



Article

A Secure Protocol Authentication Method Based on the Strand Space Model for Blockchain-Based Industrial Internet of Things

Huanhuan Gu ¹, Jing Shang ^{2,*} , Pengchuan Wang ², Jingfeng Mi ³ and Aniruddha Bhattacharjya ^{4,*} 

¹ School of Cyber Science and Engineering, Nanjing University of Science and Technology, Wuxi 214400, China; guhuanhuan@njjust.edu.cn

² School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China; wangpc@njjust.edu.cn

³ Nanjing Sinovatio Technology Co., Ltd., Nanjing 211111, China; mi.jingfeng@sinovatio.com

⁴ Department of Electronic Engineering, Tsinghua University, Beijing 100190, China

* Correspondence: shangjing@njjust.edu.cn (J.S.); li-an15@tsinghua.org.cn (A.B.)

† PhD Alumni, Department of Electronic Engineering, Tsinghua University, Beijing 100190, China.

Abstract: The rapid development of the Industrial Internet of Things (IIoT) and its application across various sectors has led to increased interconnectivity and data sharing between devices and sensors. While this has brought convenience to users, it has also raised concerns about information security, including data security and identity authentication. IIoT devices are particularly vulnerable to attacks due to their lack of robust key management systems, efficient authentication processes, high fault tolerance, and other issues. To address these challenges, technologies such as blockchain and the formal analysis of security protocols can be utilized. And blockchain-based Industrial Internet of Things (BIIoT) is the new direction. These technologies leverage the strengths of cryptography and logical reasoning to provide secure data communication and ensure reliable identity authentication and verification, thereby becoming a crucial support for maintaining the security of the Industrial Internet. In this paper, based on the theory of the strand space attack model, we improved the Fiber Channel Password Authentication Protocol (FACP) security protocol in the network environment based on symmetric cryptography and asymmetric cryptography. Specifically, in view of the problem that the challenge value cannot reach a consensus under the symmetric cryptography system, and the subject identity cannot reach a consensus under the asymmetric cryptography system, an improved protocol is designed and implemented to meet the authentication requirements, and the corresponding attack examples are shown. Finally, the effectiveness and security of the protocol were verified by simulating different networking environments. The improved protocol has shown an increase in efficiency compared with the original protocol across three different network configurations. There was a 6.43% increase in efficiency when centralized devices were connected to centralized devices, a 5.81% increase in efficiency when centralized devices were connected to distributed devices, and a 6.32% increase in efficiency when distributed devices were connected to distributed devices. Experimental results show that this protocol can enhance the security and efficiency of communication between devices and between devices and nodes (servers, disks) in commonly used Ethernet passive optical network (EPON) environments without affecting the identity authentication function.

Keywords: industrial internet of things (IIoT); secure protocol authentication; Ethernet passive optical network (EPON); blockchain-based industrial internet of things (BIIoT); strand space model; fiber channel certificate authentication protocol (FCAP)



Citation: Gu, H.; Shang, J.; Wang, P.; Mi, J.; Bhattacharjya, A. A Secure Protocol Authentication Method Based on the Strand Space Model for Blockchain-Based Industrial Internet of Things. *Symmetry* **2024**, *16*, 851. <https://doi.org/10.3390/sym16070851>

Academic Editors: Shange Gao and Sergei D. Odintsov

Received: 16 May 2024

Revised: 8 June 2024

Accepted: 29 June 2024

Published: 5 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Over the past few years, the IIoT has witnessed significant growth and advancement. Nowadays, large-scale deep models are deployed on numerous devices and embedded systems, which has become a successful paradigm for transforming traditional lifestyles into high-tech lifestyles [1]. With the continuous development of computer and network

technology, there has been unprecedented growth in connected devices such as embedded sensors, smart devices, and smart vehicles [2]. The vast amounts of sensitive data generated by these devices need to be properly protected to prevent unauthorized access and potential data tampering. To address this challenge, encryption and authentication mechanisms must be implemented to ensure the security and integrity of communications between devices [3]. In this context, blockchain technology [4–8] has shown its potential in building secure and reliable distributed databases. This technology provides a platform for sharing, replication, and synchronization for the industrial Internet through distributed ledgers (often called BIIoT), thereby enhancing the stability and security of data sharing [9,10]. In addition, with the rise of cross-chain technology, secure access to the access chain and cross-chain identity authentication have become new focuses. To solve these problems, many industries have urged to adopt EPON as the main communication network architecture to improve overall network performance and security.

Security protocols are an important means to ensure network information security [11]. Different from shared databases based on blockchain, the industrial sector generally adopts EPON as a Cyber–Physical System (CPS) application to strictly collect and monitor all information in physical space and then synchronize this information to cyberspace, which greatly increases the attack surface. EPON can be seamlessly connected to existing Ethernet and Fiber Channel (FC) storage devices in the data center and has the advantages of significantly reducing switching infrastructure, reducing the number of network card adapters and cables, and significantly reducing power and cooling costs. Many well-known IT companies have invested in the research development and production of EPON products, such as Brocade, Intel, Broadcom, Cisco, Qlogic, and Emulex [12]. At the same time, the requirements for the security and protection mechanisms of EPON networks are becoming higher and higher. Due to the immaturity of research in security-protocol-related fields, EPON security issues cannot be avoided [13]. The most typical security threats include unauthorized access, spoofing, etc. EPON can be effectively combined with various identity authentication protocols to strengthen the security of network systems. Identity authentication is a fundamental aspect when it comes to establishing a secure network system [14]. The authentication protocols supported by EPON include FCAP, Fiber Channel Password Authentication Protocol (FCPAP), Fiber Channel Extensible Authentication Protocol (FCEAP), etc. [15,16]. With the advancement of technology, certificate-based authentication protocols are more in line with current and future security needs. FCAP, as a certificate-based authentication protocol, offers higher security than password-based protocols. Researchers have proposed a variety of analysis methods and means. Fabrega has [17] introduced the concept of strand space form as a means to analyze protocol execution. The theory of strand space considers the causal dependence between events and reduces the status of the protocol combined with the theorem proving method. Therefore, strand space theory can analyze protocols of infinite size without limiting the rounds in which the subject participates in the running of the protocol, avoiding the state space explosion problem common in model-checking methods. Strand space theory expresses the execution process of the protocol through a graph-based structure, which is not only simple and intuitive but also makes it easier to analyze the protocol's security using graph theory and algorithms [18,19]. In addition, with the development of group communication applications, strand space theory has gradually been applied to analyze the security of group communication protocols [20].

In this paper, we focus on FCAP as the research object and propose improvements to the strand space model in the EPON network environment based on password systems [21]. There is relatively little research on FCAP in the existing literature, and this paper can fill this research gap by studying FCAP. This paper makes several significant contributions, which can be summarized as follows:

1. We introduce an advanced strand space model for FACP to address the challenge of achieving consensus on the challenge value in symmetric cryptographic systems. We successfully meet the authentication requirements by incorporating challenge values

- that cannot reach consensus in message components and provide corresponding attack instances to illustrate the potential vulnerabilities and risks associated with this scenario;
2. For the issue of nonconsensus on principal identities in asymmetric cryptographic systems, we propose an improved strand space model for FACP. By incorporating nonconsensus principal identities into message components, we effectively fulfill the authentication requirements. We also present attack instances that highlight the implications and risks when principal identities cannot achieve consensus in asymmetric cryptographic systems;
 3. We designed and implemented the proposed enhanced protocol, and its effectiveness and security are confirmed through simulations in various network environments.

