their potentially devastating impact on critical infrastructure and operations. This requires secure and reliable communication from the most remote field equipment through appropriate communication systems and interfaces [4]. However, this increased connectivity and sustainable energy [5], also increases the vulnerability of the industrial environment to attacks [6]. As IIoT continues to mature, the security risks it introduces become more serious, exposing the IIoT environment to a range of cyber threats [7].

To address the security concerns in IIoT systems, incorporating blockchain technology can be a promising solution [8]. Blockchain-IoT, the integration of blockchain and IoT technologies, offers several benefits such as secure and efficient data storage and management, new use cases and applications, and enhanced privacy and security. By leveraging the strengths of both technologies, Blockchain-IoT can revolutionise various industries and bring significant improvements to existing solutions. However, despite its potential benefits, the adoption of Blockchain-IoT is still in its early stages and poses significant challenges [9]. These challenges include trust, privacy, authorisation, and security. When utilizing blockchain in the IIoT environment, careful consideration must be given to its application. It is not necessary to store all data, especially sensor values generated every millisecond, in the blockchain. Instead, blockchain can serve as a transparent and immutable storage solution for critical data, such as machine maintenance records and ordering information that require confirmation from various stakeholders. Additionally, blockchain can provide a platform for achieving consensus among stakeholders. By adopting this approach, the advantages of blockchain technology can be effectively harnessed in the IIoT environment while optimizing its use for specific data types and scenarios. This would ensure a careful consideration and effective implementation of Blockchain-IoT, ultimately overcoming the challenges and ensuring successful adoption in IIoT systems.

The implementation of blockchain technology in the Industrial Internet of Things (IIoT) environment has the potential to enhance trust and transparency for devices, applications, and systems. Additionally, blockchains can track devices and their data exchanges, improving supply chain processes [10]. This is achieved by leveraging the transparency provided by blockchain, which can improve supply chain processes [11].

However, the adoption of blockchains in the IIoT has been impeded by several roadblocks. For instance, public blockchains allow users to pass the authentication procedure based on a single attribute, such as the user's local history of actions in a certain location [12]. This means that a malicious user who behaves in one zone may be able to bypass authentication in another [13]. In response, we propose an IIoT architecture that combines existing centralized and local authentication methods from fieldbus devices. Additionally, we introduce distributed cross authentication on the application layer to verify devices across different fieldbus systems. This system operates on full blockchain nodes, ensuring decentralization and distribution. The core concept involves cross authentication for different sub-networks with diverse protocols or authentication methods while maintaining the transparency provided by the blockchain.

The remainder of this paper is structured as follows. Section 2 provides an overview of the state-of-the-art, while Section 3 presents the proposed system architecture and defines the problem. Section 4 outlines the scheme for cross authentication, and Section 5 discusses formal verification and the benefits of the proposed scheme. Finally, in Section 6, the paper concludes.

2. State of the Art

Cross-authentication is a critical aspect of distributed systems that enables secure communication between different entities in a network. With the increasing adoption of distributed systems, cross-authentication has become a significant research area to ensure the integrity and confidentiality of data transmission.

2.1. Cross Authentication

Cross-authentication plays a vital role in ensuring secure communication among different entities in distributed systems. As the adoption of distributed systems continues to grow, cross-authentication has emerged as a significant research area aimed at safeguarding the integrity and confidentiality of data transmission.

In the process of cross-authentication, users in different network domains are authenticated through the issuance of cross-certificates across multiple certificate authorities [14]. This approach involves trust anchor certificate authorities utilizing their private keys to issue digital certificates, establishing trust between domains.

To address security concerns such as key escrow and certificate maintenance complexity, Qikun et al. introduced a dynamic and cross-domain authenticated asymmetric group key agreement protocol that incorporates cross-domain authentication [15]. This protocol enables secure communication between diverse network domains. Similarly, Lee et al. proposed a cross-layer authentication protocol for the Internet of Things, featuring a novel integration technique [16]. This protocol offers the option of utilizing an additional secret key, exhibiting lower computational complexity and reduced overhead compared to conventional Authentication and Key Agreement (AKA) protocols, while still maintaining competitive authentication performance.

Shawky et al. presented a cross-layer authentication scheme designed for secure vehicular communication [17]. This scheme verifies the legitimacy of terminals at upper protocol layers and performs re-authentication at the physical (PHY) layer using unique PHY-layer signatures.

Jia et al. introduced an identity-based cross-domain authentication scheme for the Internet of Things that employs blockchain as a decentralized trust anchor, as opposed to traditional certificate authorities [14]. This approach utilizes an identity-based self-authentication algorithm as a replacement for traditional Public Key Infrastructures (PKI) authentication. Furthermore, Chen et al. proposed a cross-authentication model for heterogeneous domains, implementing mutual entity authentication based on certificate-based-PKI and ID-based authentication [18]. In another study, Jan et al. identified shortcomings in previous protocols for securing Internet-of-Drones (IoD) and proposed an improved and robust public key infrastructure (PKI)-based authentication scheme [19].

2.2. Cross Authentication in Distributed Systems

The distributed nature of blockchain technology enables the emergence of novel business models and organizational structures, fostering self-organizing economies [20]. Nevertheless, it is crucial to address privacy and security concerns when transitioning to this new paradigm.

In distributed networks involving multiple domains, preserving privacy for nodes and domains is of utmost importance. Cross-authentication across different domains serves as an effective means of securing communication. To enhance the efficiency and credibility of authentication in the IoT domain, Guo et al. proposed a master-slave chain-based cross-domain authentication technique [21].

Wang et al. presented a blockchain-based multi-certificate authority (CA) cross-domain authentication scheme within a decentralized autonomous network [22]. The scheme aims to improve the efficiency of cross-domain authentication by enabling the sharing of cross-domain certificate information among multiple domains. Additionally, a cross-domain certificate revocation mechanism is designed.

In the context of the Industrial Internet of Things (IIoT), Zhong et al. proposed a distributed cross-domain message authentication scheme with conditional privacy preservation [23]. This scheme leverages secret sharing technology and batch authentication to reduce latency and enhance system flexibility.

