International Journal on Semantic Web and Information Systems
Volume 19 • Issue 1

A Lightweight Cross-Domain Authentication Protocol for Trusted Access to Industrial Internet

Tiantian Zhang, Information Engineering College, Henan University of Science and Technology, Luoyang, China, & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, Luoyang, China, & Henan Intelligent Manufacturing Big Data Development Innovation Laboratory, Henan University of Science and Technology, Henan Luoyang, China

Zhiyong Zhang, Information Engineering College, Henan University of Science and Technology, Luoyang, China, & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, Luoyang, China, & Henan Intelligent Manufacturing Big Data Development Innovation Laboratory, Henan University of Science and Technology, Henan Luoyang, China


https://orcid.org/0000-0003-3061-7768

Kejing Zhao, Information Engineering College, Henan University of Science and Technology, Luoyang, China, & Henan International Joint Laboratory of Cyberspace Security Applications, Henan University of Science and Technology, Luoyang, China, & Henan Intelligent Manufacturing Big Data Development Innovation Laboratory, Henan University of Science and Technology, Henan Luoyang, China

Brij B. Gupta, Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan, & Symbiosis Centre for Information Technology (SCIT), Symbiosis International University, Pune, India, & Lebanese American University, Beirut, Lebanon, & School of Computing, Skyline University College, Sharjah, UAE*

Varsha Arya, Varsha Arya, Department of Business Administration, Asia University, Taiwan, & Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, India, & Chandigarh University, Chandigarh, India

ABSTRACT

This paper proposes a hierarchical framework for industrial Internet device authentication and trusted access as well as a mechanism for industrial security state perception, and designs a cross-domain authentication scheme for devices on this basis. The scheme obtains hardware device platform configuration register (PCR) values and platform integrity measure through periodic perception, completes device identity identification and integrity measure verification when device accessing and data transmission requesting, ensures secure and trustworthy access and interoperation of devices, and designs a cross-domain authentication model for trustworthy access of devices and related security protocols. Through the security analysis, this scheme has good anti-attack abilities, and it can effectively protect against common replay attacks, impersonation attacks, and man-in-the-middle attacks.

KEYWORDS

Cross-Domain, Identity Authentication, Industrial Internet Security, Integrity Measurement, Trusted Access

1. INTRODUCTION

The rapid development of Industrial Internet and Industrial Internet of Things (IIoT) has promoted and accelerated the digitalization and intelligent transformation and upgrading of manufacturing industry

DOI: 10.4018/IJSWIS.333481 *Corresponding Author

(Rakas et al., 2021). With the extremely rapid expansion of industrial equipment and industrial scale, cross-regional, cross-platform, cross-infrastructure security access and communication interaction of industrial equipment will be more frequent, and the industrial Internet, as the key information infrastructure for intelligent manufacturing, is facing the dual challenges of internal risks and external threats while improving the productivity of advanced manufacturing and providing the facilitation of the whole elements of the industrial chain value chain and the whole lifecycle of network communication (Serror et al., 2020;Wollschlaeger et al., 2017). Devices and services in different domains of the Industrial Internet need to be able to trust each other and communicate and interact within a secure channel. Cross-domain authentication is a necessary condition and a key approach to ensure interoperability and mutual trust, which aims to verify each other's identities for devices and systems from different domains and to ensure the secure transmission of data and information, thus realizing device interoperability, device security and industrial network security. Industrial equipment in the local network domain and cross-domain access to identity authentication and security verification, has become the primary equipment for safe and reliable access to the "barrier", without the authentication of authorized industrial equipment, will be controlled by malicious attackers and pretend to be a legitimate device to access the industrial network, access to sensitive industrial control systems and equipment data, manipulate and interfere with normal production processes and procedures, breaking the normal industrial ecosystem.

Currently, most of the industrial equipment identity authentication solutions establish a distributed trust mechanism across network domains through blockchain technology, weakening the dependence on trusted third party(TTP) platforms and the complexity of management, while effectively avoiding the security risks brought by centralized storage, Ensures the security, trust and traceability of users and devices in industrial Internet scenarios, and provides a distributed storage, computing and security infrastructure platform for realizing secure and trustworthy device authentication. However, the existing industrial Internet and IIoT identity authentication scheme based on blockchain technology does not fully consider the real-time nature of industrial equipment security brought about by complex and changeable industrial application scenarios, and lacks the ability to perceive the security elements of industrial equipment and computing platforms, while ignoring the integrity measure and verification of equipment during the device authentication of the two sides of the communication to ensure secure and trustworthy access to the equipment. Trusted computing, as a high-security enhancement mechanism, realizes the identity authentication and integrity measure of the device platforms of the two communicating parties through the trusted platform module (TPM), ensures the identity security of the devices and the integrity of the platforms by using the platform configuration registers (PCR) and the remote attestation (RA) technology, effectively prevents unauthorized devices from accessing the network, and improves the overall security of the communication system's message interactions and interoperability. To this end, this paper proposes a layered framework for industrial Internet device authentication and trusted access as well as an industrial state security perception mechanism, and designs a cross-domain authentication scheme for devices on this basis. The main contributions of this paper are as follows:

(1) An authentication layered framework for trusted access of industrial Internet devices and a mechanism for perception of the security status of industrial devices are constructed. Based on the decentralized blockchain system architecture, a layered authentication framework for devices is established; based on the trusted computing technology to complete the cross-domain identity authentication and integrity verification for industrial equipment access, using periodic perception to obtain the PCR values and measure logs of industrial devices, dynamic real-time perception and updating of device identities and statuses are realized.
(2) A cross-domain authentication model and security protocol for trusted access of equipment is designed. Based on the security perception mechanism of industrial equipment, it designs local and cross-domain identity identification and integrity verification for equipment access, realizes

"one-time access, simultaneous verification", effectively improves the efficiency of equipment authentication. It also solves the overhead problem caused by the centralized architecture, effectively avoids the security problems caused by equipment integrity damage or identity impersonation invasion, and ensures the local and cross-domain attack resistance and security in industrial application scenarios.

The rest of this paper is organized as follows. Section 2 describes related research work at home and abroad. Section 3 details the cross-domain authentication layered architecture and scheme design for trusted access of industrial Internet devices. Section 4 gives the security protocol design for the authentication scheme. Section 5 analyzes the security, computational performance and overhead of the scheme in this paper. Finally, conclusion is briefly presented.

2. RELATED WORK

Industrial devices trusted access to industrial Internet has several important steps and processes such as identity authentication, data storage, and security detection, while involving different application scenarios in local and cross-domain. Traditional authentication schemes are overly dependent on trusted third parties, while message data storage and interoperability schemes based on the decentralized characteristics of blockchain are conducive to the implementation of cross-domain authentication and effectively avoid security threats such as data privacy leakage and achieve identity traceability.

2.1 Authentication Solutions for the Traditional Internet

For traditional Internet-oriented (cross-domain) security authentication schemes, key negotiation and cross-domain authentication between heterogeneous domains proposed in Yuan et al. (2017) realize cross-domain access, but carry a large computational load. In order to better realize the security goals of message integrity, message authentication, and entity authentication, Kumar & Venkaiah (2022c) proposed a new hash function (QGMD5-384) and an efficient message authentication code (QGMAC-384, Hu B. et al. 2022) based on a quasigroup. Fatima & Ahmad (2021) to ensure the 'security' of data in cloud computing, quantum key cryptography is introduced, proposed method made use of quantum key distribution with Kerberos to secure the data on the cloud. Existing distributed authentication schemes establish a federation through blockchain to attenuate the related management work of third-party platforms. Zhang et al. (2020) proposes for the first time a complete cross-domain authentication scheme executed on chain code, which reduces the computational burden of the authentication server and ensures the reliability of the results. Kubilay et al. (2019) proposes CertLedger, a blockchain-based architecture with certificate transparency and eliminates the traditional insufficient and incompatible certificate validation processes implemented by different software vendors. Chen et al. (2021) proposes a cross-domain authentication solution XAuth that separates the storage and control layers and designs an efficient cross-domain data management mechanism and cross-domain anonymous authentication protocol. Wang et al. (2022) proposed a multi-Certificate Authority (CA)-based authentication architecture to establish distributed trust among multiple domains and share cross-domain certificate information. Liu et al. (2021) designed an efficient cross-domain anonymous authentication scheme based on blockchain and proposed an authentication protocol that combines PKI environment and blockchain. In summary, traditional Internet authentication schemes are deficient in security, scalability, and performance, and lack authentication of devices.