The structure of the paper unfolds as follows: The second Section 2 presents a comprehensive survey of FACP and protocol formal analysis methods. The FCAP protocol and strand space model are given in Section 3, and the attacker model is elaborated here. The extended testing methods for certification are detailed in Section 4. Section 5 has showcased the model analysis of the extended FCAP strand space model. In Section 6, we conduct security and performance tests on the improved protocol. Finally, Section 7 summarizes the findings and concludes the paper.

2. Related Works

With the rise of Industry 4.0, IIoT is rapidly becoming a key driver of intelligent manufacturing and automation. The high-reliability requirements of IIoT stem from its role in critical infrastructure and systems such as energy management, traffic control, and smart manufacturing. Failures in these systems can lead to significant economic losses, safety risks, and even loss of life. Therefore, ensuring the security and stability of IIoT networks is crucial for maintaining the continuity and efficiency of industrial operations. This study aims to explore how to build a secure and efficient IIoT environment by integrating the strand space model with EPON architecture. We proposed a novel authentication method to enhance the authentication process of users and devices and contributed to a niche area of study that is vital for advancing network security protocols.

In the realm of IIoT, the convergence of blockchain technology with EPON architectures is emerging as a pivotal strategy to bolster network security and streamline user authentication processes. Blockchain's decentralized ledger offers an innovative framework for managing the authentication of users and devices within the IIoT, reducing reliance on centralized authorities and fortifying the system against a single point of failure. We called this type of architecture BIIoT. Usman and his team developed a highly scalable regional access control system based on blockchain technology [22]. The system is designed to deal with data leakage and data integrity issues that resource-constrained devices in the IIoT may encounter and is committed to improving the efficiency and response speed of information management. As an efficient communication architecture, EPON can be combined with blockchain technology to provide more stable and high-quality services and meet the high-reliability requirements of IIoT. To mitigate security risks in the system, Roh [23], for instance, designed an authentication and session key exchange protocol as a solution, but this increased the cost due to the need for an authentication server. Pedro et al. [24] introduced a method to enhance system security through a key exchange protocol. In the context of EPON, encryption of the preamble in each frame is employed to ensure its uniqueness, but this approach can significantly increase system delays. To ensure the security of the EPON protocol in the industrial environment, researchers have explored different analysis methods and models, including the formal logic method [25] and the formal analysis method [26].

The formal logic method is a method based on mathematical logic for describing and verifying the properties and properties of security protocols. Burrows et al. [27] first proposed Burrows–Abadi–Needham (BAN) logic based on knowledge and belief using formal logic methods. This logic was used to analyze the security of several classic

authentication protocols, such as Needham–Schroeder and Kerberos, and successfully discovered known and unknown vulnerabilities in the protocols. It describes the security requirements of the protocol by defining the protocol's status, messaging, and attack models and using logical formulas. Subsequently, the researchers have expanded the BAN logic and proposed GNY logic [28], AT logic, VO logic, and SVO logic [29]. Formal logic methods can be used to discover logical loopholes and weaknesses in protocols and verify whether the protocol meets expected security properties.

The formal analysis method is a method of detailed analysis and verification of protocols using mathematical tools and techniques. A variety of model-checking tools have emerged, such as Brutus [30] for analyzing security protocols and Symbolic Model Checking (SMV) based on symbolic model-checking technology developed in [31]. Another type of formal analysis method is the method based on theorem proving, which is a new research hotspot in security protocols. The most representative of the theorem proving methods are the inductive method [32] and strand space theory [33–35]. Researchers have conducted a lot of work on applying strand space theory to the formal analysis of security protocols and achieved corresponding results. Dong et al. [36] performed a comprehensive analysis by combining the chain space model with cross-routing attacks, specifically targeting the route reply phase of routing protocols. This analysis aims to identify and understand the potential vulnerabilities and risks associated with this phase and deduce various attacks that could potentially result in the nonexistence of routes. Focardi [35] proposed an innovative approach to key management by introducing a policy model based on the strand space theory. Xiao [37] made significant contributions by expanding the strand space theory and applying a hybrid chain space model to analyze the security of the AKA protocol. Through this analysis, they were able to identify and expose multiple previously unknown attacks.

In asymmetric cryptographic systems, if a consensus on the principal identity cannot be reached, it means that the parties involved in the communication cannot effectively verify each other's identity. This situation can lead to serious security risks, including identity impersonation, Man-in-the-Middle attacks (MITM), and breaches of data integrity and confidentiality, as well as Denial-of-Service attacks (DoS). Once the consensus on identity is missing, the entire security architecture may be compromised, making the system vulnerable to exploitation by attackers. Therefore, ensuring accurate consensus on principal identity in asymmetric cryptographic systems is crucial for maintaining communication security and data protection.

With the support of blockchain technology, a series of analysis methods and models provide in-depth analysis and solid verification tools to improve the security of the EPON protocol. This paper specifically focuses on developing a secure EPON protocol based on strand space theories for the blockchain-based industrial Internet, which can be used to identify potential security risks, discover vulnerabilities and weaknesses in protocols, and provide guidance for improving protocol design. By applying these methods and models, the security of the EPON protocol in the blockchain-based industrial Internet can be strengthened, ensuring the confidentiality and integrity of critical business operations and data.

3. FCAP Protocol and Strand Space Model

3.1. Security Certification of FCAP Protocol

Blockchain-based industrial Internet security is an important component of cyberspace security. FCAP is a secure authentication protocol used for authenticating and encrypting fiber channel network communication, aimed at providing secure data transmission and identity verification to protect the security of communication traffic in the blockchain-based industrial Internet. The authentication process of the FCAP protocol is illustrated in Figure 1.

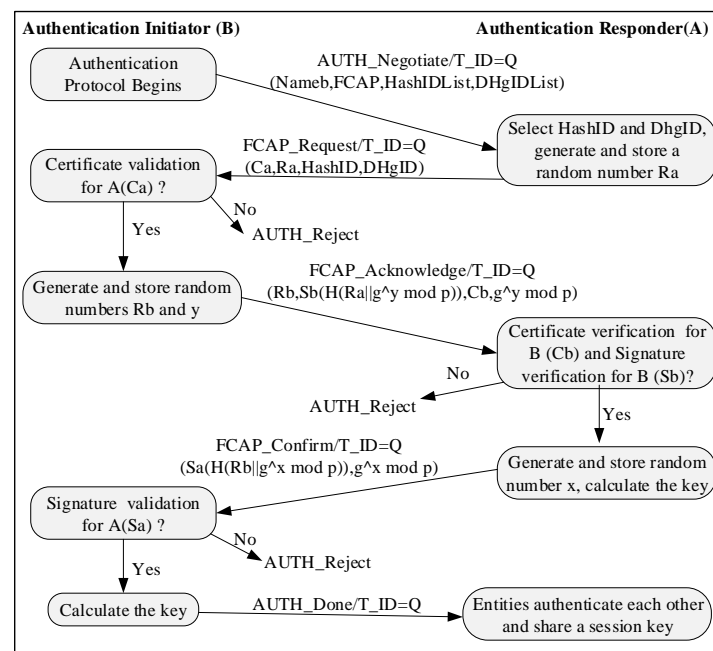


Figure 1. Certification flow chart of FCAP protocol.