Yuan et al. proposed a dynamic cross-domain authentication scheme (DCAGS-IoT) for the Internet of Things (IoT) using group signature technology and a distributed system

architecture of blockchain [24]. This scheme allows group signature users to sign on behalf of a group, protecting individual privacy and enabling tracking of suspicious users.

Huang et al. introduced a unified blockchain-assisted secure cross-domain authorization and authentication framework for smart cities [25]. The framework ensures transparent cross-domain resource access while preserving user privacy. Privacy-preserving techniques such as homomorphic encryption and zero-knowledge proofs are employed to safeguard users' sensitive information.

Xue et al. proposed a secure and efficient cross-domain authentication scheme based on two cooperative blockchains (BCs) for medical consortium systems [26]. The scheme utilizes intra-domain and inter-domain BCs to record authentication information and protect against unauthorized access.

Zhang et al. have previously proposed a blockchain-based approach for cross-domain authentication [27]. However, assuming that all domains have trustworthy users is unrealistic, and relying on a single authentication server in each domain poses a significant risk of failure.

To address these issues, Wang et al. utilize consortium blockchain technology to construct a decentralized network with root certificate authorities serving as verification nodes [28]. The hash values of permitted certificates are stored in each block, and the verification procedure simply checks whether the computed hash of the user's certificate matches the hash stored in the blockchain.

Shen et al. introduced BASA, a blockchain-assisted secure device authentication system for cross-domain IIoT [29]. They propose the use of a consortium blockchain to foster trust development across distinct domains. Throughout the authentication process, identity-based signatures (IBS) are utilized. However, they recommend employing a Storage server for cross-authentication and assume the environment to be completely trustworthy for sharing domain-specific data.

3. System Overview and Problem Definition

This section is organized into four subsections for clarity and structure. Section 3.1, "System Overview", describes a use case that establishes distributed connections between different factories. The network consists of various devices that communicate with each other using local and cross-domain communication.

Section 3.2, "Cross Domain Problem Statement", addresses the challenge of cross-domain communication, where multiple enterprises and organizations share resources in a decentralized network environment. Two approaches are discussed to overcome this problem, including the use of PKI for secure communication, and the challenges of integrating field devices into the blockchain network.

Section 3.3, "Blockchain Vulnerabilities", highlights the security issues that may arise from the utilization of blockchain and emphasizes the importance of addressing them to ensure a secure system.

Lastly, Section 3.4, "Requirements", introduces and discusses the requirements based on the previous subsections that are necessary to address the cross-domain challenge. This reorganization improves the flow and style of the text, making it easier to understand the main points of each subsection.

3.1. System Overview

The industrial revolution, commonly referred to as Industry 4.0 or even 5.0, has brought forth new opportunities and challenges for factories operating in an increasingly interconnected world. Traditionally, each industry has maintained its own security management system, resulting in limited collaboration and interoperability with other industries. Recognising this need for cross-industry collaboration, the Schloss system was developed [30].

The Schloss system represents a decentralized network that connects multiple factories, leveraging blockchain technology to foster mutual benefit and cooperation as shown in Figure 1. In this system, each local user is authenticated within their own company and is subsequently invited to join a private blockchain. To become an active node within the

network, authentication through a full node is required, and an ID is obtained from the authorisation management process. The establishment of trust among selected subnetwork for each company stakeholder as member in private blockchain is facilitated through the universal Trust Management System (TMS). The TMS serves as a mechanism to establish and maintain trust across the network, enabling secure collaboration and data exchange among diverse industrial stakeholders.