2.2 Authentication Solutions for the Internet of Things

In recent years, domestic and foreign researchers have conducted research on security authentication models, mechanisms and security protocols for IoT application scenarios (Cvitić et al. 2021, Al-Qerem et al. 2020, Gupta et al. 2020, Liao et al. 2019a; Li. S et al. 2022). Xiao et al. (2020) proposes

cross-domain nearest-neighbor authentication method for IoT scenarios, based on IOTA blockchain and with the help of mobile edge computing capability, to realize lightweight authentication process for IoT devices. In addition to this, Jia et al. (2020a), Jia et al. (2020b), Khalid et al. (2020), Ma et al. (2021), Tong et al. (2022) and Zhang et al. (2022) also implements local or cross-domain distributed authentication schemes based on blockchain for IoT environments, and Gope & Sikdar (2018) proposes a two-factor authentication protocol for privacy protection of IoT devices, which utilizes the intrinsic properties of Physical Unclonable Functions (PUFs) to effectively improve security. Kumar et al. (2022a) reviews authentication in IoT and its related areas, analyzes the potential of existing technical approaches, and discusses the fundamentals of authentication and its related attacks. Tiwari et al. (2022) proposed an adaptive Ontology-Based IoT Resource Provisioning in Computing Systems. Raj et al. (2022) proposed a Chaotic whale crow optimization algorithm for secure routing in the IoT environment. Almomani et al. (2022) proposed a phishing website detection with semantic features based on machine learning. Tembhurne et al. (2022) proposed a fake news detection using multi-channel deep neural networks. Vinoth et al. (2022) proposed a new cloud-based session key agreement and data storage scheme which consists of an improved authentication mechanism for MIoT, achieves anonymous pre-authentication and post-authentication. Chen et al. (2019b) proposed a clustering based physical-layer authentication scheme (CPAS) and it is a novel cross-layer secure authentication approach for edge computing system with asymmetric resources. A light-weight radio frequency fingerprinting identification (RFFID) scheme that combines with a two-layer model is proposed to realize authentications for a large number of resource-constrained terminals under the mobile edge computing (MEC) scenario (Chen et al. 2019a). A convolutional neural network (CNN) enhanced radio frequency fingerprinting (RFF) authentication scheme is presented for IoT (Xie et al. 2019). Zhai et al. (2022) presented a secure detection service and it is deployed on every node of WSN to monitor, manage and control the messages passing through them in real-time. In this regard, the existing IoT authentication schemes still have flaws and shortcomings in terms of privacy issues, resource constraints, communication security, and scalability, and device vulnerabilities need to be addressed with security measures.

2.3 Authentication Solutions for the Industrial Internet and IIoT

Researchers proposed many solutions for IoT and IIoT environments (Khanam et al. 2022, Kiran et al. 2022, Kumar et al. 2022b, Sadatacharapandi et al. 2022; Gaurav et al. 2022; Madhu S. et al. 2022). For (cross-domain) authentication and trust schemes for Industrial Internet and IIoT. Bao et al. (2022) proposes a privacy-preserving identity management system for IIoT based on blockchain utilizing multiple cryptographic techniques, but it may impose a large burden on the system. Shen et al. (2020) introduces federated blockchain to build trust between different domains, and proposes an efficient and secure blockchain-assisted device anonymous authentication mechanism BASA for cross-domain IIoT. Wang et al. (2022) designs a cross-domain authentication scheme CL-BASA based on BASA for cross-domain of IIoT, and a secure and efficient anonymous and certificate-less public-key signing scheme CL-PKS that effectively avoid the security threats that BASA may bring. Zhang et al. (2022) designed a hardware-assisted multi-factor key derivation method via PUF and proposed a new cross-domain trust construction method. Zhong et al. (2023) proposed a distributed cross-domain message authentication model that generates pseudonyms and keys for devices, and the edge gateway realizes distributed authentication and token distribution to the devices through secret sharing technique to achieve bulk authentication. Cui et al. (2022) proposes a lightweight anonymous cross-domain authentication scheme that introduces edge devices to alleviate the computational pressure on authentication servers and IIoT devices, and combines blockchain and dynamic accumulator techniques to achieve fast authentication. Jeong (2022) proposes an IIoT augmentation model to sense information in real time and ensure the integrity of the generated IIoT information. Li et al. (2022) designs a blockchain-based PUF device authentication framework and proposes two distributed device authentication schemes with PUF. A deep learning (DL)-based physical (PHY)

layer authentication framework is proposed to enhance the security of industrial wireless sensor networks (IWSNs) (Liao et al. 2019b). Liu et al. (2023) proposes a blockchain-enforced authentication framework for cross-trust domain communication in IIoT systems and a blockchain-enforced cross-domain private protection authentication and key agreement scheme BP-AKAA, which can effectively protect the authentication privacy of IIoT devices. In summary, the identity authentication scheme for industrial Internet and IIoT has the shortcomings of management and implementation complexity, poor compatibility, network delay, etc., and there are also deficiencies in the identity identification and integrity state verification of industrial devices, which cannot satisfy the security authentication problem of the current industrial Internet intelligentized devices.

3. TRUSTED ACCESS AUTHENTICATION SCHEME FOR INDUSTRIAL INTERNET DEVICES

This paper proposes a layered framework for industrial Internet device authentication and trusted access as well as an industrial security state perception mechanism, and designs a cross-domain authentication scheme for devices on this basis, which effectively solves the problem of missing device authentication and improves system security and reliability.

3.1 A Layered Framework for Industrial Internet Device Authentication and Trusted Access

This proposal firstly illustrates a layered framework for industrial Internet device authentication and trusted access, as shown in Figure 1. There exist massive, heterogeneous, and multi-type industrial equipment entities in the smart manufacturing digital factory scenario, including intelligent devices, servers, cloud platforms, and so on. The layered framework involves the data layer, business layer, execution layer and perception layer, corresponding to the field general-presentation layer, control layer, network layer and application layer in the Industrial Internet.

Data Layer: the data layer contains mainly industrial data blockchain and service resources of related domains.

The proposal uses blockchain as the underlying basic platform for the storage of cross-domain information of both domains, which can be regarded as a secure channel for information sharing between specific domains, and is indispensable for the authentication of the identity of users and equipment in each domain. The data resource services in this layer are the relevant industrial equipment, generated data information, production materials, and related services in each domain, respectively.

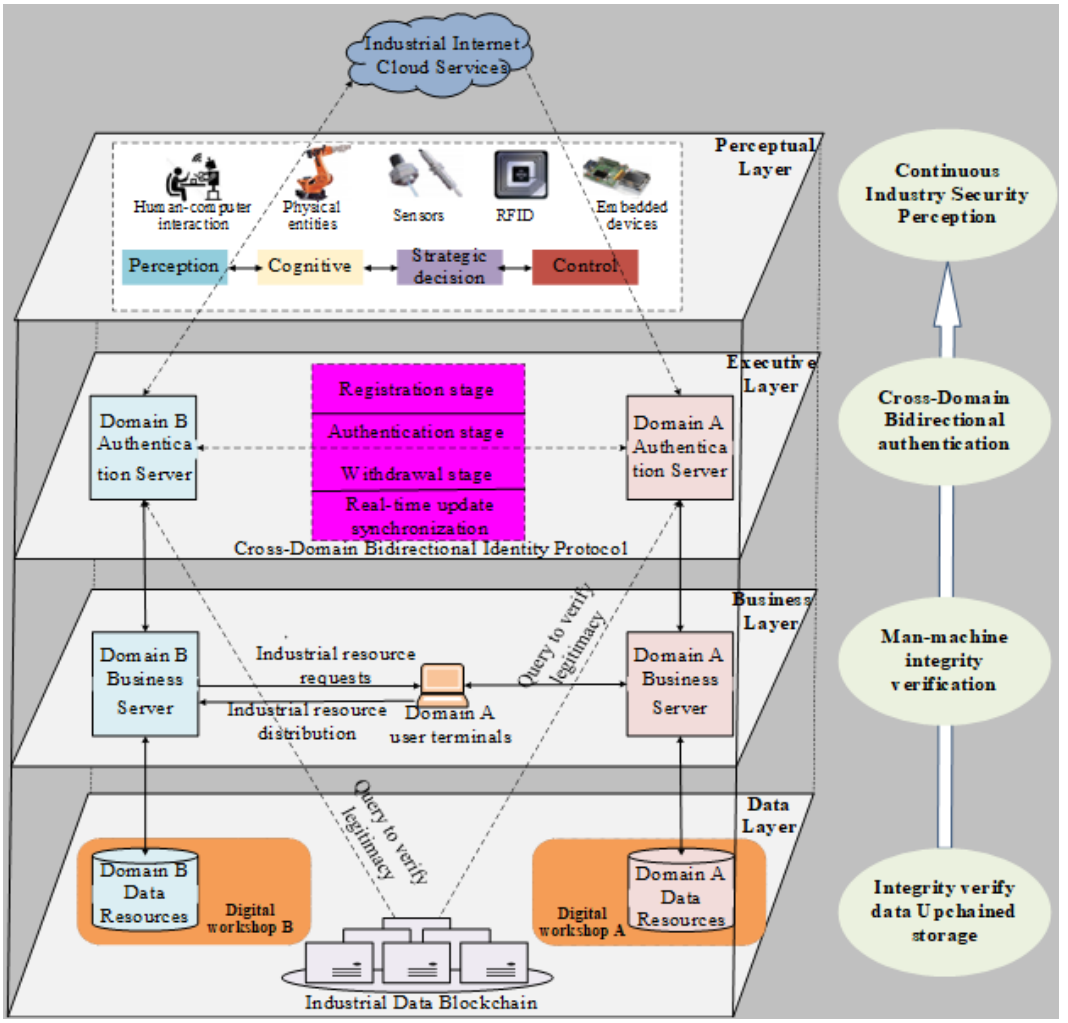
Business layer: The business layer mainly contains user terminals, business server entities, and workflows such as requesting resources and resource distribution.

In order to clarify the function of the authentication server and reduce the workload of the authentication server, a business server is independently deployed in each network domain for resource scheduling, and completes the authentication and carries out resource distribution by calling the authentication server. The user terminals in this layer are equipment entities that can use industrial resources and access industrial data, and can access the resources and services in the local and non-local regions by utilizing the legal identity and passing the request.

Execution layer: The execution layer mainly contains the authentication server and related authentication process protocols, of which the authentication protocols mainly include registration, local domain (cross-domain) authentication, industrial sensing and revocation, while ensuring real-time update of data.