The authentication process in the FCAP protocol involves the negotiation of hash functions and Diffie–Hellman (DH) [38,39] identifiers through the *AUTH_Negotiate* message. Upon receiving the *AUTH_Negotiate* message, the authentication responder selects the hash functions and DH identifiers based on the initiator’s supported parameters and sends an *FCAP_Request* message containing Ra , the selected hash ID and DHgID, and the responder’s certificate Ca .

After receiving the *FCAP_Request* message, the authentication initiator validates the responder’s certificate Ca and generates its own random number Rb and a random value y . The initiator then sends an *FCAP_Acknowledge* message to the responder, including its own parameters Rb , DH parameters $g^y \bmod p$, certificate Cb , and signature Sb . Next, the authentication responder verifies the initiator’s certificate Cb and signature Sb , computes the session key Ks if the verification is successful, and sends an *FCAP_Confirm* message containing its own signature Sa and DH parameters $g^x \bmod p$ to the authentication initiator. Finally, the authentication initiator validates the responder’s signature Sa by decrypting it with the RSA public key of the responder. If the signature verification succeeds, the initiator computes the session key Ks and sends an *AUTH_Done* message to the responder to indicate the completion of the authentication process.

3.2. The FCAP Strand Space Model Based on Cryptosystem

The strand space model is an algebraic theorem proving method based on the invariant set, which transforms the description of the protocol and the target security attributes into a graph structure [40]. This is conducive to protocol security analysis with the help of graph theories and algorithms. In the theory of strand space models, strands are used to describe the behavior of entities participating in the protocol sending and receiving messages [41]. A strand is a sequence of actions by honest actors or attackers in the protocol. For an honest party, a strand represents the behavior in a round of the protocol. The strand of an attacker represents a series of actions where the attacker receives messages, tampers with messages, and sends messages. The execution of a protocol is represented by a bundle consisting of multiple strands of honest actors and attackers. Here are some basic definitions in strand space [42].

Definition 1. The strand space model is commonly represented by a tuple (Σ, tr) , where Σ is the set of strands and tr is the trajectory mapping. The construction method for strand space can be described as follows:

- (1) A node is represented as a tuple $\langle s, i \rangle$, where $s \in \Sigma$ and i is an integer that meets $1 \leq i \leq \text{length}(tr(s))$. The set of nodes is denoted as N . Each node $\langle s, i \rangle$ belongs to a unique strand s .
- (2) For a node $n = \langle s, i \rangle \in N$, we define $\text{index}(n) = i$, $\text{strand}(n) = s$, and $\text{term}(n) = (tr(s))_i$. Here, $\text{term}(n)$ represents the i -th symbol item in strand s .
- (3) The relation " \rightarrow " is defined as follows: for nodes $n_1, n_2 \in N$, $n_1 \rightarrow n_2$ indicates that $n_1 = +t$ and $n_2 = -t$. This means n_1 sends message t to n_2 , or n_2 receives message t from n_1 . This relation captures a causal connection in the strand space.
- (4) The relation " \Rightarrow " is defined as follows: for nodes $n_1 = \langle s, i \rangle, n_2 = \langle s, i + 1 \rangle \in N$, $n_1 \Rightarrow n_2$ represents that n_1 is the direct causal predecessor of n_2 on strand s . " \Rightarrow^+ " is used to denote causal predecessors on the same strand s , which may not necessarily be direct causal predecessors.
- (5) An unsigned term t appears in a node $n \in N$ if and only if $t \subset \text{term}(n)$.
- (6) Let I be a set of unsigned terms. A node $n \in N$ is called the entry point of I if and only if $\text{term}(n) = +t$ for some $t \in I$. Additionally, for all nodes $n \Rightarrow^+ n'$, it must satisfy $\text{term}(n) \notin I$.
- (7) An unsigned term t originates from a node $n \in N$ if and only if n is the entry point of the set $I = \{t : t \subset t\}$.
- (8) An unsigned term t has a unique origin if and only if t originates from a unique node $n \in N$.

Therefore, it can be seen that the strand space is constituted by a node set N and edge relations " \rightarrow " and " \Rightarrow ", forming an oriented graph $\langle N, (\rightarrow \cup \Rightarrow) \rangle$.

Definition 2. In the context of an oriented graph $\langle N, (\rightarrow \cup \Rightarrow) \rangle$, a bundle refers to a subgraph denoted as C , which satisfies the following conditions:

- (1) C is a finite set of nodes.
- (2) For any node $n_1 \in N_c$ where $\text{term}(n_1) = -$, there exists a unique node n_2 that satisfies $n_1 \rightarrow n_2 \in C$.
- (3) If $n_1 \in N_c$ and $n_2 \Rightarrow n_1$, then $n_2 \Rightarrow n_1 \in C$.
- (4) C is noncyclic.

Definition 3. Let C be a bundle. The C -height of a strand s , denoted as $C\text{-height}(s)$, is defined as the maximum value of i such that $\langle s, i \rangle \in C$.

3.3. Attacker Model

The adversary model is the most important component in the formalized model of security protocols. Table 1 is the behavior trace of the attacker.

Table 1. Symbols and definitions.

Symbol	Definition
M	Message: $\langle +a \rangle$, where $a \in A$
K	Key: $\langle +K \rangle$, where $K \in K_p$
F	Fetch: $\langle -g \rangle$
T	Transmission: $\langle -g, +g, +g \rangle$
C	Connection: $\langle -g, +h, +gh \rangle$
S	Separation: $\langle -gh, +g, +h \rangle$
E	Encryption: $\langle -k, -h, +\{h\}_k \rangle$
D	Decryption: $\langle -k^{-1}, -\{h\}_{k'}, +h \rangle$

Complex security protocols often consist of multiple individual protocols, including composite security protocols that utilize the D-H protocol as a foundation. The original authentication testing method has certain limitations in analyzing such protocols, as it

only considers some simple operations and cannot describe the increasingly prevalent DH calculation operations used in security protocols. Therefore, an extension to the strand space model is needed.

Assume D is a new set of data types representing the values obtained by DH calculation. The elements of D are d_1, d_2, \dots, d_n , where each element represents a tuple $\langle g, n \rangle$. Here, g represents the generator, and n is an arbitrary exponent. In order to enable the strand space model to describe the DH calculation used in security protocols, its formal definition is as follows:

$$\text{DH calculation : } D \times D \rightarrow D, \quad (1)$$

For example, $DH(d_1, d_2) = g^{xy}$, with $d_1 = g^x, d_2 = g^y$. For the message item, it is necessary to add the following on the existing basis: (1) Add random values from the set $\{1 \dots |G|\}$ to the message item. (2) Add DH calculation $D \times D \rightarrow D$ to the corresponding atomic item. Use D to represent the generator g and the values g^x, g^y, g^{xy} obtained from DH calculation. (3) Add the free DH assumption in the corresponding free assumption. If $DH(d_1, d_2) = DH(d'_1, d'_2)$, then it follows that $d_1 = d'_1$ and $d_2 = d'_2$. (4) Establish the subitem relationship $t \subset DH(d_1, d_2)$ in the corresponding scenario if and only if $t \subset d_1$ or $t \subset d_2$ or $t \subset DH(d'_1, d'_2)$. (5) Append DH calculation $\langle x, -g^y, +g^{xy} \rangle$ to the behavioral trajectory of the attacker's string.