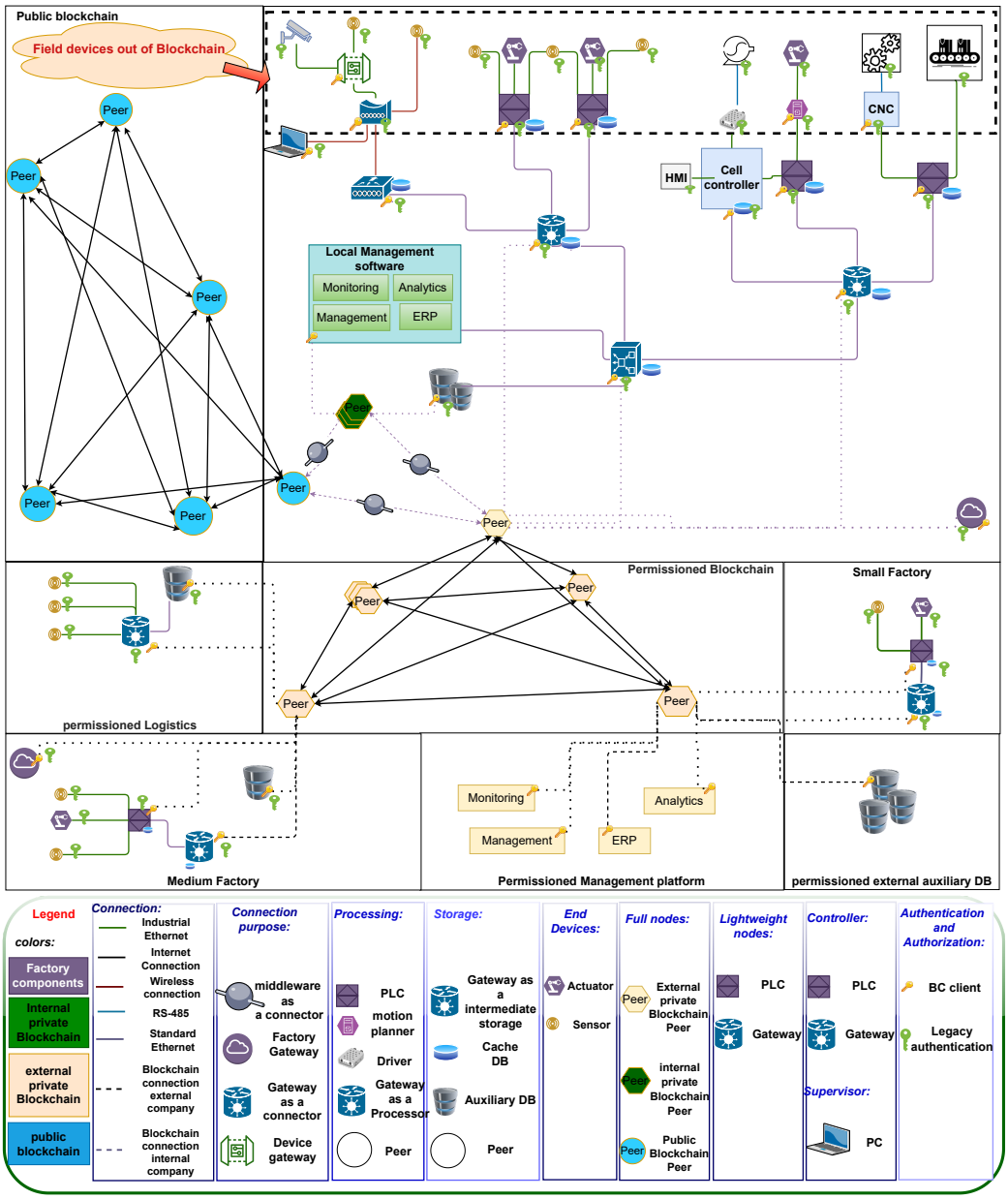

Figure 1. The used Schloss system architecture [30].

The trust level of nodes is calculated for a certain amount of time and stored in blockchain. The performance of nodes within the network is assessed based on their behavior. These nodes consist of various devices, including gateways, computers, controllers, as well as end devices such as sensors and actuators. There are two types of communication exists between nodes: local communication for communication to local devices and authentication in each subnetwork, and cross-domain communication, which involves transferring local user authentication from one subnetwork to another. Nodes may only access data on the network after being authenticated through a full node and obtaining an ID from the Authorization Management (AM), which consists of the most trustworthy

nodes in the blockchain. The trust value is calculated based on various factors, including a device's behavior, behavioral history, impact on the network, and certificate status in the current authentication system. Depending on the level of privacy and network behavior needed, different entities may be required to ensure that the system meets requirements.

3.2. Cross Domain Problem Statement

In Figure 2, we see the problem model where multiple enterprises and organizations share resources in a decentralized network environment. In this scenario, a single trust domain cannot provide numerous services, requiring users to visit several domains. Consider User A from domain A who wants to access Service A in domain B. To validate User A, the authentication server in domain B may require User A's root CA certificate to obtain their identity certificate. However, this method has drawbacks, including a complex authentication process, frequent signature verification, and certificate management complexity.

Alternatively, Domains A and B can be certified by a third-party certification body. While this approach is more efficient, it also has some disadvantages. Third-party certification authorities can create single points of failure and privacy breaches.

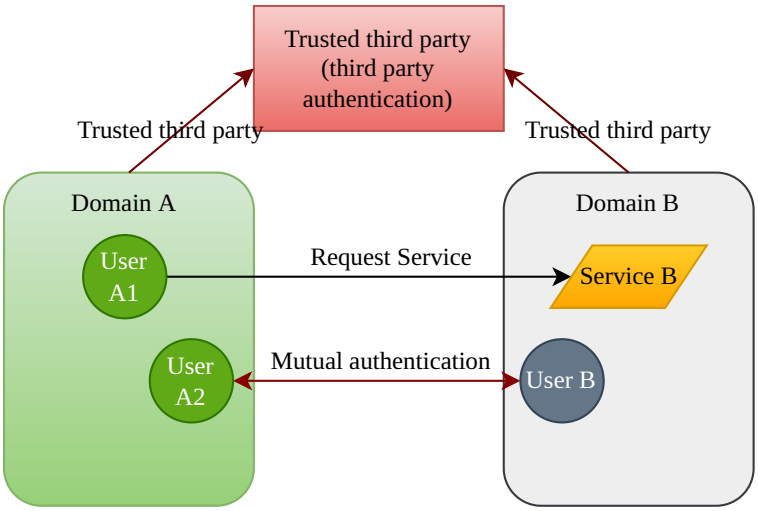

Figure 2. Cross domain problem model.

The private blockchain network that connects the factories and enables cooperation was described in Section 3.1. Nodes within this network are certified and use PKI for secure communication. Communication between blockchain nodes takes place over the internet, utilizing the TCP/IP protocol.

As shown in Figure 1, field devices are not directly part of the blockchain network. Instead, they may connect to controllers which act as blockchain clients. However, as the Operational Technology (OT) section of the plants must be highly secure, direct internet access is not allowed. As a result, most factories still use classic fieldbuses, and within those buses, different machines may use different field protocols. While it is possible to have local PKI, valid certificates may not be recognized on the internet due to security concerns.

In addition to the cross domain problem, there are several blockchain vulnerabilities that need to be addressed, which will be discussed in the following section.

3.3. Blockchain Vulnerabilities

Blockchain technology, specifically private blockchains, relies on collaborative maintenance by multiple nodes in the network to ensure transparency and security of transaction and smart contract data. However, there are vulnerabilities that can be exploited by attackers to undermine the integrity of the blockchain network [31]. This section highlights some of the potential attacks that can occur in a private blockchain environment.

The private blockchain is maintained collaboratively by all nodes on the network, ensuring that all transaction and smart contract data is visible to all nodes.

1. Edge nodes and nearby nodes are inquisitive about the endpoints' identities in order to gain more advantageous information.
2. By impersonating end devices, attackers may intercept communication data and undermine system security.