In this application scenario, the authentication server is introduced to take charge of the main work of cross-domain authentication, complete the signature generation and identity verification operations, and cooperate with the business server to complete the cross-domain authentication request. The key step in the registration process is the generation of initial identity credentials, which is an important basis for authentication and will be dynamically updated in the industrial security perception phase

Figure 1. Industrial internet device authentication and trusted access layered framework



of each authentication to ensure that the identity credentials carried by each authentication are real and effective, and to avoid industrial network security problems caused by identity credential leakage. The authentication process can be divided into two key steps and segments, the two key steps in the same-domain authentication is the user device identity authentication and industrial equipment security perception; cross-domain authentication in the two key steps is the industrial equipment security perception and user device identity authentication.

Perception layer: The perception layer contains physical entities, industrial sensors, embedded devices, RFID and other hardware devices, the device itself can perceive the environment and its security status, and faithfully report real-time perception data information.

Based on industrial network intelligence scenarios, the authentication process, in addition to the stage of authentication identity, also introduces the stage of industrial security perception, i.e., periodic industrial security perception of hardware devices, making the corresponding analysis of the domain decision-making, dynamically updating the identity credentials, avoiding the waste of resources or even intentional access to the requesting domain user due to the request change or hardware device

insecurity and other reasons, so as to achieve the full-cycle identity security guarantee and data privacy protection.

The architecture of the layers work together to maintain the full-cycle security state of the industrial Internet equipment, at the same time, based on the scenario design of the layered framework diagram from the data layer to the perception layer of each layer of the first need for integrity verification data on-chain storage, on top of the underlying foundation also need to be in order to human-computer integrity verification, cross-domain bi-directional identity authentication, continuous industrial security perception, so as to achieve the full-cycle identity security guarantee and data privacy protection.

3.2 A Novel Cross-Domain Authentication Model for Devices

Aiming at the security defects and deficiencies existing in the current industrial Internet device authentication scheme, we propose a new cross-domain authentication model for trusted access of industrial Internet devices, which includes real-time perception of the security state of industrial devices and industrial device security authentication (identity authentication and integrity verification) to realize bidirectional device authentication between the two sides of the communication. The new device cross-domain authentication model is shown in Figure 2.

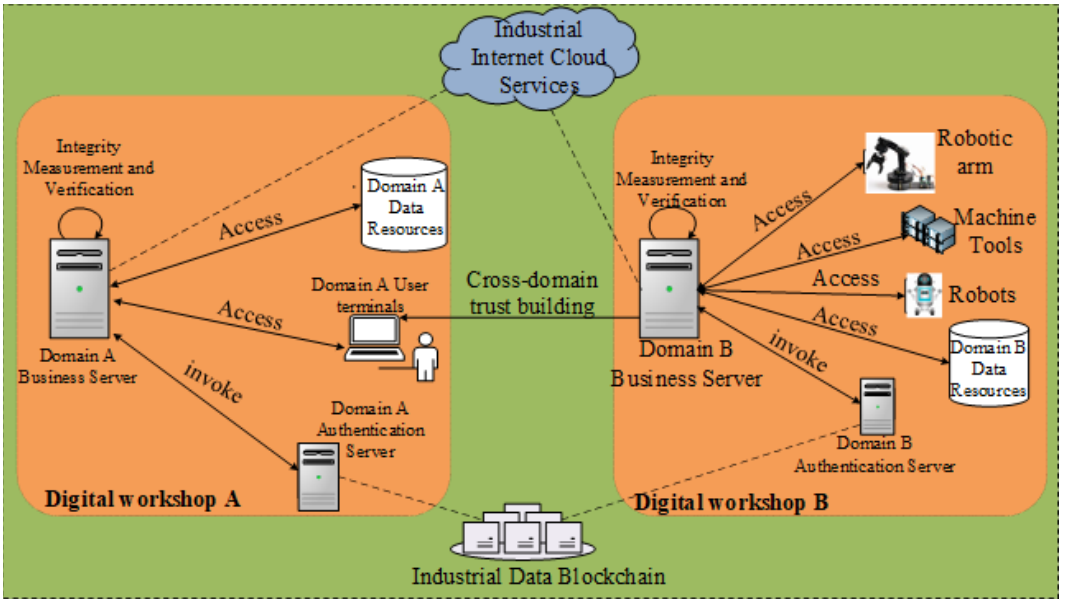
A digital factory consists of several independent digital workshops, different digital workshops may use different network connections and data structures, and the workshop entities are jointly involved in maintaining the security and normal operation of the digital factory, including user terminals, servers, and service resources (Ren P. et al. 2021, Cvitić I et al. 2021b). Each orange rectangular box in the model represents a digital workshop, i.e., a security domain, and the following specifically describes the cross-domain authentication process. When a user in domain A wants to access the resources in domain B, the detailed description is as follows: the user in domain A firstly initiates a resource request message to the business server in domain B, and the business server responds and calls the authentication server for identity authentication; at the same time, the users of the two domains and the servers and other equipment determine the identity of the users and the equipment of the communicating parties through bidirectional identity authentication, bidirectional integrity measurement and verification, and the relevant computation and analysis decision-making, and whether the user's identity and the equipment of the communicating parties have been damaged. Whether the equipment on both sides of the communication has been damaged to ensure the trusted access of the equipment. If the result shows that the identity of the equipment of the other party is not trustworthy or the integrity has been damaged, the data interaction process between the two parties will be terminated immediately to prevent the access of unauthorized equipment.

Assuming that the user requesting resources belongs to domain A, the user has to register with the local authentication server in advance, and the authentication server issues key pairs for it. When domain A users access local resources, they can directly request the local authentication server and access the resources after passing the verification; when domain A users access domain B resources, the domain B authentication server needs to authenticate the users and their devices to ensure the security of the identity and the integrity of the device, and at the same time, the relevant hardware devices in domain B need to carry out the identity legitimacy verification and the device integrity measure, to ensure that the two sides of the device are trustworthy and real. Among them, terminal devices, servers and other entities are configured with TPM chips, and the alliance blockchain is composed of authentication servers for each security domain that store user information and permissions.

In the cross-domain authentication phase, the model aims to establish trusted authentication and communication interactions between different domains, including the following key elements:

1. Two-way authentication: The cross-domain authentication model first requires devices or systems to authenticate between different domains. The authentication ensures that only legitimate devices or systems can participate in cross-domain communication and have access to specified resources or both parties can communicate within a certain period of time.

Figure 2. Cross-domain authentication model of devices for trusted access for industrial internet



2. Device Integrity Metrics and Verification: Use TPM to perform hardware integrity metrics, monitor whether the device has been tampered with or damaged, and verify the integrity of the other party's hardware.
3. Industrial security perception: Once the device passes the identity verification, it also needs to carry out periodic industrial security perception to ensure that each access is a safe and trustworthy device that has been successfully verified by both domains, to ensure the validity of the identity as well as the real-time nature of the message.
4. Encryption and secure communication: The cross-domain authentication model uses encrypted transmission and secure communication protocols to protect the confidentiality of messages and data integrity during cross-domain transmission of data or resources to ensure that the transmission of data between different domains is secure.

The cross-domain authentication model establishes an industrial network device trust relationship, secures industrial data, and realizes reliable communication between devices and systems in different domains. Based on this, devices on both sides can communicate and interact and access resources through trusted access.

3.3 Industrial Equipment Security State Perception Mechanism

In industrial Internet scenarios, the number of devices is increasing and the network communication is becoming more and more complex, so it is particularly important to ensure the security and integrity of the devices. In this paper, we propose a industrial device security state perception mechanism to perceive and judge the device integrity, security state and the environment in which it is located. The following is the industrial equipment security perception process:

- **Regular request:** In a regular time interval, the client actively sends a request to the server, so as to realize the real-time perception of equipment status. This enables timely perception of the operating status of the equipment, security indicators and the environment in which it is located,

so that potential problems can be detected at an early stage and timely responses can be made to reduce the impact of potential threats to the system stability of the equipment.

- **Integrity state perception:** Both the server and the client are equipped with TPM chips, using the TPM for hardware integrity measure, monitoring whether the device has been tampered or damaged, and verifying the hardware integrity of the other party. In the perception process, TPM plays a key role in the authentication of device identity and data integrity verification to prevent the invasion and tampering of malicious devices, as shown in Algorithm 1.
- **Data Transmission Perception**: Monitor the data transmission process for any anomalies, such as ata tampering, interception, and so on. By verifying the signature to ensure that it comes from a legitimate user and comparing the hash value of the data, we can determine whether the data is complete and legitimate.
- **Device health state perception**: Monitor the working state and operation condition of the device, and detect whether there is abnormal behavior in the device. Judge whether the device is in normal working condition through the device's operation data and status information.
- **Credential issuance**: If the verification is successful, the server issues temporary identity credentials to the client, allowing it to carry out specific operations; if the verification fails, set the device status as abnormal and take corresponding security measures.
- **Authentication and Authorization Judgment**: Based on the results of bidirectional authentication and identity credentials issuance, determine whether the device has access rights.

Through the above perception and judgment results, the industrial Internet system can realize comprehensive security monitoring and management of the equipment, and guarantee the overall security and stability of the system.