4. Extended Testing Methods for Certification

4.1. Testing Methods for Certification Based on the Strand Space Model

The certification testing method utilizes the strand space model, where all the definitions and properties in the strand space model as its foundation, leveraging all the existing definitions and properties within the model. Additionally, the certification testing method introduces new concepts such as test components, transition edges, target edges, out-tests, in-tests, and active-tests.

Definition 4. A transition edge with respect to $a \in A$ is denoted as $n_1 \Rightarrow^+ n_2$ and defined as follows: If n_1 is a positive node and n_2 is a negative node, and there exists a new component t_2 of n_2 such that $a \subset \text{term}(n_2)$, then the edge $n_1 \Rightarrow^+ n_2$ represents a transition.

Definition 5. A test for a is defined as follows: If a uniquely generates in n_0 and the edge $n_0 \Rightarrow^+ n_1$ is the target edge for a , then $n_0 \Rightarrow^+ n_1$ is referred to as a test for a .

Definition 6. In the strand space Σ , a test component is a specific part of a regular strand that guarantees the existence of other regular strands within the bundle. A term $t = \{h\}_k$ is considered a test component of term a in node n if the following conditions hold: (1) $a \subset t$ and t is a component of n ; (2) t is not a proper subterm of any component of a regular node $n' \in \Sigma$.

- (1) **Out-test:** As shown in Figure 2, $m_0 \Rightarrow^+ m_1$ belongs to bundle C . The data item a is uniquely originated and only is sent out by node m_0 in the form of $\{\dots a \dots\}_K$, where K is secure. Then a is received by node m_1 in a different form other than $\{\dots a \dots\}_K$. In bundle C , there must exist an edge $n_0 \Rightarrow^+ n_1$ that belongs to another valid entity, where $\text{term}(n_0)$ contains component $\{\dots a \dots\}_K$, $\text{term}(n_1)$ contains component t , where $a \subset t$ and $t \neq \{\dots a \dots\}_K$. The edge $n_0 \Rightarrow^+ n_1$ is called a transition edge, symbolically represented as $\{\dots a \dots\}_K \rightarrow a$, and $m_0 \leq n_0 \leq n_1 \leq m_1$.
- (2) **In-test:** As shown in Figure 3, $m_0 \Rightarrow^+ m_1$ belongs to bundle C . If data item a is received by node m_1 in the form of $\{\dots a \dots\}_K$, where K is secure. If a was previously sent by node m_0 in a form different from $\{\dots a \dots\}_K$, then there must exist an edge $n_0 \Rightarrow^+ n_1$ in the bundle C that belongs to another valid entity, where $\{\dots a \dots\}_K \subset \text{term}(n_1)$ and $\{\dots a \dots\}_K \not\subset \text{term}(n_0)$. Assuming the component $t \subset \text{term}(n_1)$, and $a \subset t$, the edge $n_0 \Rightarrow^+ n_1$ is called a transition edge, symbolically represented as $a \rightarrow \{\dots a \dots\}_K$, and $m_0 \leq n_0 \leq n_1 \leq m_1$.

- (3) *Active-test*: If there is a node n in bundle C , where $\{h\}_K \subset \text{term}(n)$ and K is secure, then there must exist another valid node m in bundle C , such that $\{h\}_K \subset \text{term}(m)$.

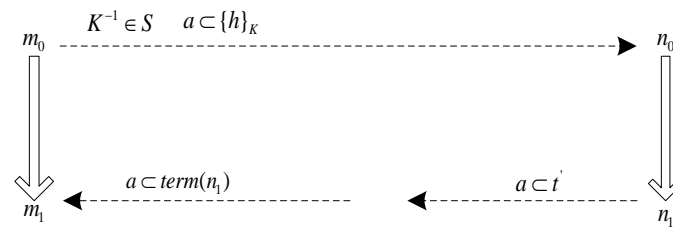


Figure 2. Test method of the out-test.

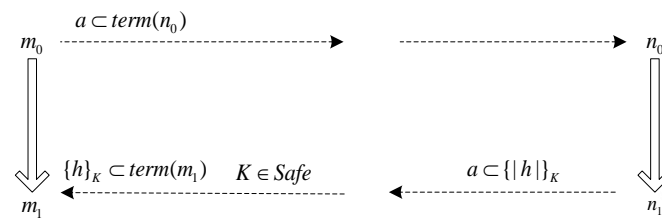


Figure 3. Test method of the in-test.

4.2. Extended Testing Methods for Certification Based on the Strand Space Model

In the strand space model, a new set of data types and DH calculations are added to the message. Additionally, the challenge value C and DH value d are uniquely originated from the same node in terms of FCAP. Considering similar tests involving two data items, we extended the certification testing methods.

Definition 7. Let $a, b(d)$ be terms that uniquely occur in node n_0 . If the edge $n_0 \Rightarrow^+ n_1$ is the target edge for a and $b(d)$, then the pair $(n_0, n_0 \Rightarrow^+ n_1)$ is referred to as a joint test for a and $b(d)$.

- (1) *Extended out-test methods*: If n_0 and $n_0 \Rightarrow^+ n_1$ is a joint test for $a, b(d)$, and $k^{-1} \notin K_p$, then $n_0 \Rightarrow^+ n_1$ is the joint out-test for $a, b(d)$ in n_0 , where $a, b(d)$ are only included in the joint component t of n_0 , and t is the joint test component for $a, b(d)$ in n_0 .
Let C be a bundle, and $n, n' \in C$. Suppose $n_0 \Rightarrow^+ n_1$ is the joint out-test of a and $b(d)$ in n_0 with respect to t , and t_1 is the newly generated joint component. Then, (a) there exists a normal node $m, m \in C$ making t a connected component of m , and $m \Rightarrow^+ m$ is a transition edge of $a, b(d)$. (b) Assuming a and $b(d)$ exist only in the joint component $t_1 = \left\{ \left| h_{a,b(d)} \right| \right\}_k$ of m , where t_1 is not a proper subset of any regular component, and no term in any node is a multiple encryption term, and $k^{-1} \notin K_p$, then there exists a negative regular node where t_1 serves as the joint component.
- (2) *Extended in-test methods*: If $n_0 \Rightarrow^+ n_1$ is a joint test for $a, b(d)$, and $k \notin K_p$, then $t = \left\{ \left| h_{a,b(d)} \right| \right\}_k$ is the joint in-test for $a, b(d)$, where t is the joint test component for $a, b(d)$ in t . Let C be a bundle, and $n, n' \in C$. Suppose $n \Rightarrow^+ n$ is the joint in-test of a and $b(d)$ in $t = \left\{ \left| h_{a,b(d)} \right| \right\}_k$. Then, there exists a regular node $m \in C$, where $t = \left\{ \left| h_{a,b(d)} \right| \right\}_k$ is a joint component of m , and $m \Rightarrow^+ m$ is a transition edge for a and $b(d)$.
- (3) *Extended active-test methods*: If $t = \left\{ \left| h_{a,b(d)} \right| \right\}_k$ is any joint test component of $a, b(d)$ in n , and $k \notin K_p$, then the negative node n serves as a joint active-test for t . Let C be a bundle, and $n \in C$. Suppose n serves as a joint active-test for $t = \left\{ \left| h_{a,b(d)} \right| \right\}_k$, then there exists a positive node $m \in C$, and t is a joint component of m .