According to the above assumptions, the following attacks are possible:

1. Man-in-the-middle attack: an attacker intercepts communication data and spoofs both sides.
2. Distributed denial-of-service (DDoS) attack: the attacker overwhelms the majority of network nodes and disables regular communication.
3. Replay attack: an attacker replicates authorized communication without the counterpart's consent in order to fool him.
4. Sybil Attack: in this attack, a single malicious node assumes many identities and relocates itself around the network. This results in massive resource allocation being made in an unjust manner.
5. Spam attack: in this attack, when numerous transactions are submitted to a blockchain network in a short amount of time, the network's nodes must receive, verify, send, and store data; as a result, blockchain networks may get overwhelmed with data packet traffic.

3.4. Requirements

The following section introduces and discusses the requirements based on the cross domain problem and vulnerabilities of blockchain. In manufacturing, blockchain technology is increasingly recognized for its potential to enhance security and administration. This is particularly important as traditional industrial networks, including SCADA systems, are vulnerable to security threats, especially with the increasing transmission of data through them [32]. Authentication plays a crucial role in ensuring network security, as it verifies the identity of devices and users requesting access to protected resources [33]. By restricting communication to only authenticated devices and processes, companies can prevent unauthorized access and maintain secure connections between identified field devices that use industry protocols. To address the cross-domain problem, establishing a secure connection between the domains is necessary. To achieve this, specific requirements must be met, which we will outline as follows:

1. Bus-internal communication: the bus-internal communication is the native fieldbus communication between field devices and possibly directly integrated controllers.
2. Establishing end-to-end secure communication between two endpoints is the presence of cryptographic keys and/or certificates for authentication there.
3. (PKI) can be extended to the field level or integrated into it. The entire life cycle of a field device was taken into account. In particular, this includes the internal PKI, it means it is just valid inside field bus area. it is necessary to avoid direct connection from outside of subnetwork without monitoring.
4. Trusty full nodes: Trusty full nodes act as the manager of the blockchain authenticator for the factory to which the node belongs and as the manager of the private blockchain. They are also responsible for managing the devices in the factories' domain and providing blockchain nodes.
5. Table of trusty neighbor nodes for each node in blockchain.
6. Using Transport Layer Security (TLS). TLS is a cryptographic protocol and a good starting point because of the following properties:
    * The dependencies of TLS on layers above and below are low. TLS can be considered mature due to its widespread and mass use.
    * TLS is also continuously and intensively put to the test.
    * TLS is very flexible and allows adaptation to given requirements or boundary conditions via numerous parameters.

* TLS does not require an IP-based network, but only the possibility of the targeted delivery of data packets, the so-called TLS records, to a specific recipient.

4. Proposed Scheme

4.1. Cross-Fieldbus Communication Model

In this section, we will discuss the secure end-to-end channel establishment for field devices. A typical field device consists of a fieldbus application and a module for fieldbus communication. Existing modules communicate via integration within the fieldbus communication area, and new interfaces or services can be provided if required. The primary objective is to establish a secure end-to-end channel using TLS across the communication path or multiple channels.

When the bus's own communication is secured, the goal is extended to secure the actual fieldbus communication itself, which is achieved through an adaptation known as "TLS-over-X". However, before TLS can be used, data must be exchanged in some form between the endpoints. It may not be possible to address user data explicitly and without interaction with a specific endpoint. For instance, when communicating from a non-IP-based automation network over the internet, address translation is required at the edge of the automation network, which may not be controllable by the field device.

To address this issue, blockchain nodes in each subnetwork that already have a trust value for one another can authenticate each other and act as a bridge between two endpoint devices in different field devices. This enables secure communication between various field equipment, as shown in Figure 3.

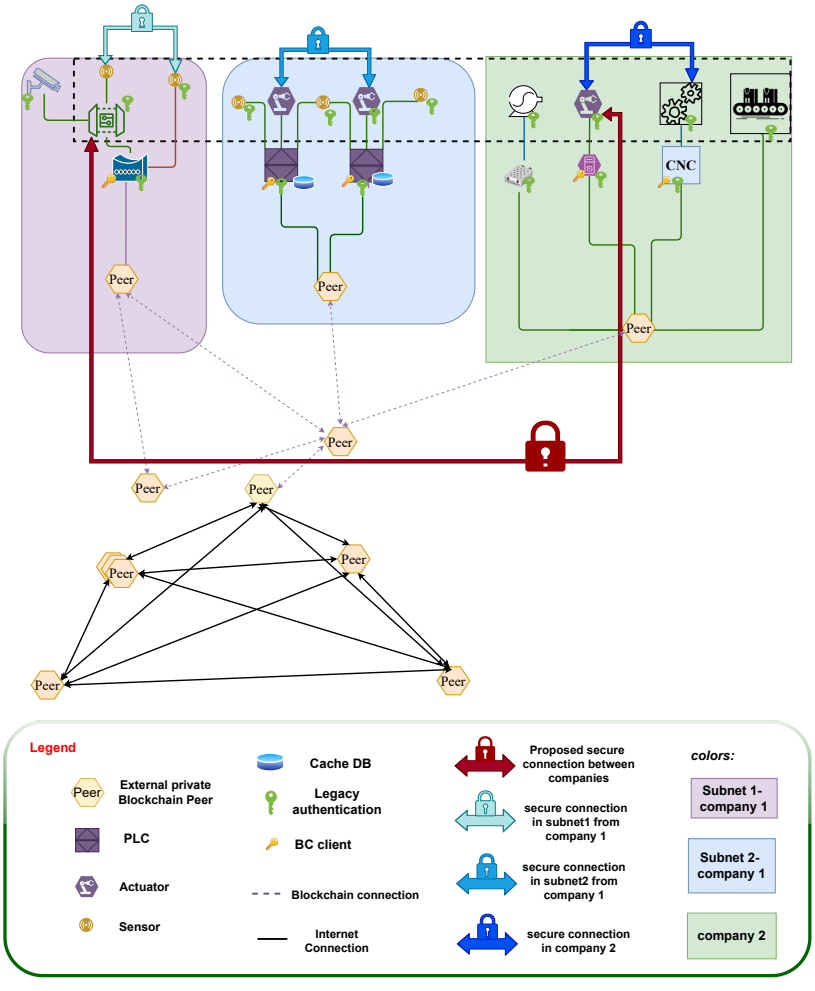

Figure 3. Cross authentication between different subnets.