4. CROSS-DOMAIN AUTHENTICATION SECURITY PROTOCOL DESIGN

In order to ensure user and device identity security in the cross-domain process, we design an industrial security state perception mechanism and a cross-domain authentication security protocol. When a

Algorithm 1. Integrity measurement and verification algorithm

Input: $PCR_i, SML, Timestamp, S\#SK\left(PCR_i, Timestamp, SML\right)$

Output: $True\ or\ False$

$1: First,\ data = \ "id + \ timestamp \ + \ number"\ is\ calculated,\ then\ sha256\ is\ performed\ on\ the\ string.$

$SHA256\_DATA = 'echo\ "data"\ \left|\ openssl\ dgst\ -sha256\ -binary\ \right|\ xxd\ -p\ -c\ 32'$

$2: Assuming\ that\ the\ selected\ PCR15\ extend\ operation\ and\ validation.$

$The\ data\ obtained\ in\ the\ previous\ step\ is\ extended,\ and\ the\ extended\ result\ is\ placed\ in\ PCR15.$

$tpm2\_pcrextend\ 15: sha256 = \$SHA256\_DATA$

$The\ pcr\ value\ was\ re\text{-}read\ after\ extend\ tpm2\_pcrread\ sha256: 15.$

$Use\ the\ command\ to\ calculate\ the\ expected\ value\ PCR.$

$INITIAL\_SHA256\_DATA = "0000000000000000000000000000000000000000000000000000000000000000"$

$CONCATENATED = 'echo\ -ne\ \$INITIAL\_SHA256\_DATA;$

$echo\ \$SHA256\_DATA';echo\ \$CONCATENATED;echo\ \$CONCATENATED\ \left|\ xxd\ -r\ -p\ \right|\ openssl\ dgst\ -sha256.$

$3: Excute\ TPM2\text{-}toolbox.quote\ operation.$

$Get\ a\ set\ of\ values\ that\ contain\ quote.out, sig.out, pcr\ and\ digest.$

$This\ is\ the\ real\ measure\ obtained\ and\ compared\ with\ the\ calculated\ expected\ value\ to\ confirm\ the\ accuracy\ of\ the\ PCR.$

$4: Verify\ that\ the\ expected\ value\ is\ the\ same\ as\ the\ obtained\ true\ value$

$if\ obtain\ PCR\ equal\ expected\ PCR\ \&\&\ Timestamp\ is\ fresh$

$True$

$else\ False.$

user requests a cross-domain industrial device data resource, the relevant device carries out integrity measure based on the TPM, periodically and continuously perceives the industrial security state, updates the identity credentials, and ensures the security and timeliness of cross-domain message interaction. Table 1 briefly describes some of the important notations used in this protocol.

4.1 Registration Stage Protocol

Before joining the production line, the device must send a request to the authentication server of the local domain for registration. When registering for the first time, the application registration process is shown in Figure 3 (taking domain A as an example), and the participants mainly include domain A user terminals, authentication servers and business servers, and blockchain. The specific flow is as follows:

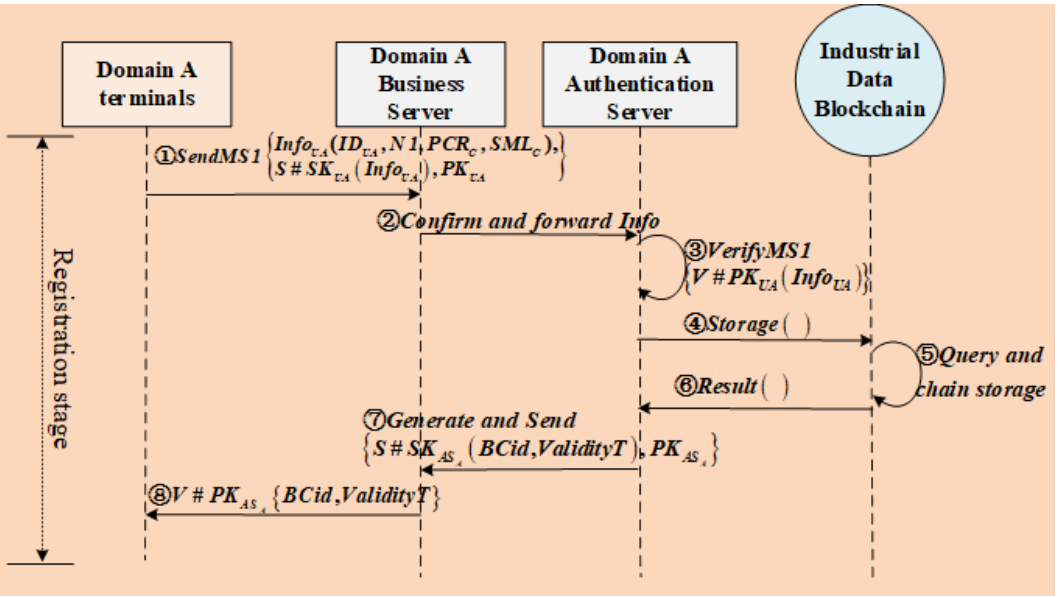
The user U_A sends a registration request to the BS_A, including its own *ID, PCR value, AIK public key, random number,* etc., which is signed and then sent together with the user information to the BS_A, which initially confirms its security and forwards it to the AS_A to call it for authentication and registration. The AS_A uses its public key to validate the freshness of the random number and whether the identity information already exists. The blockchain queries whether this device information already exists, and if it does, the registration fails; otherwise, it performs the registration storage operation on the device and returns the final result to the AS_A.

After the AS_A receives the registration success message, it generates the initial identity credential *BCid* as well as the validity period *ValidityT* and returns the result to the BS_A. The identity credential *BCid* generation and update algorithm is shown in Algorithm 2. The BS_A returns the message to the U_A, which uses the public key to verify the signature and obtains the identity credential *BCid*. Based on this, the registration of the device is complete, and the initial identity credential has been established.

Table 1. Description of protocol notation

Notation	Description
$Info_{d_i}\left(\ \right)$	Information about the device d_i
U_i, BS_i, AS_i	Domain i users, business servers and authentication servers(i=A,B)
$PCR_i; SML_i$	The PCR value and stored measurement logs of hardware devices
$I \,\&\, V_A^{d_i}$	Integrity measurement and verification of Domain A device d_i
$Session\_key$	Session key
$BCid; BCid'$	Existing identification credentials; Updated identification credentials
$ValidityT$	Validity of identity credential
$E*K\{\ \}; D*K\{\ \}$	Encrypting or decrypting messages using K
$S\#K\{\ \}; V\#K\{\ \}$	Sign or verify the message using K (K is the public or private key)
$N; T$	Random number; Timestamp
$SK_i; PK_i$	Private and public keys of the device

Figure 3. Registration protocol



Algorithm 2. Identity certificate BCid generation and update algorithm

Input: $ID, Timestamp, R, S\#SK\left(ID, Timestamp, R\right)$

Output: $BCid$

1 : *First enter the ID, timestamp, random number N, and sign the message to the authentication server.*

2 : *Verify the random factor and timestamp, and the three are combined to get string 'data'. Generate random salt, PBKDF2 is used to hash and salt data, and the 'hashedData' is generated by iterating 1000 times.*

$R' = V\#PK\left(R, Timestamp\right), data \Rightarrow \left(ID \,||\, Timestamp \,||\, R\right)$

if R' *equal* R *&& Timestamp is fresh*

$\Rightarrow \left(hashedData + salt\right) \xrightarrow{base64} BCid$ *and* $E*SK\left(BCid\right)$, *storage BCid and return*

else Message error stop.

3 : *When BCid needs to be updated to BCid', the generation of BCid' needs to trigger industrial perception verifies the status of hardware equipment such as its PCR value.*

if pass then *update the certificate;*

$\Rightarrow BCid = BCid'$

else disconnect the connection.

4.2 Authentication Stage Protocols

All service nodes in the domain have been registered locally before authentication. When requesting, first verify whether there are existing identity credentials, and if so, verify the legitimacy and validity of the identity credentials; in the authentication process, continuous industrial security perception of the state of the hardware device integrity measure and verification to ensure that the two sides of the

domain authentication success of the security of the trusted device before the subsequent operation, so as to update the identity credentials, to ensure that the validity of the identity as well as real-time message. Authentication is divided into local domain authentication and cross-domain authentication.

4.2.1 Local Domain Authentication

When a user requests a certain information service in the local domain, the participants are mainly the business servers and authentication servers in the local domain, and the design flow of the authentication protocol in the local domain is shown in Figure 4.

The U_A carries the *BCid* and sends a resource request to the BS_A, which receives the request and calls the AS_A, which verifies the legitimacy of its identity credentials, and if the verification fails, triggers the industrial security perception in the local domain to re-integrity measure and update the identity credentials of the device. The industrial perception stage encrypts the transmission process with session key *Session_key* and performs integrity measure and verification on the device as shown in Figure 5. The AS_A verifies the result and returns it to the BS_A for analyzing the decision and deciding whether to issue the resources or not. Based on this, this local domain trust is established to allow resource access and interactive operations for a certain period of time.