5. Model Analysis of Extended FCAP Strand Space Model

The FCAP strand space model consists of legitimate strands (initiator and responder) and illegitimate strands (attacker). In the model, the collections of initiator strings (*Init*),

responder strings ($Resp$), and attacker strands (P) are denoted as $\Sigma = Init \cup Resp \cup P$. The DH values obtained after modulo operation in specific protocols are represented by d_1, d_2 , and $DH(d_1, d_2)$. We use the serial space model to describe FCAP.

5.1. Analysis Method and Extended FCAP Strand Space Model Based on Symmetric Cryptographic System

The analysis of FCAP within the framework of a symmetric cryptographic system is conducted using the extended authentication testing approach in the strand space model. Here, K represents a shared key between entities M and N . The analysis of FCAP using the extended authentication testing method is as follows, where $\langle s, i \rangle$ represents the i th node of strand s . The goal of FCAP is to achieve mutual authentication between M and N .

First, according to the goal of the protocol, N authenticates M . The authentication process is analyzed as follows:

- (1) Construction of test components: As both $C1$ and d_1 are uniquely generated at node m_1 , $h_K(T_i, K_m, C1, DH(d_1, d_2))$ serves as the combined test component for $m_1 \Rightarrow^+ m_2$.
- (2) Extended input testing: Since $C1$ and d_1 uniquely originate from m_1 , there exist regular nodes $n, n' \in C$ such that $term(n') = h_K(T_i, K_m, C1, DH(d_1, d_2))$, and $n \Rightarrow^+ n'$ represents the transition edge for $C1$ and d_1 .
- (3) Definition of node n' : It can be determined that n' is a positive node belonging to the chain S' initiated by protocol participants, represented as $S' = Init[M', N', C1', C2', d'_1, d'_2, DH(d'_1, d'_2)]$, $n' = \langle S', 3 \rangle$, and $term(\langle S', 3 \rangle) = h_K(T_i, K_m, C1, DH(d_1, d_2))$.
- (4) Comparison strand content: By comparing $term(\langle S', 3 \rangle)$ with the components in the initiator strand, the following observations can be made: $M = M', N = N', C2 = C2', DH(d_1, d_2) = DH(d'_1, d'_2)$. From $DH(d_1, d_2) = DH(d'_1, d'_2)$, it can be deduced that $d_1 = d'_1$ and $d_2 = d'_2$.

Therefore, it can be inferred that $C2'$ does not necessarily equal $C2$, indicating that N cannot definitively reach consensus with M on $C2$.

Secondly, according to the goal of the protocol, M certifies N . The certification process is analyzed as follows:

- (1) Constructing test components. As both $C2$ and d_2 are uniquely generated at node n_2 , $h_K(T_i, K_m, C2, DH(d_1, d_2))$ serves as the combined test component for $n_2 \Rightarrow^+ n_3$. $n_2 \Rightarrow^+ n_3$ constructs the combined input test involving $C2$ and d_2 in $h_K(T_i, K_m, C2, DH(d_1, d_2))$.
- (2) Apply the extended input testing method. Since $C2$ and d_2 uniquely originate from n_2 , there exists a normal node $m, m' \in C$ making $term(m') = h_K(T_i, K_n, C2, DH(d_1, d_2))$, and $m \Rightarrow^+ m'$ are the transition edges of $C2, d_2$ in $h_K(T_i, K_n, C2, DH(d_1, d_2))$.
- (3) Definition of node m' : Based on the outcome of (ii), m' is a positive node. Assuming m' is a node in the responder strand S' in the protocol, $S' = Init[M', N', C1', C2', d'_1, d'_2, DH(d'_1, d'_2)]$, $n' = \langle S', 4 \rangle$, and $term(\langle S', 4 \rangle) = h_K(T_i, K_m, C2, DH(d_1, d_2))$.
- (4) Comparison strand content: By comparing $term(\langle S', 4 \rangle)$ and the components in the initiator strand, it can be observed that: $M = M', N = N', C2 = C2', DH(d_1, d_2) = DH(d'_1, d'_2)$. From $DH(d_1, d_2) = DH(d'_1, d'_2)$, we can deduce $d_1 = d'_1$ and $d_2 = d'_2$.

Based on the analysis above, it is concluded that during the N authentication M process, N can only verify that M has participated in one round of the protocol but cannot ensure the successful completion of the entire protocol. Furthermore, consensus cannot be reached on the challenge value $C2$ due to the lack of verification for $C2$. To address these issues, it is proposed to incorporate $C2$ into the message component $R1$ to ensure consensus on the temporary value. Similar conclusions can be drawn for the authentication process of M authenticating N , where consensus cannot be reached on challenge value $C1$ due to the lack of verification for $C1$. Likewise, we suggested including $C1$ in the message component $R2$. As a result, an advanced model of the symmetric cryptographic system is obtained, as shown in Figure 4.

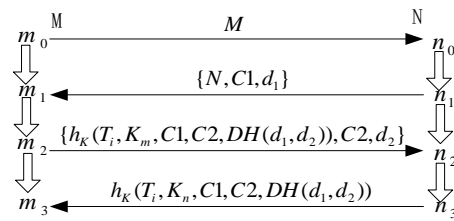


Figure 4. Advanced strand space model under a symmetric cryptosystem.

Furthermore, considering the failure of achieving consensus on challenge value C2, various attack instances can be derived. As shown in Table 2, when authenticating M to N with the same password configuration for M, N, and P, attackers P(M) and P(N) impersonate entities M and N, respectively. By relaying messages in the first and second rounds, and modifying the challenge value in the third round to a new value C2', the attacker has successfully completed the protocol with entity N. This attack is possible due to the absence of challenge value validation in R1.

Table 2. Attack instance of M authentication N.

Event	Sequence of Event
1	$M \rightarrow P(N) : M$
1'	$P(M) \rightarrow N : M$
2'	$N \rightarrow P(M) : N, C1, d_1$
2	$P(N) \rightarrow M : N, C1, d_1$
3	$M \rightarrow P(N) : h_K(T_i, K_n, C1, DH(d_1, d_2)), C2, d_2$
3'	$P(M) \rightarrow N : h_K(T_i, K_n, C1, DH(d_1, d_2)), C2, d_2$
4'	$N \rightarrow P(M) : h_K(T_i, K_n, C2, DH(d_1, d_2))$

5.2. Analysis Method and Extended FCAP Strand Space Model Based on Asymmetric Cryptographic System

Similarly, the following basic assumptions are made: (1) C₁ and d₁ are uniquely generated; (2) C₂ and d₂ are uniquely generated; and (3) C₁ ≠ C₂; (4) d₁ ≠ d₂. According to the goal of the protocol, M authenticates N. For M to authenticate N, we assumed that the key in the fourth message is the private key of N, and K ∉ K_P. The authentication process is as follows:

- (1) Construct the test components. Since C₂ and d₂ are uniquely generated at node n₂, h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)) is the joint test component of n₂ ⇒⁺ n₃. m ⇒⁺ m' constructs the joint in-test of C₂ and d₂ in h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)).
- (2) Apply the in-test method extension. Since C₂ and d₂ originate solely from n₂, there exists a normal node m, m' ∈ C make term(m') = h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)), and m ⇒⁺ m' is the transition edge of C₂ and d₂ in h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)).
- (3) Define node m'. From the result of step (2), m' is a positive node. Assume that m' is a node in the strand S' of some responder in the protocol, S' = Init[M', N', C1', C2', d'1, d'2, DH(d'1, d'2)], n' = ⟨S', 4⟩, and term(⟨S', 4⟩) = h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)).
- (4) Compare the contents of the strands. By comparing term(⟨S', 4⟩) with the components in the initiator strand, we can determine N = N', C₁ = C₁', C₂ = C₂', DH(d₁, d₂) = DH(d'1, d'2)'. From DH(d₁, d₂) = DH(d'1, d'2)', then we can deduce d₁ = d'1 and d₂ = d'2.