4.2. Cross-Fieldbus Authentication Model

The authentication model in this study relies on X.509 certificates, which are asymmetric objects in credential form that can be used for authentication during the TLS handshake. TLS is a well-established and widely recognized solution for achieving confidentiality, integrity, and authenticity in secure communication on the internet. However, using TLS can significantly increase communication and computing effort, especially during the handshake phase when client and server authentication and connection key derivation take place.

The key idea of this model is to establish trust between two participants who share only one common root of trust by validating a subordinate certificate through the creation and verification of the certificate chain up to the trust anchor. This enables a direct relationship of trust to be established between participants who may have otherwise never been in contact before.

In the case of blockchain nodes, trust between nodes can be established based on the trust value list stored in the blocks and the trust management system used. However, in areas without blockchain nodes, such as different subnetworks, direct authentication between nodes is not possible, and different authentication protocols may be used. To illustrate the authentication process and its steps, a sequence diagram is provided in Figure 4.

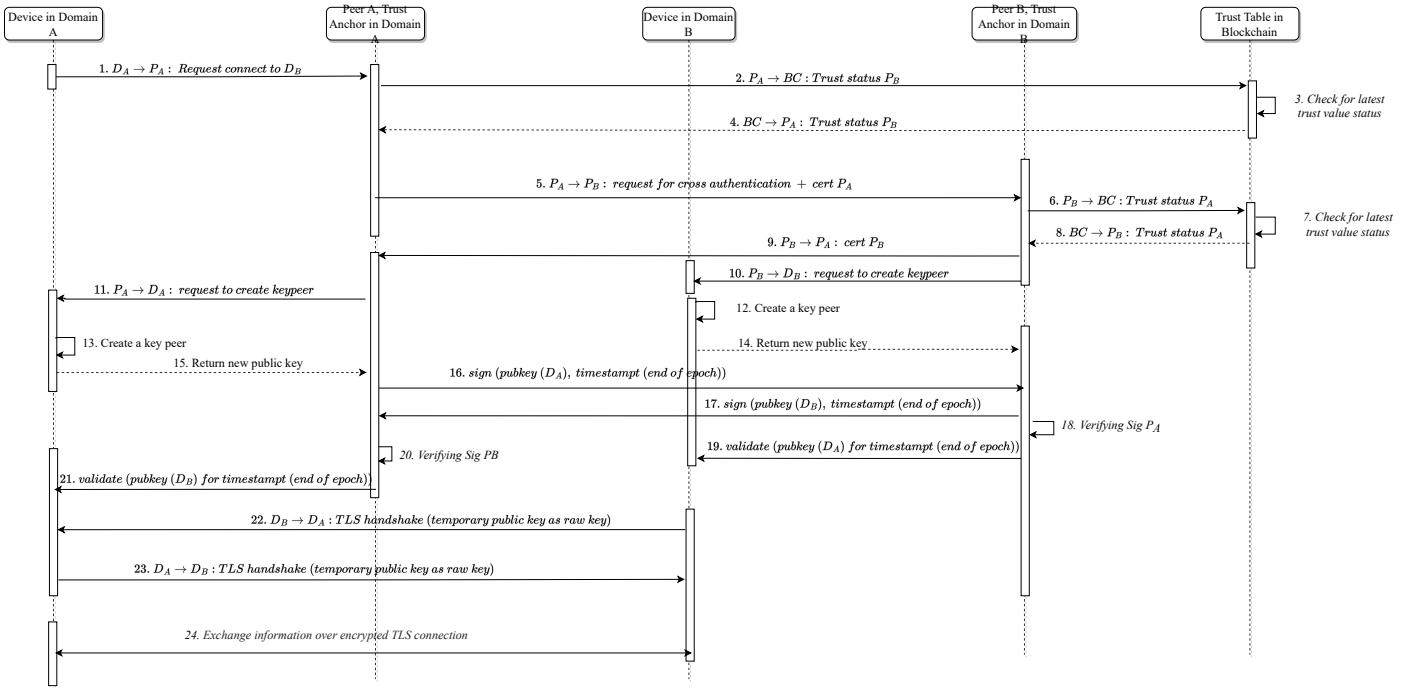

Figure 4. Cross authentication sequence diagram.

In Figure 4, cross authentication sequence diagram is presented to illustrate the flow of interactions between components in a system. To aid in understanding the diagram, Table 1 provides a set of symbols along with their corresponding explanations. In the following steps, explains the authentication process.

- D_A the request function $Valid(D_B)$ to check if the registration time in the domain B is valid. P_A query operation is performed on the consortium blockchain from trust value lists and the result $(P_B||T_i)$ is returned. If T_i is not valid, then P_A return the refuse request D_A for connection to D_B and finish the session (steps 1–4 in Figure 4).
- P_A request to P_B to connect to D_B. P_B checks the validity of device $(P_A||T_i)$ to check if P_A is trustful or not. After it P_B is decided based on trust value P_A that continue to communicate or finish the session (steps 5–8 in Figure 4) .
- If P_B decide to continue, request to $Valid(D_A)$ to P_A. P_A sign the $certD_A$ and send it D_A and approve to allowance to have a connection (steps 9–21 in Figure 4).

- D_B send the TLS handshake with D_A with temporary public key (step 22 in Figure 4).
- D_A send the TLS handshake with D_B with temporary public key (step 23 in Figure 4).
- Establishing a session between D_A and D_B, and exchange information over encrypted TLS connection (step 24 in Figure 4).

Table 1. Description of symbols.