In this local industrial perception process, the U_A first sends request information to the BS_A, including device information, random numbers, signed device information, and existing identity credentials. The AS_A queries and verifies the identity credentials, and verifies the U_A*'s* integrity

Figure 4. Local domain authentication protocol

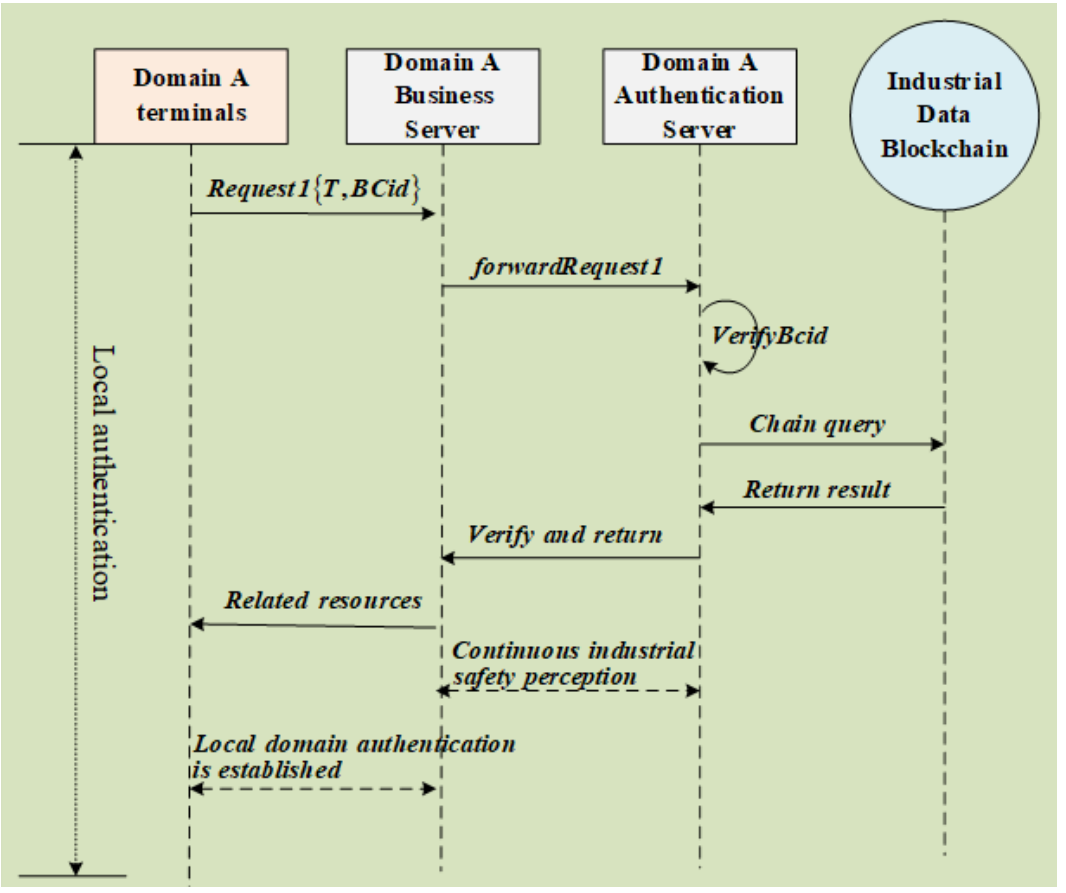
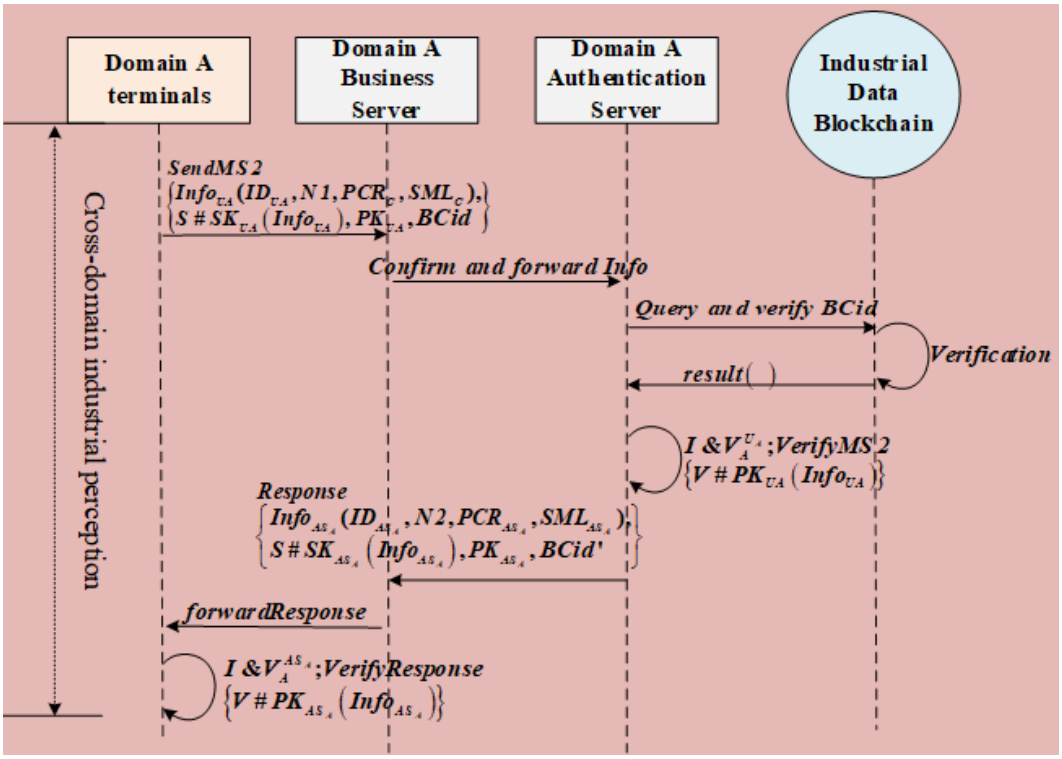


Figure 5. Local domain industry perception



measure results, verifying the integrity of the device and the security of the identity. After the above verification is passed, the AS_A regenerates the identity credentials and the validity period, and sends its own device information and random numbers, signs and sends them to BS_A, and AS_A forwards the message to the user terminal. The U_A verifies the AS_A*'s* integrity measure results and verifies the integrity of the device and the security of the identity. Through industrial security awareness, integrity measures and verifications of hardware devices are accomplished, and identity credentials are updated to ensure user security as well as information accuracy.

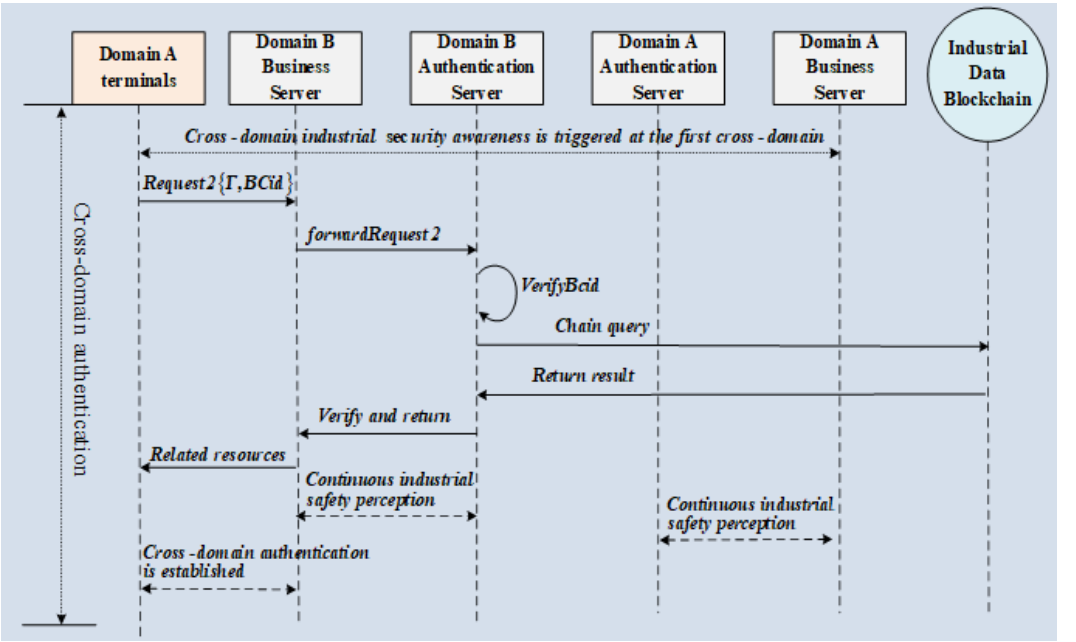
4.2.2 Cross-Domain Authentication

When a user requests an information service that is not local to the domain, the participants are mainly the two domain's authentication servers, business servers, and the blockchain. The design flow of the cross-domain authentication protocol is shown in Figure 6.

The initial cross-domain authentication steps are as follows:

When a user in domain A first accesses a resource in domain B, cross-domain industrial security perception is triggered, and this phase encrypts the message with the session key *Session_key*, completes the device integrity measure and verification, and then can generate unique identity credentials and their validity for this cross-domain, as shown in Figure 7. The U_A carries the obtained identity credentials and timestamps and sends a request to the BS_B, which forwards the request and initiates a call to the AS_B, which verifies the validity of the *BCid*. The AS_B verifies that the identity is trusted and returns the result to the BS_B; otherwise, it remeasures the integrity of the device and updates the identity credentials according to the cross-domain industrial security perception. The AS_B verifies the result and returns it to the BS_B, which analyzes the decision and decides whether to issue resources. After the above bidirectional authentication, the devices of both parties establish