From this, it can be seen that M' does not necessarily equal M, indicating that M cannot reach a consensus with N on M. The improvement method is to include M in the message component of the fourth step, h_K(T_i, K_n, C₁, C₂, DH(d₁, d₂)), resulting in an enhanced strand space model under asymmetric cryptographic systems, as shown in Figure 5.

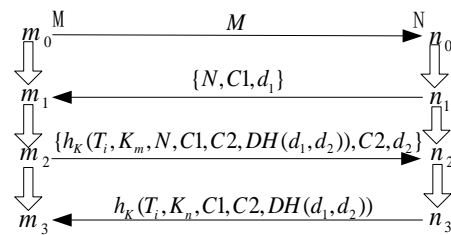


Figure 5. Advanced FCAP strand space model under asymmetric cryptosystems.

It is not difficult to see that in asymmetric cryptographic systems, authentication is mainly provided by the signature of the private key. However, if there is no subject identity identification in the signature, it can be easily forwarded or replayed. In other words, the absence of proper verification of the counterparty’s subject identity during authentication paves the way for an MITM attack. Attack instances can be derived as illustrated in Table 3, considering the scenario of authenticating N to M, where M, N, and P share the same password configuration. Here, P represents the attacker, while P(M) and P(N) act as impersonators of M and N, respectively.

Table 3. Attack instance of N authentication M.

Event	Sequence of Event
1	$M \rightarrow P : M$
1'	$P(M) \rightarrow N : M$
2'	$N \rightarrow P(M) : N, C1, d_1$
2	$P \rightarrow M : N, C1, d_1$
3	$M \rightarrow P : h_{K_{M^{-1}}}(T_i, K_m, C1, DH(d_1, d_2)), C2, d_2$
3'	$P(M) \rightarrow N : h_{K_{M^{-1}}}(T_i, K_m, C1, DH(d_1, d_2)), C2, d_2$
4'	$N \rightarrow P(M) : h_{K_{M^{-1}}}(T_i, K_n, C2, DH(d_1, d_2))$
4	$P \rightarrow M : h_{K_{M^{-1}}}(T_i, K_n, C2, DH(d_1, d_2))$

6. Experiments and Test Validation

In the process of testing identity authentication, the results can be categorized as successful authentication and failed authentication. Successful authentication can be further classified into one-way authentication and mutual authentication, depending on the password configuration at each end. Failed authentication can occur due to unsuccessful parameter negotiation or incorrect password configuration. Here, this paper focuses on discussing the case of incorrect password configuration.

6.1. Experiment Environments

The choice of the testing environment being based on Comware V7 devices and HP Network Simulator for identity authentication and security testing is primarily due to its popularity and practicality. Comware V7 has become an industry standard due to its wide application across various network devices, including routers, switches, FC switches, and network security devices. Meanwhile, the HP Network Simulator serves as a powerful network simulation tool that can efficiently simulate complex network environments at a low cost, making it highly suitable for learning and testing purposes. The practicality of this environment is reflected in its ability to support the testing of different network topologies, including connections between centralized and distributed switches. Comware V7 devices use the Comware network operating system, which includes various traditional routers, switches, FC switches, wireless network devices, and network security devices. In this test, Comware V7 devices primarily refer to FC switches. The HP Network Simulator is an X86-based network simulator that can simulate the networking environment of Comware V7 devices. The Comware virtual machines in the HP Network Simulator run on the VirtualBox emulator. Due to the limitations of VirtualBox, the performance of

Comware virtual machines is lower than that of actual devices. However, for the protocol improvement testing, the performance of Comware virtual machines is sufficient.

6.2. Experiment Settings

For security enhancement testing, this paper modifies the content of the messages manually and sends them with delayed timers for verification. For performance testing, we analyzed the time attributes during the authentication process. Switches can be classified into two types: centralized and distributed. During testing, different networking scenarios need to be tested, including centralized-to-centralized, centralized-to-distributed, and distributed-to-distributed connections. Their corresponding virtual machine networking configurations are shown in Figures 6–8.



Figure 6. The virtual network diagram on a PC (centralized to centralized).

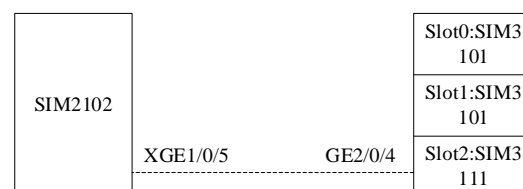


Figure 7. The virtual network diagram on a PC (centralized to distributed).

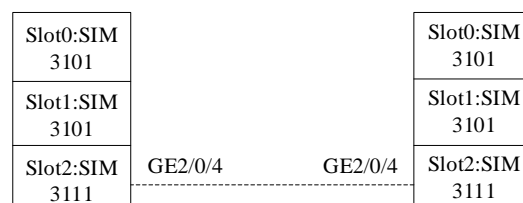


Figure 8. The virtual network diagram on a PC (distributed to distributed).

In the implementation, an enumeration type is defined as the return type for authentication results. The specific definition is in Table 4. For the three different networking scenarios, the experiment should be performed separately for the FC port and VFC port. First, we tested the case where the connection is centralized. During testing, double-sided authentication is used because two-way authentication can be considered a special case of double-sided authentication, eliminating the need for redundant work. The test cases and corresponding results are provided below. We assume WWN_m : 20:00:00:00:00:00:01 and WWN_n : 20:00:00:00:00:00:02.

Table 4. The type definition of authentication results.

<i>FCSP_Auth_Result</i>	<i>FCSP_AUTH_RESULT_E</i>
FCSP_AUTH_SUCCESS =0	//0: Authentication successful
FCSP_AUTH_FAILED	//1: Authentication failed
FCSP_AUTH_WAIT	//2: Waiting for authentication result
FCSP_AUTH_CONTINUE	//3: Authentication successful
FCSP_AUTH_MAX	//4: Invalid value

6.3. Security Testing

For three different networking scenarios, we tested the FC port and VFC port, respectively. During testing, it is all two-factor two-way authentication, because two-factor two-way authentication can be regarded as a special two-way authentication, and there is no need to perform repeated work. In the certification test of FC ports and VFC ports, we conducted three different cases: successful certification, Type 1 certification failure, and Type 2 certification failure. For successful authentication, this work configured the passwords on devices M and N to match correctly. The test methods for centralized-to-distributed and distributed-to-distributed scenarios are the same as those for centralized-to-centralized scenarios, and the test results obtained are also in line with expectations. All test scenarios were successfully verified. For security testing, we used the above networking diagram to simulate replay attacks and malicious modifications by manually modifying the sending of messages (starting the delay timer) and modifying the message content. After testing, the improved protocol has a certain resistance to replay attacks and malicious modifications, and its security has been improved.