Description	Parameter
Device in domain A	D_A
Peer in domain A	P_A
Device in domain B	D_B
Peer in domain B	P_B
Trust value device i	T_i
Blockchain	BC
Certificate	Cert
Signature	Sig

4.3. Formalize the Protocol

The formal verification rules presented here are a set of axioms and inference rules that are used to prove the correctness of a system or protocol. These rules are expressed in first-order logic and are used to reason about the behavior of the system or protocol in a rigorous and systematic manner. The rules presented here include the Belief Rule, which governs the propagation of beliefs among parties, the Authentication Rule, which ensures that messages are authenticated by the appropriate parties, the Key Generation Rule, which governs the generation of key pairs, the Key Distribution Rule, which governs the distribution of keys, and the Hashing Rule, which ensures that messages are not tampered with during transmission. By applying these rules, one can rigorously prove the correctness of a system or protocol, which is essential for ensuring the security and reliability of computer systems.

4.3.1. Rules Definition

Belief Rule:

$$\forall P_A, X, Y \left(\left(Believes(P_A, X) \wedge (X \Rightarrow Y) \right) \Rightarrow Believes(P_A, Y) \right)$$

Let X be "Trust Status(P_B) = Good" and Y be "Can Establish Connection(P_A, A, B)"

$$\forall P_A, P_B \left(\left(Believes(P_A, TrustStatus(P_B) = Good) \wedge SendsCertificate(P_B, P_A) \right) \Rightarrow \right.$$
$$\left. Believes(P_A, CanEstablishConnection(P_A, A, B)) \right)$$

Assume that an agent P_A believes a proposition X and X implies another proposition Y. Use the definition of implication to show that if X implies Y, then the negation of Y implies the negation of X. Assume that P_A does not believe Y and show that this leads to a contradiction. Conclude that P_A must believe Y.

Authentication Rule:

$$\forall P_A, B, M, K_B \left(\left(ReceivesMessage(P_A, M) \wedge SignedBy(M, B, K_B) \right) \right.$$
$$\left. \wedge Believes(P_A, BelongsTo(K_B, B)) \right) \Rightarrow Believes(P_A, Sent(M, B)) \Big)$$

Let K'_A be the new key pair generated by A. Assume that an agent P_A receives a message M that is signed by another agent B using a key K_B, and P_A believes that the signature is valid and belongs to B. Assume that P_A believes that B belongs to the key K_B. Use the definition of digital signature to show that if M is signed by B using K_B, then M must have been sent by B. Conclude that P_A should believe that M was sent by B.

Key Generation Rule:

$$\forall A, K'_A \Big(GeneratesKeyPair(A, K'_A) \Rightarrow \big(Believes(A, BelongsTo(K'_A, A)) \wedge Believes(A, \neg KnowsPrivateKey(K'_A)) \big) \Big)$$

Let K'_A be the new key pair generated by A and K'_B be the new key pair generated by B. Assume that an agent A generates a new key pair K'_A. Use the definition of key generation to show that if A generates a new key pair, then A should believe that it owns the private key and that no one else knows it. Conclude that A should believe that it owns the private key and that no one else knows it.

Key Distribution Rule:

$$\forall P_A, P_B, K'_A, T \Big(Sends(P_A, Signs(K'_A, A, T)) \wedge Believes(P_B, BelongsTo(K'_A, A)) \wedge Believes(P_B, SignatureValid(Signs(K'_A, A, T))) \Rightarrow CanDecrypt(P_B, M, EncryptsWith(M, K'_A)) \Big)$$

Assume that an agent P_A sends a signed message to another agent P_B using a key pair K'_A. Assume that P_B believes that K'_A belongs to A, and P_B believes that the signature is valid. Use the definition of encryption and decryption to show that if P_B believes that K'_A belongs to A, and P_B believes that the signature is valid, then P_B should be able to decrypt the message using the public key. Conclude that P_B should be able to decrypt the message using the public key.

Hashing Rule:

$$\forall P_A, P_B, M, M' \Big(\big(ReceivesMessage(P_A, M) \wedge SignedBy(M, A, K'_A, T) \wedge Believes(P_A, BelongsTo(K'_A, A)) \wedge Believes(P_A, SignatureValid(Signs(M, A, K'_A, T))) \wedge ReceivesMessage(P_B, M') \wedge SignedBy(M', B, K'_B, T) \wedge Believes(P_B, BelongsTo(K'_B, B)) \wedge Believes(P_B, SignatureValid(Signs(M', B, K'_B, T))) \wedge (Hash(M) = Hash(M')) \big) \Rightarrow \big(Believes(P_A, M = M') \wedge Believes(P_B, M = M') \big) \Big)$$

Assume that an agent P_A receives a message M that is signed by another agent A using a key K'_A and that P_A believes that the signature is valid and belongs to A. Assume that P_A believes that A belongs to the key K'_A. Assume that an agent P_B receives a message M' that is signed by another agent B using a key K'_B and that P_B believes that the signature is valid and belongs to B. Assume that P_B believes that B belongs to the key K'_B. Use the definition of hashing to show that if two messages have the same hash value, then they are identical. Use the definition of digital signature to show that if M and M' are signed by the correct device.

4.3.2. Proof of the Belief Rule Using First-Order Logic

Premises:

1. $\forall P_A, X, Y \ (Believes(P_A, X) \wedge (X \Rightarrow Y) \Rightarrow Believes(P_A, Y))$
2. $Believes(P_A, TrustStatus(P_B) = Good) \wedge SendsCertificate(P_B, P_A)$
3. $X =$ "TrustStatus(P_B) = Good"
4. $Y =$ "CanEstablishConnection(P_A, A, B)"
5. $X \Rightarrow Y$

Conclusion:

$Believes(P_A, CanEstablishConnection(P_A, A, B))$

Proof:

1. $Believes(P_A, X)$ (Assumption)
2. $X \Rightarrow Y$ (Assumption)
3. $Believes(P_A, X \Rightarrow Y)$ (From 1 and 2, by Modus Ponens)
4. $Believes(P_A, Y)$ (From 3 and the Belief Rule)
5. $Y =$ "CanEstablishConnection(P_A, A, B)" (Assumption)
6. $Believes(P_A, CanEstablishConnection(P_A, A, B))$ (From 4 and 5, by Substitution)

Therefore, we have proved that if a party P_A believes that the trust status of another party P_B is good and P_B sends a certificate to P_A, then P_A believes that they can establish a connection with P_B.