Figure 6. Cross-domain authentication protocol



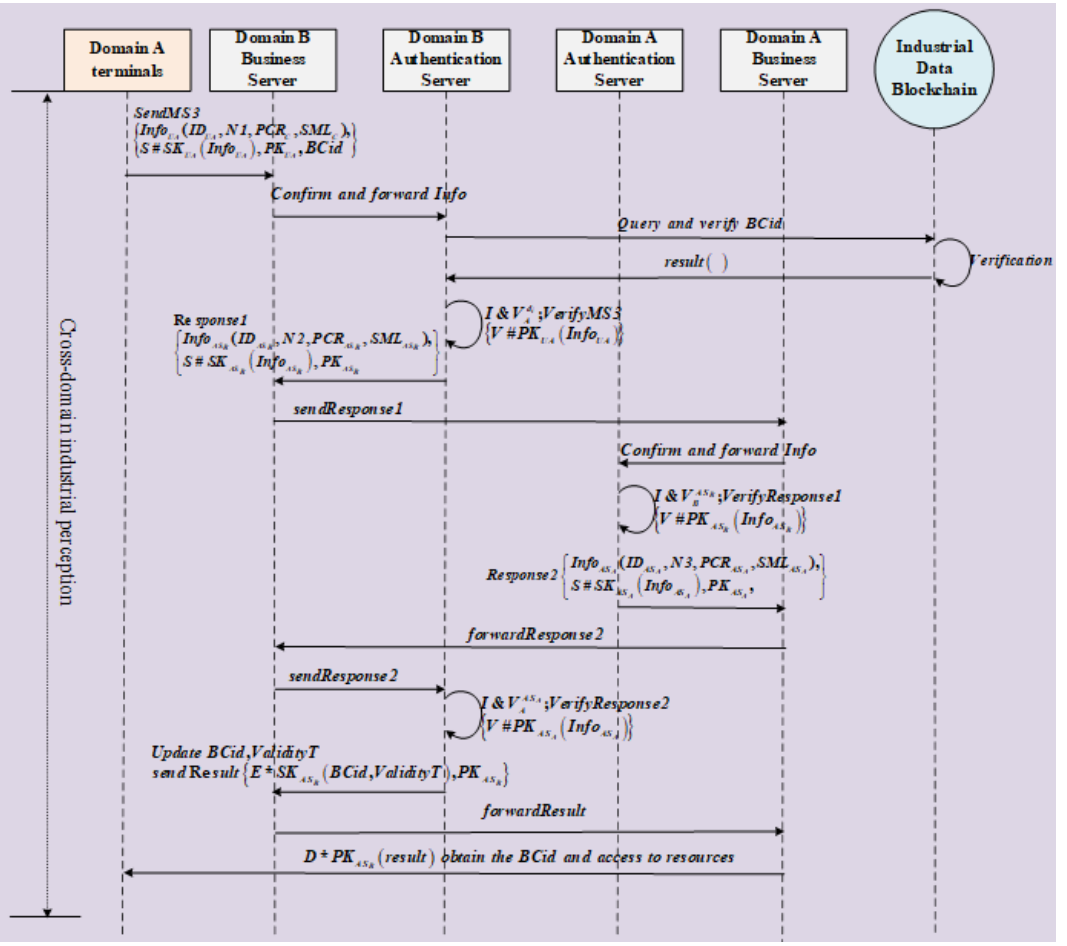
trusted access, and the BS_B resources are available for the U_A to access and interact with for a certain period of time.

The user sends a request message to the BS_B including device information, random numbers, signed device information and existing identity credentials. The AS_B queries and verifies the identity credentials and verifies the result after the U_A integrity measure, verifying the integrity of the device and the security of the identity. After verification, sign and send the AS_B device information and random numbers. the AS_A checks the results of the AS_B integrity measure, verifying the integrity of the device and the security of the identity. Subsequently, the signature sends the AS_A device information as well as a random number. The AS_B checks the result after the AS_A integrity measure and verifies the integrity of the device and the security of the identity. The AS_B re-generates the identity credentials and the validity period, encrypts them using the private key and sends them to the BS_B. The U_A decrypts them using the public key to obtain the latest identity credentials and the validity period.

Through cross-domain industrial security perception, it ensures the health status of the environment in which the hardware device is located, obtains the identity credentials, and guarantees the security of the user as well as the accuracy of the information.

After the initial cross-domain authentication is over, if the user accesses the same domain resources within a certain period, i.e., when cross-domain communication is performed again, there is no need for re-authentication. Taking the above cross-domain authentication of domain A user as an example, the U_A only needs to send the currently held *Bcid, ValidityT*, and random numbers to the BS_B, which will make a call to the AS_B to query the identity legitimacy and its validity period to make a decision judgment, and at the same time, check whether the corresponding random number N is fresh or not. If the verification passes, the resource distribution is carried out; if the verification fails, it is necessary to carry out industrial perception to query the state of hardware devices and identity credentials, and after the integrity measure of the hardware devices passes the verification, the identity credentials are updated, so as to carry out the above cross-domain authentication process.

Figure 7. Cross-domain industry perception



4.3 Revocation Stage Protocol

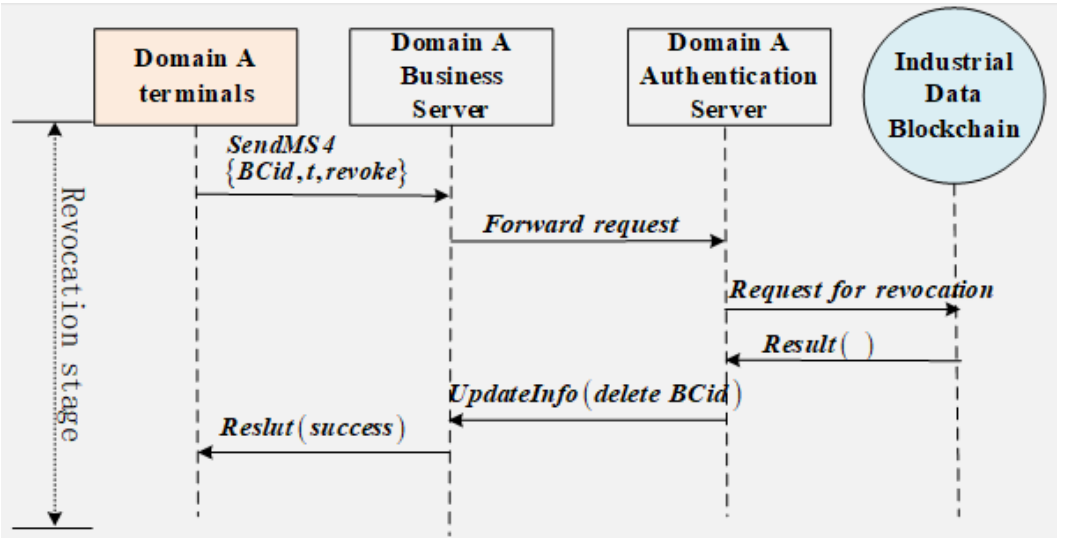
When a user's information needs to be deleted, submit a revocation request to the local authentication server, and the authentication server deletes the user's identity information and returns the result after verification. The flow of the identity information revocation protocol is shown in Figure 8.

The U_A submits a revocation request to the BS_A, sends the timestamp and the identity credentials it currently holds, and the BS_A forwards the message to the AS_A. The AS_A verifies whether the device information exists, sends the revocation request to the blockchain, updates the information by querying it on the blockchain and returns the result. The AS_A verifies the result, updates the information, forwards the result to the BS_A, and then returns it to the U_A. After successful revocation, its identity credentials are not available even within the validity period. If the U_A wants to access the information in the domain or request access to other domain resources again, it needs to reapply for registration, get the identity credentials and pass the authentication before accessing.

5. ANALYSIS AND COMPARISON OF SCENARIOS

The analysis of the security of the protocol and the judgment of the performance are important indicators of the efficiency of the protocol and whether it is applicable to specific scenarios. This

Figure 8. Revocation protocol



section firstly describes the potential attack model, and then combines the proposed design with a comprehensive analysis of the security, computational performance and overhead.

5.1 Attack Models

In digital factories and workshops operating in industrial Internet scenarios, a machine device or terminal may be subject to malicious attacks from external or internal sources once it is connected to the industrial network, assuming that an attacker with malicious threats exists and has the following capabilities:

1. The attacker will use the maliciously intercepted authenticated session information to re-initiate the authentication before the user authentication, and carry out communication interactions with the help of the obtained authenticated security information.
2. The attacker will use the relevant technology to forge false identities, impersonate legitimate workshop users, snoop on data privacy, tamper with the relevant data to destroy its integrity and authenticity or obtain data to cause data leakage or even malicious damage to the user terminal.
3. The attacker will use equipment vulnerabilities and defects to enter the network to change the control system and the control status of the equipment, to obtain the enterprise's key production data, resulting in major production accidents.

5.2 Security Analysis

For the attack models in the previous section to analyze the corresponding anti-attack ability and protocol security of this scheme, the specific security comparison is shown in Table 2.

Bidirectional authentication: The device cross-domain authentication scheme is mainly used to solve the problem of missing device authentication in industrial Internet scenarios. The authentication process first authenticates the client user identity and equipment, and then verifies the server side, realizing trusted cross-domain authentication between the two interacting parties.

Device integrity measurement: Based on the TPM, the integrity measurement and verification of the device is carried out to ensure that both users not only have legitimate identities, but also the

Table 2. Protocol security analysis

Protocols and Mechanisms	Bidirectional Authentication	Device Integrity Measurement	Replay Attack	Impersonation Attack	Man-in-the-Middle Attack	Identity Anonymity
Yuan et al.	×	×	√	√	√	√
Shen et al.	×	×	√	×	√	√
Jia et al.	×	×	√	√	√	×
Ours	√	√	√	√	√	√

hardware devices are in a security state, which effectively prevents the security threats brought by the hardware devices.

Replay attack: Both parties in the authentication process send messages using random numbers to ensure the freshness of the message, even if the message is intercepted by the adversary in the middle, the message is not fresh and will lead to authentication failure, effectively preventing replay attacks.

Impersonation attack: Each access needs to verify the user's identity credentials, and only legitimate users can carry out access operations. The identity credentials carried by this scheme when transmitting messages are hashed and salted and processed repeatedly for many times, which is quite difficult to crack, thus effectively preventing the replacement of impersonation attacks.

Man-in-the-middle attack: Both parties in the communication transmit messages by means of signature and encryption, and both parties use their own private key signatures that cannot be forged. If the attacker tampers with the message, the authentication cannot be passed and the message cannot be obtained, effectively preventing man-in-the-middle attacks.