6.4. Performance Testing

To test the performance, we executed the original protocol's *simware* version and the enhanced protocol's *simware* version separately using the HP Network Simulator. The network configurations for all three scenarios remained consistent with those described in the preceding section. We captured packet information using the packet capturing tool *Wireshark*. In the notation, *cen* and *dis* denote centralized and distributed devices, respectively. t_1 and t_2 denote the starting and ending times of authentication in the original protocol, while t'_1 and t'_2 represent the starting and ending times of authentication in the improved protocol. The specific values of the timing attributes (ignoring the leading common bits, measured in seconds) that we obtained are shown in Table 5.

Table 5. Starting and Ending Times of Three Types of Network Authentication.

Time	cen ↔ cen	cen ↔ dis	dis ↔ dis
t_1	0.839359	0.964431	0.911869
t_2	0.859327	0.985216	0.947953
t'_1	0.790771	0.918244	0.917031
t'_2	0.828139	0.957399	0.984638

The required time and the percentage improvement in efficiency of the original protocol with one-way mutual authentication and the improved protocol with two-way mutual authentication can be calculated from Table 2 for three network scenarios. The percentage improvement in efficiency here refers to the percentage increase in efficiency of the improved protocol running once (with two-way mutual authentication) compared with the efficiency improvement of the original protocol with two authentications. This information is shown in Table 6.

Table 6. Reduced Authentication Time and Improved Efficiency in Original Protocol and Enhanced Protocol.

Type	cen ↔ cen	cen ↔ dis	dis ↔ dis
FCAP	0.019968	0.020785	0.036084
Improve FCAP	0.037368	0.039155	0.067607
Efficiency improvement	6.43%	5.81%	6.32%

According to Table 6, the improved protocol shows increased efficiency compared with the original protocol in three different networking scenarios. When connecting centralized

devices to centralized devices, the efficiency improves by 6.43%. When connecting centralized devices to distributed devices, the efficiency improves by 5.81%. When connecting distributed devices to distributed devices, the efficiency improves by 6.32%. It is possible that there may be some errors between the measured values and the actual values in these three scenarios, as the timing of packet capture by the sniffing tool may have a slight deviation from the actual packet transmission and reception timing. However, these errors are not expected to be significant. Overall, the improved protocol has achieved certain performance improvements compared with the original protocol. In conclusion, we believe that the improved protocol not only achieves identity authentication functionality but also enhances security and performance.

7. Conclusions

Due to the original strand space model only considering simple operations and not taking into account cumbersome operations such as DH calculations, this paper first introduces a new data type, DH calculation, and extends the strand space model. Then, addressing the issue of the original authentication testing method not supporting the analysis of two data items, the authentication testing method is expanded. Subsequently, the extended authentication testing method is used to analyze the FCAP security based on symmetric and asymmetric cryptographic systems. To address the problem of consensus failure in random values under cryptographic systems, the initial FCAP strand space model is improved, resulting in a secure strand space model for symmetric cryptographic systems. The same method is then applied to analyze FCAP under asymmetric cryptographic systems. The test results are consistent with expectations, demonstrating the feasibility and effectiveness of the proposed approach. Our improved protocol shows increased efficiency compared with the original protocol across three different network configurations. There was a 6.43% increase in efficiency when centralized devices were connected to centralized devices, a 5.81% increase in efficiency when centralized devices were connected to distributed devices, and a 6.32% increase in efficiency when distributed devices were connected to distributed devices. In order to address the problem of consensus failure in subject identification under asymmetric cryptographic systems, the strand space model was further improved based on the improved strand space model for symmetric cryptographic systems, achieving authentication requirements under asymmetric cryptographic systems. In future work, we will investigate other protocols and how the improved protocol can defend against potential security threats, thereby demonstrating the effectiveness of the refinement measures.

Author Contributions: Conceptualization, H.G. and A.B.; methodology, J.S.; validation, A.B.; formal analysis, J.M. and H.G.; writing—original draft preparation, J.S.; writing—review and editing, P.W.; A.B. and J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Special Fund for Transformation of Scientific and Technological Achievements of Jiangsu Province (No. BA2022011) and the Special Fund for Transformation and Upgrading of Industrial and Information Industry of Jiangsu Province (Tackling and Industrialization of Threat Detection and response System for Industrial Internet Terminals).

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author/s.

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

References

1. Gou, J.; Chen, Y.; Yu, B.; Liu, J.; Du, L.; Wan, S.; Yi, Z. Reciprocal Teacher-Student Learning via forward and Feedback Knowledge Distillation. *IEEE Trans. Multimed.* **2024**, *26*, 7901–7916.
2. Chen, C.; Si, J.; Li, H.; Han, W.; Kumar, N.; Berretti, S.; Wan, S. A High Stability Clustering Scheme for the Internet of Vehicles. *IEEE Trans. Netw. Serv. Manag.* **2024**, *early access*.
3. Zagrouba, R.; AlAbdullatif, A.; AlAjaji, K.; Al-Serhani, N.; Alhaidari, F.; Almuhaideb, A.; Rahman, A. Authenblue: A new authentication protocol for the industrial Internet of Things. *Comput. Mater. Contin.* **2021**, *67*, 1103–1119.