5. Evaluation and Security Analysis

The Evaluation and Security Analysis section of this report consists of several subsections, including formal proof, addressing the vulnerabilities identified in Section 3.3, and benefits. In the formal proof subsection, we provide a rigorous mathematical demonstration of the correctness of the proposed solution. The addressing vulnerabilities subsection describes how we have identified and addressed potential security risks in the system. Finally, the benefits subsection outlines the advantages of the proposed solution over proposed scheme.

5.1. Addressing the Vulnerabilities of Section 3.3

We conduct a security study of the proposed strategy, taking the aforementioned possible risks into consideration.

1. Man-in-the-middle attack: any two communicating parties' communication data is symmetrically encrypted using the TLS session key, which eliminates the risk of leaking private data. Even if the data is stolen, the attacker will be unable to decipher future ciphertexts in order to acquire meaningful information due to the use of Perfect Forward Secrecy [34].
2. 51% attack: according to the blockchain consensus method, an attacker may compromise the blockchain system's security only if they control more than 51% of the nodes or arithmetic power, which is considered unfeasible in terms of practicality and likelihood [35]. Furthermore, for authentication, peers for each subsystem verify the other side's peer trust value, lowering the danger of connecting to a rogue node.
3. Replay attack: random values and a counter for nodes in each session are used to guarantee that communication messages remain current across sessions, avoiding replay attacks [34].
4. Sybil Attack: Schloss has a TMS that accomplishes the objective via the use of a trust-based mechanism. Schloss is used as a trust factor when routing choices are made and rogue nodes are detected. The choice is made entirely on the basis of node trust, and bad nodes are swiftly separated from the network.
5. Spam attack: blockchain technology has the potential to guard against spam assaults [36]. All communication is handled as transactions, and each transaction is given a time stamp indicating that it requires a consensus phase to take effect. As a result, an attacker cannot insert spam messages since they would be rejected by the consensus process.

5.2. Benefits

The suggested schema provides an additional verification layer to the system, which can be used in conjunction with authentication management to dynamically manage access and communication between nodes in a distributed manner. This enhanced security mechanism is based on blockchain authentication, which allows for more secure and transparent communication.

While this added layer of security is promising, it is important to note that any new system element can also introduce new attack surfaces that must be carefully considered. Thus, to ensure the effectiveness of this security mechanism, a comprehensive security analysis must be conducted to identify and address any vulnerabilities in the system.

The security analysis should include a thorough evaluation of the system's architecture, communication protocols, and access controls. It should also assess the potential impact of attacks on the confidentiality, integrity, and availability of the system's data and resources. Based on the results of the analysis, appropriate security measures and countermeasures should be implemented to mitigate any identified risks.

Overall, by incorporating this proposed schema into the system and conducting a thorough security analysis, organizations can enhance the security of their networks and systems, enabling more secure and reliable communication between nodes.

6. Conclusions

In this study, we have introduced a novel certificate-based cross-domain authentication mechanism tailored for various field devices operating in industrial environments. Our approach goes beyond the standard authentication system by incorporating several key improvements. Firstly, we leverage a cross-domain authentication technique that relies on trust values generated by blockchain nodes, enabling secure and reliable authentication across different domains. This ensures that devices from separate domains can establish trust and authenticate each other effectively.

Furthermore, we have developed a robust multi-domain joint authentication mechanism, which enables coordinated authentication processes among multiple domains. This mechanism promotes seamless and efficient authentication procedures, facilitating interoperability and collaboration among different entities within industrial networks.

To guarantee the confidentiality and integrity of communication channels, we have employed end-to-end secure communication utilising the TLS (Transport Layer Security) protocol. This ensures that data transmitted between authenticated devices remains protected against unauthorised access or tampering.

By synergistically combining these approaches, we have successfully created a decentralized cross-domain authentication mechanism. This mechanism offers enhanced security, efficiency, and interoperability for industrial settings, where the authentication of diverse field devices is essential for maintaining operational integrity and safeguarding critical processes.

Moving forward, we are committed to further advancing this area of research. Our future endeavors will focus on exploring connections with other industrial authenticator frameworks to foster compatibility and seamless integration. Additionally, we plan to investigate the incorporation of hardware-based authentication techniques, leveraging the latest advancements in hardware security, to augment the overall robustness and resilience of our authentication mechanism.

Overall, our proposed mechanism holds immense potential in elevating the security and efficiency of authentication practices in industrial settings. By addressing the unique challenges and requirements of cross-domain authentication, we aspire to inspire further research and development efforts in this critical domain, driving advancements in industrial security and fostering a safer and more interconnected industrial landscape.

Author Contributions: Conceptualization, F.S.; methodology, F.S.; formal analysis, F.S.; writing—original draft preparation, F.S.; writing—review and editing, C.R.; visualization, F.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Federal Ministry of Education and Research (BMBF) under reference number COSMIC-X 02J21D144, and supervised by Projektträger Karlsruhe (PTKA).

Data Availability Statement: All data were presented in main text.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dzung, D.; Naedele, M.; Von Hoff, T.P.; Crevatin, M. Security for industrial communication systems. *Proc. IEEE* **2005**, *93*, 1152–1177. [CrossRef]
2. Prinsloo, J.; Sinha, S.; von Solms, B. A review of industry 4.0 manufacturing process security risks. *Appl. Sci.* **2019**, *9*, 5105. [CrossRef]
3. Schönle, D.; Wallis, K.; Stodt, J.; Reich, C.; Welte, D.; Sikora, A. Industry Use Cases on Blockchain Technology. In *Industry Use Cases on Blockchain Technology Applications in IoT and the Financial Sector*; IGI Global: Hershey, PA, USA, 2021; pp. 248–276.