Identity anonymity: This program uses temporary identity credentials for authentication, which need to be renewed after the expiration date, making the identity somewhat anonymous, avoiding malicious tracking and effectively improving identity security.

5.3 Computational Performance and Overhead Analysis

To compare the performance of this scheme with other existing cross-domain authentication protocol schemes, reference is made to the experimental results conducted by Kilinc & Yanik (2013) on a configuration of Intel Pentium Dual CPU E2200 2.20GHz, 2048MB RAM, and Ubuntu 12.04 32-bit operating system. The operations such as encryption and decryption operations, signature verification operations and hash operations are mainly evaluated and the meaning of the symbols is shown in Table 3. The evaluation metrics are mainly computation overhead and communication overhead.

This scheme is compared and analyzed with several other cross-domain authentication schemes, and Table 4 shows the statistical analysis of the overhead of different schemes cross-domain authentication schemes in terms of both computation and communication. In order to standardize the criteria to compare the protocols, it is assumed that the same asymmetric encryption/decryption algorithm as well as the same signature/check-signature algorithm and the same identity-based signature/check-signature algorithm are used.

The computational tasks of each protocol are mainly concentrated on the client or server side, and Fig. 9 shows the analysis and comparison chart of the computational time at each end. We can conclude that the computational overhead of this scheme at each end and in general is significantly lower than that of Yuan et al. (2017), and the computational overhead is also lower than that of the other two schemes. This scheme mainly takes session key encryption and decryption, verification of identity credentials and other operations in the authentication process, and the operations such as integrity measure and checking of the device and the generation and updating of the identity credentials are mainly placed in the industrial perception stage, and the authentication is done by only sending a message with the identity credentials to request resources, and the server side also only

Table 3. Meaning of calculation time symbols

Operation	Description	Operation	Description
H	Hash operation	T_{IBS}	Identity-based signature
T_{PE}	Public-key based encryption	T_{IBV}	Identity-based signature verification
T_{PD}	Public-key based decryption	T_{SE}	Symmetric encryption
T_{AS}	Asymmetric signature	T_{SD}	Symmetric decryption
T_{AV}	Asymmetric signature verification	T_{IDV}	Identity credential verification time
T_{P}	Bilinear pair	T_{IDTV}	Authority verification time

Table 4. Comparative analysis of computing overhead

Protocols and Overheads	Computational Operation	Time-Consuming(ms)	Communication(bit)
Yuan et al.I	$T_{IBS}+T_{IBV}+3T_{AS}+4T_{AV}+5T_{PE}+5T_{PD}+3T_{SE}+3T_{SD}+3T_{P}+4H$	116.25	1808
Yuan et al.II	$2T_{IBS}+2T_{IBV}+2T_{AS}+2T_{AV}+4T_{PE}+4T_{PD}+3T_{SE}+3T_{SD}+H$	111.05	1408
Shen et al.	$T_{IBS}+T_{IBV}+2T_{P}+2H$	41.364	1376
Jia et al.	$T_{IBS}+T_{IBV}+T_{IDTV}$	40.502	592
Ours	$T_{IDV}+2T_{SE}+2T_{SD}+T_{AS}+T_{AV}$	13.936	1184

needs to verify the identity credentials, which effectively reduces the communication overhead and computation of both sides. When authenticating, only the identity credentials are needed to send a message for resource request, and the server side only needs to verify the identity credentials, which effectively reduces the communication overhead and computation overhead between the two sides and improves the authentication speed.

Combined with the above charts, it can be concluded that this paper has a significant advantage over other schemes in terms of cross-domain authentication computation overhead, and the communication volume is also reduced. In the communication process due to the inclusion of identity credentials, which contain IDs, random numbers and other identities for multiple hashing and salting, so the communication volume is higher than Jia et al. (2020), but still better than several other schemes. Therefore, this scheme has better communication performance and the detailed communication overhead comparison is shown in Figure 10.

In the authentication process, latency is also a key indicator of the protocol, which can affect the availability, efficiency and user experience of the system. For the local and cross-domain authentication of this scheme, we conducted latency tests, and the test results are shown in Figure 11. In addition, in order to better evaluate the performance of this solution, we also conducted concurrency tests

Figure 9. Comparative analysis of computational overhead at each end

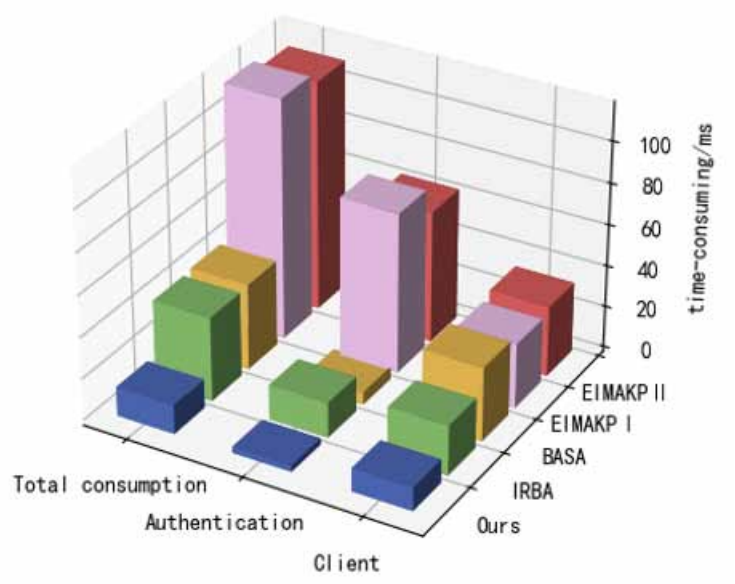
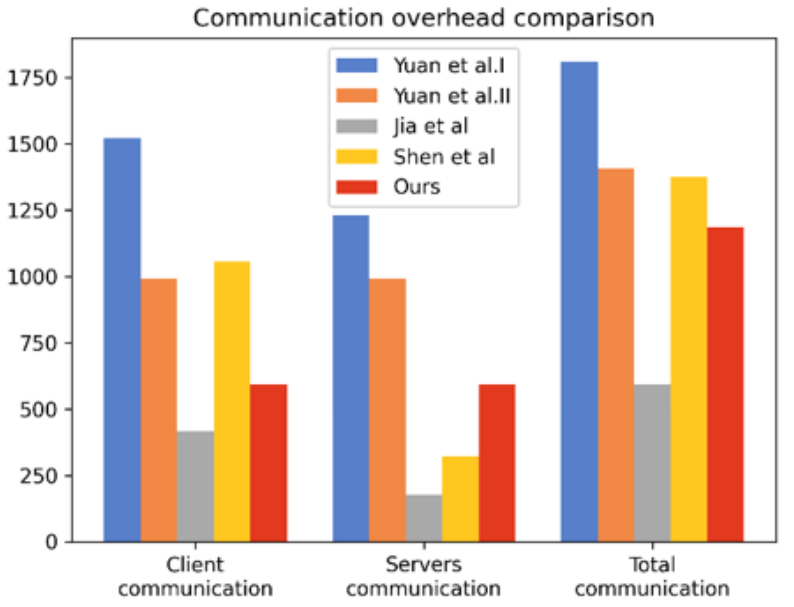


Figure 10. Comparative analysis of communication overhead at each end



to measure and record the average latency under different numbers of concurrency. By measuring and analyzing the latency, we can better determine whether the protocol has a better performance, so that we can further understand the efficiency and usability of this solution. Figure 12 shows the results of the latency test under different number of concurrences, which shows that this protocol has good usability.