4. Bhattacharjya, A. A Holistic Study on the Use of Blockchain Technology in CPS and IoT Architectures Maintaining the CIA Triad in Data Communication. *Int. J. Appl. Math. Comput. Sci.* **2022**, *32*, 403–413. <https://doi.org/10.34768/amcs-2022-0029>.
5. Bhattacharjya, A.; Wisniewski, R.; Nidumolu, V. Holistic Research on Blockchain's Consensus Protocol Mechanisms with Security and Concurrency Analysis Aspects of CPS. *Electronics* **2022**, *11*, 2760. <https://doi.org/10.3390/electronics11172760>.
6. Bhattacharjya, A.; Kozdrój, K.; Bazydło, G.; Wisniewski, R. Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things. *Electronics* **2022**, *11*, 2560. <https://doi.org/10.3390/electronics11162560>.
7. Bachani, V.; Bhattacharjya, A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* **2023**, *15*, 4. <https://doi.org/10.3390/sym15010004>.
8. Bazydło, G.; Kozdrój, K.; Wiśniewski, R.; Bhattacharjya, A. Trusted Third Party Application in Durable Medium e-Service. *Appl. Sci.* **2024**, *14*, 191. <https://doi.org/10.3390/app14010191>.
9. Bary, T.A.A.A.A.; Elomda, B.M.; Hassan, H.A. Multiple Layer Public Blockchain Approach for Internet of Things (IoT) Systems. *IEEE Access* **2024**, *12*, 56431–56438.
10. Li, C.; Jiang, K.; Zhang, Y.; Jiang, L.; Luo, Y.; Wan, S. Deep Reinforcement Learning-Based Mining Task Offloading Scheme for Intelligent Connected Vehicles in UAV-Aided MEC. *ACM Trans. Des. Autom. Electron. Syst.* **2024**, *29*, 54.
11. Zhang, K.; Shi, Y.; Karnouskos, S.; Sauter, T.; Fang, H.; Colombo, A.W. Advancements in industrial cyber-physical systems: An overview and perspectives. *IEEE Trans. Ind. Inform.* **2022**, *19*, 716–729.
12. Tong, W. Performance comparison of FCoE and iSCSI. In Proceedings of the Photonics and Optoelectronics Meetings (POEM) 2009: Optical Storage and New Storage Technologies, Wuhan, China, 8–10 August 2009; SPIE: Bellingham, WA, USA, 2009; Volume 7517, pp. 264–270.
13. Li, Q.; Long, H.; Xu, Z.; Hou, J.; Cai, J. A threat recognition solution of edge data security in industrial internet. *World Wide Web* **2022**, *25*, 2109–2138.
14. Li, Q.; Wang, X.; Wang, P.; Zhang, W.; Yin, J. FARDA: A fog-based anonymous reward data aggregation security scheme in smart buildings. *Build. Environ.* **2022**, *225*, 109578.
15. Wei, J.; Zhu, Q.; Li, Q.; Nie, L.; Shen, Z.; Choo, K.K.R.; Yu, K. A redactable blockchain framework for secure federated learning in industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 17901–17911.
16. He, Z.; Zhou, J. Inference attacks on genomic data based on probabilistic graphical models. *Big Data Min. Anal.* **2020**, *3*, 225–233.
17. Fábrega, F.J.T.; Herzog, J.C.; Guttman, J.D. Strand spaces: Why is a security protocol correct? In Proceedings of the 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186), Oakland, CA, USA, 6 May 1998; IEEE: New York, NY, USA, 1998; pp. 160–171.
18. Li, D.; Li, Q.; Ye, Y.; Xu, S. Arms race in adversarial malware detection: A survey. *ACM Comput. Surv. (CSUR)* **2021**, *55*, 15.
19. Zhou, X.; Hu, Y.; Wu, J.; Liang, W.; Ma, J.; Jin, Q. Distribution bias aware collaborative generative adversarial network for imbalanced deep learning in industrial IoT. *IEEE Trans. Ind. Inform.* **2022**, *19*, 570–580.
20. Li, Q.; Meng, S.; Sang, X.; Zhang, H.; Wang, S.; Bashir, A.K.; Yu, K.; Tariq, U. Dynamic scheduling algorithm in cyber mimic defense architecture of volunteer computing. *ACM Trans. Internet Technol.* **2021**, *21*, 1–33.
21. Wei, G.; Liqun, C.; Chunming, R.; Kaitai, L.; Xianghan, Z.; Jiangshan, Y. Security Analysis and Improvement of a Redactable Consortium Blockchain for Industrial Internet-of-Things. *Comput. J.* **2021**, *65*, 2430–2438.
22. Usman, M.; Sarfraz, M.S.; Aftab, M.U.; Habib, U.; Javed, S. A Blockchain based Scalable Domain Access Control Framework for Industrial Internet of Things. *IEEE Access* **2024**, *12*, 56554–56570.
23. Roh, S.S.; Kim, S.H.; Kim, G.H. Design of authentication and key exchange protocol in Ethernet passive optical networks. In Proceedings of the International Conference on Computational Science and Its Applications, Assisi, Italy, 14–17 May 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1035–1043.
24. Chowdhury, S.; Maier, M. Security issues in integrated EPON and next-generation WLAN networks. In Proceedings of the 2010 7th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 9–12 January 2010; IEEE: New York, NY, USA, 2010; pp. 1–2.
25. Yin, A.; Chen, D.; Ding, Y. An efficient and secure authentication scheme based on NTRU for 10G ethernet passive optical. *Optik* **2014**, *125*, 7207–7210.
26. Petridou, S.; Basagiannis, S.; Mamas, L. Formal methods for energy-efficient EPONs. *IEEE Trans. Green Commun. Netw.* **2017**, *2*, 246–259.
27. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst. (TOCS)* **1990**, *8*, 18–36.
28. Fariss, M.; El Gafif, H.; Toumanari, A. Formal security analysis of an IoT mutual authentication protocol. In Proceedings of the ITM Web of Conferences, Bali, Indonesia, 29–30 August 2023; EDP Sciences: Les Ulis, France, 2023; Volume 52, p. 01003.
29. Zhang, H.; Lai, Y.; Chen, Y. Authentication methods for internet of vehicles based on trusted connection architecture. *Simul. Model. Pract. Theory* **2023**, *122*, 102681.
30. Saarinen, M.J.O. The BRUTUS automatic cryptanalytic framework: Testing CAESAR authenticated encryption candidates for weaknesses. *J. Cryptogr. Eng.* **2016**, *6*, 75–82.
31. James, A.; Tiu, A.; Yatapanage, N. PFMC: A parallel symbolic model checker for security protocol verification. In Proceedings of the International Conference on Formal Engineering Methods, Madrid, Spain, 24–27 October 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 173–189.

32. Cheikhrouhou, L. Inductive Verification of Cryptographic Protocols Based on Message Algebras. Ph.D. Thesis, Universität des Saarlandes Saarbrücken, Saarbrücken, Germany, 2022.
33. Yao, M.m.; Zhang, J.; Weng, X. Research of formal analysis based on extended strand space theories. In *Proceedings of the International Conference on Intelligent Computing*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 651–661.
34. Moran, M.; Lafourcade, P.; Puys, M.; Williams, D. An Introduction to Tools for Formal Analysis of Cryptographic Protocols. In *Handbook of Formal Analysis and Verification in Cryptography*; CRC Press: Boca Raton, FL, USA, 2023; pp. 105–152.
35. Focardi, R.; Luccio, F.L. Secure Key Management Policies in Strand Spaces. In *Protocols, Strands, and Logic: Essays Dedicated to Joshua Guttman on the Occasion of his 66.66 th Birthday*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 175–197.
36. Dong, X.; Yang, C.; Sheng, L.; Wang, C.; Ma, J. A new method to deduce counterexamples in secure routing protocols based on strand space model. *Secur. Commun. Netw.* **2016**, *9*, 5834–5848.
37. Xiao, Y.; Gao, S. Formal verification and analysis of 5G AKA protocol using mixed strand space model. *Electronics* **2022**, *11*, 1333.
38. Salem, O.; Mehaoua, A. Ephemeral Elliptic Curve Diffie-Hellman to Secure Data Exchange in Internet of Medical Things. In *Emerging Trends in Cybersecurity Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 3–20.
39. Li, D.; Li, Q.; Ye, Y.; Xu, S. A framework for enhancing deep neural networks against adversarial malware. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 736–750.
40. Li, Q.; Hou, J.; Meng, S.; Long, H. GLIDE: A game theory and data-driven mimicking linkage intrusion detection for edge computing networks. *Complexity* **2020**, *2020*, 1–18.
41. Li, Q.; Liu, Y.; Meng, S.; Zhang, H.; Shen, H.; Long, H. A dynamic taint tracking optimized fuzz testing method based on multi-modal sensor data fusion. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 110.
42. Li, Q.; Yin, X.; Meng, S.; Liu, Y.; Ying, Z. A security event description of intelligent applications in edge-cloud environment. *J. Cloud Comput.* **2020**, *9*, 23.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.