4. Mumtaz, S.; Alsohaily, A.; Pang, Z.; Rayes, A.; Tsang, K.F.; Rodriguez, J. Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation. *IEEE Ind. Electron. Mag.* **2017**, *11*, 28–33. [CrossRef]
5. Tiwari, S.; Rosak-Szyrocka, J.; Żywiołek, J. Internet of things as a sustainable energy management solution at tourism destinations in India. *Energies* **2022**, *15*, 2433. [CrossRef]
6. Stodt, J.; Schönle, D.; Reich, C.; Ghovanlooy Ghajar, F.; Welte, D.; Sikora, A. Security audit of a blockchain-based industrial application platform. *Algorithms* **2021**, *14*, 121. [CrossRef]
7. Adaros Boye, C.; Kearney, P.; Josephs, M. Cyber-risks in the industrial internet of things (IIoT): Towards a method for continuous assessment. In *Proceedings of the International Conference on Information Security, Guildford, UK, 9–12 September 2018;* Springer: Berlin/Heidelberg, Germany, 2018; pp. 502–519.
8. Stodt, F.; Stodt, J.; Reich, C. Blockchain Secured Dynamic Machine Learning Pipeline for Manufacturing. *Appl. Sci.* **2023**, *13*, 782. [CrossRef]
9. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
10. Ghajar, F.G.; Sartakhti, J.S.; Dorri, A. Providing a Model for Creating Trust and Guaranteeing the Originality of Goods in the Machine Woven Carpet Supply Chain Based on Blockchain. *Pharmaceuticals* **2020**, *3*, 10.
11. Chod, J.; Trichakis, N.; Tsoukalas, G.; Aspegren, H.; Weber, M. On the financing benefits of supply chain transparency and blockchain adoption. *Manag. Sci.* **2020**, *66*, 4378–4396. [CrossRef]
12. Ghovanlooy Ghajar, F.; Salimi Sratakhti, J.; Sikora, A. Sbtms: Scalable blockchain trust management system for vanet. *Appl. Sci.* **2021**, *11*, 11947. [CrossRef]
13. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Karimipour, H.; Srivastava, G.; Aledhari, M. Enabling drones in the internet of things with decentralized blockchain-based security. *IEEE IoT J.* **2020**, *8*, 6406–6415. [CrossRef]
14. Jia, X.; Hu, N.; Su, S.; Yin, S.; Zhao, Y.; Cheng, X.; Zhang, C. IRBA: An identity-based cross-domain authentication scheme for the internet of things. *Electronics* **2020**, *9*, 634. [CrossRef]
15. Zhang, Q.; Gan, Y.; Zhang, Q.; Wang, R.; Tan, Y.-A. A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application. *IEEE Access* **2018**, *6*, 24064–24074.
16. Lee, Y.; Yoon, J.; Choi, J.; Hwang, E. A Novel Cross-Layer Authentication Protocol for the Internet of Things. *IEEE Access* **2020**, *8*, 196135–196150. [CrossRef]
17. Shawky, M.A.; Abbasi, Q.H.; Imran, M.A.; Ansari, S.; Taha, A. Cross-layer authentication based on physical-layer signatures for secure vehicular communication. In Proceedings of the 2022 IEEE Intelligent Vehicles Symposium (IV), Aachen, Germany, 5–9 June 2022; pp. 1315–1320.
18. Chen, Q.; Li, Z.; Yu, S. A cross-authentication model for heterogeneous domains in active networks. In Proceedings of the IEEE 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007), Dalian, China, 18–21 September 2007; pp. 140–143.
19. Jan, S.U.; Abbasi, I.A.; Algarni, F. A mutual authentication and cross verification protocol for securing Internet-of-Drones (IoD). *Comput. Mater. Contin.* **2022**, *72*, 5845–5869.
20. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
21. Guo, S.; Wang, F.; Zhang, N.; Qi, F.; Qiu, X. Master-slave chain based trusted cross-domain authentication mechanism in IoT. *J. Netw. Comput. Appl.* **2020**, *172*, 102812. [CrossRef]
22. Wang, M.; Rui, L.; Yang, Y.; Gao, Z.; Chen, X. A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2664–2676. [CrossRef]
23. Zhong, H.; Gu, C.; Zhang, Q.; Cui, J.; Gu, C.; He, D. Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things. *Ad Hoc Netw.* **2023**, *144*, 103137. [CrossRef]
24. Yuan, W.; Li, X.; Li, M.; Zheng, L. DCAGS-IoT: Dynamic Cross-Domain Authentication Scheme Using Group Signature in IoT. *Appl. Sci.* **2023**, *13*, 5847. [CrossRef]
25. Huang, C.; Xue, L.; Liu, D.; Shen, X.; Zhuang, W.; Sun, R.; Ying, B. Blockchain-assisted transparent cross-domain authorization and authentication for smart city. *IEEE IoT J.* **2022**, *9*, 17194–17209. [CrossRef]
26. Xue, L.; Huang, H.; Xiao, F.; Wang, W. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2409–2420. [CrossRef]
27. Zhang, H.; Chen, X.; Lan, X.; Jin, H.; Cao, Q. BTCAS: A blockchain-based thoroughly cross-domain authentication scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102538. [CrossRef]
28. Wang, W.; Hu, N.; Liu, X. BlockCAM: A blockchain-based cross-domain authentication model. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; pp. 896–901.
29. Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 942–954. [CrossRef]
30. Ghovanlooy Ghajar, F.; Sikora, A.; Welte, D. Schloss: Blockchain-based system architecture for secure industrial iot. *Electronics* **2022**, *11*, 1629. [CrossRef]

31. Aslam, S.; Tošić, A.; Mrissa, M. Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions. *J. Cybersecur. Priv.* **2021**, *1*, 164–194. [CrossRef]
32. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
33. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2985–2996. [CrossRef]
34. Esfahani, A.; Mantas, G.; Matischek, R.; Saghezchi, F.B.; Rodriguez, J.; Bicaku, A.; Maksuti, S.; Tauber, M.G.; Schmittner, C.; Bastos, J. A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE IoT J.* **2017**, *6*, 288–296. [CrossRef]
35. Yin, D.; Zhang, L.; Yang, K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. *IEEE Access* **2018**, *6*, 24694–24705. [CrossRef]
36. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]