Figure 11. Protocol latency analysis

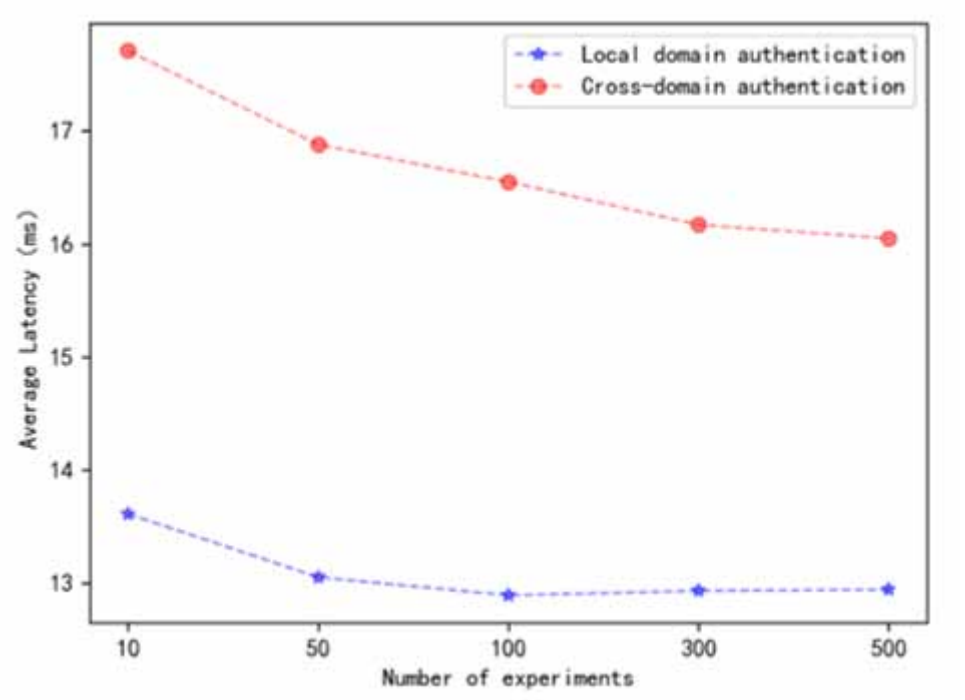
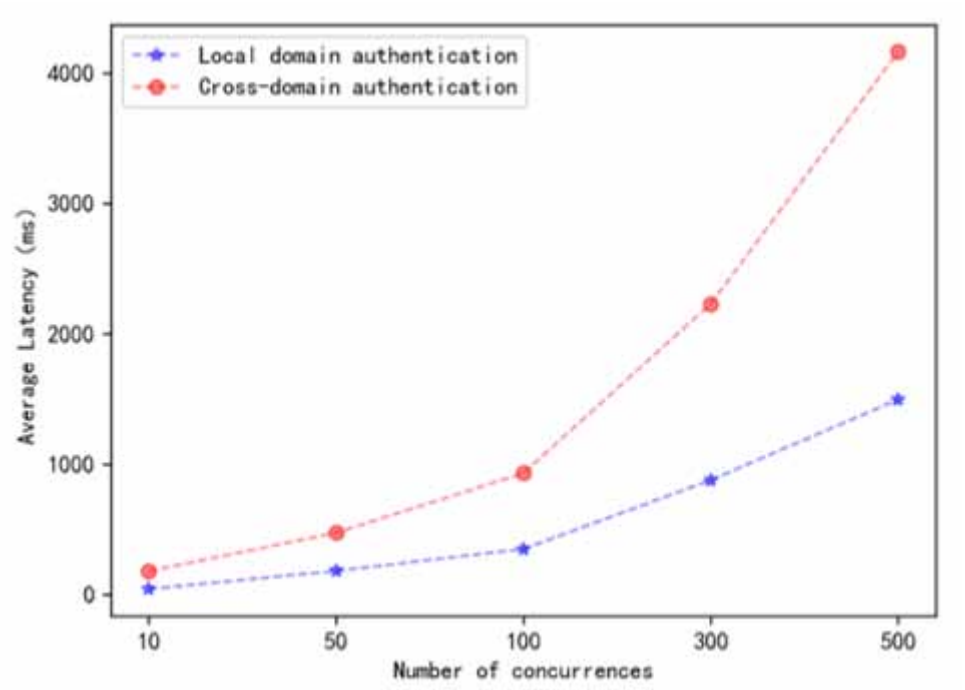


Figure 12. Average latency with different number of concurrencies



6. CONCLUSION

This paper proposes a layered framework for industrial Internet device authentication and trusted access, as well as an industrial security state awareness mechanism, and designs a cross-domain authentication scheme for devices based on the deep integration of trusted computing and blockchain technology for the current increasingly severe industrial Internet security environment. This scheme effectively solves the problem of cross-domain authentication and security verification of industrial equipment, realizes "one-time access, simultaneous verification", effectively improves the efficiency of equipment authentication, solves the overhead problem brought by the centralized architecture, effectively avoids the security threat brought by equipment integrity damage or identity fake invasion, and ensures that the local and cross-domain attacks in the industrial application scenarios can be avoided. It can effectively avoid security threats caused by equipment integrity damage or identity impersonation intrusion, and ensure the defense and security of local and cross-domain attacks in industrial application scenarios. Under the premise of comprehensively ensuring the identity trustworthiness and state security of industrial equipment, this program reduces the number of signatures and calculation time in the authentication process, effectively improving the authentication efficiency. The schemes and protocols proposed in this paper can be applied to industrial internet scenarios, providing critical support for industrial security, data privacy, automation and industry 4.0 trends to ensure secure and reliable communication and data exchange. In addition, seamless communication between devices, sensors, and systems has become particularly important in today's industrial networks, and cross-domain authentication is a key element to enable seamless communication, helping to achieve the goals of smart manufacturing, automated production, and resource optimization. As a next step, we will introduce the idea of industrial contextual security, expand industrial security perception elements, further improve the security and trustworthiness of industrial Internet device access, and comprehensively guarantee and enhance the security of industrial Internet key information infrastructure.

CONFLICT-OF-INTEREST STATEMENT

This to confirm that this article is authored by an Editor of this journal, who left the responsibility of handling this paper to another Managing Editor.

ACKNOWLEDGMENT

This work was supported by Project of Leading Talents in Science and Technology Innovation in Henan Province under Grant 204200510021, Program for Henan Province Key Science and Technology under Grant 222102210177, Grant 222102210072 and Grant 212102210383, as well as Henan Province University Key Scientific Research Project under Grant 23A520008. The authors appreciated the constructive feedback from the reviewers and editors during the whole reviewing process.

REFERENCES

Al-Qerem, A., Alauthman, M., Almomani, A., & Gupta, B. B. (2020). IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. *Soft Computing*, *24*(8), 5695–5711. doi:10.1007/s00500-019-04220-y

Almomani, A., Alauthman, M., Shatnawi, M. T., Alweshah, M., Alrosan, A., Alomoush, W., Gupta, B. B., Gupta, B. B., & Gupta, B. B. (2022). Phishing website detection with semantic features based on machine learning classifiers: A comparative study. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–24. doi:10.4018/IJSWIS.297032

Bao, Z., He, D., Khan, M. K., Luo, M., & Xie, Q. (2022). PBidm: Privacy-Preserving Blockchain-Based Identity Management System for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *19*(2), 1524–1534. doi:10.1109/TII.2022.3206798

Chen, J., Zhan, Z., He, K., Du, R., Wang, D., & Liu, F. (2021). XAuth: Efficient privacy-preserving cross-domain authentication. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3301–3311. doi:10.1109/TDSC.2021.3092375

Chen, S., Wen, H., Wu, J., Xu, A., Jiang, Y., Song, H., & Chen, Y. (2019). Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication. *Sensors (Basel)*, *19*(16), 3610. doi:10.3390/s19163610 PMID:31430988

Chen, Y., Wen, H., Wu, J., Song, H., Xu, A., Jiang, Y., Zhang, T., & Wang, Z. (2019). Clustering based physical-layer authentication in edge computing systems with asymmetric resources. *Sensors (Basel)*, *19*(8), 1926. doi:10.3390/s19081926 PMID:31022882

Cui, J., Liu, N., Zhang, Q., He, D., Gu, C., & Zhong, H. (2022). Efficient and Anonymous Cross-Domain Authentication for IIoT Based on Blockchain. *IEEE Transactions on Network Science and Engineering*, *10*(2), 899–910. doi:10.1109/TNSE.2022.3224453

Cvitić, I., Perakovic, D., Gupta, B. B., & Choo, K. K. R. (2021). Boosting-based DDoS detection in internet of things systems. *IEEE Internet of Things Journal*, *9*(3), 2109–2123. doi:10.1109/JIOT.2021.3090909

Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3179–3202. doi:10.1007/s13042-020-01241-0

Fatima, S., & Ahmad, S. (2021). Quantum key distribution approach for secure authentication of cloud servers. *International Journal of Cloud Applications and Computing*, *11*(3), 19–32. doi:10.4018/IJCAC.2021070102

Gaurav, A., Psannis, K., & Peraković, D. (2022). Security of cloud-based medical internet of things (miots): A survey. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–16. doi:10.4018/IJSSCI.285593

Gope, P., & Sikdar, B. (2018). Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet of Things Journal*, *6*(1), 580–589. doi:10.1109/JIOT.2018.2846299

Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation*, *32*(21), e4946. doi:10.1002/cpe.4946

Hu, B., Gaurav, A., Choi, C., & Almomani, A. (2022). Evaluation and comparative analysis of semantic web-based strategies for enhancing educational system development. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–14. doi:10.4018/IJSWIS.302895

Jeong, Y. S. (2022). Secure IIoT information reinforcement model based on IIoT information platform using blockchain. *Sensors (Basel)*, *22*(12), 4645. doi:10.3390/s22124645 PMID:35746431

Jia, X., Hu, N., Su, S., Yin, S., Zhao, Y., Cheng, X., & Zhang, C. (2020). IRBA: An identity-based cross-domain authentication scheme for the internet of things. *Electronics (Basel)*, *9*(4), 634. doi:10.3390/electronics9040634

Jia, X., Hu, N., Yin, S., Zhao, Y., Zhang, C., & Cheng, X. (2020). A2 chain: A blockchain-based decentralized authentication scheme for 5G-enabled IoT. *Mobile Information Systems*, *2020*, 1–19. doi:10.1155/2020/8889192

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), 2067–2087. doi:10.1007/s10586-020-03058-6

Khanam, S., Tanweer, S., & Khalid, S. S. (2022). Future of Internet of Things: Enhancing Cloud-Based IoT Using Artificial Intelligence. *International Journal of Cloud Applications and Computing*, *12*(1), 1–23. doi:10.4018/IJCAC.297094

Kilinc, H. H., & Yanik, T. (2013). A survey of SIP authentication and key agreement schemes. *IEEE Communications Surveys and Tutorials*, *16*(2), 1005–1023. doi:10.1109/SURV.2013.091513.00050

Kiran, M. A., Pasupuleti, S. K., & Eswari, R. (2022). Efficient Pairing-Free Identity-Based Signcryption Scheme for Cloud-Assisted IoT. *International Journal of Cloud Applications and Computing*, *12*(1), 1–15. doi:10.4018/IJCAC.305216

Kubilay, M. Y., Kiraz, M. S., & Mantar, H. A. (2019). CertLedger: A new PKI model with Certificate Transparency based on blockchain. *Computers & Security*, *85*, 333–352. doi:10.1016/j.cose.2019.05.013

Kumar, A., Saha, R., Conti, M., Kumar, G., Buchanan, W. J., & Kim, T. H. (2022). A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *Journal of Network and Computer Applications*, *204*, 103414. doi:10.1016/j.jnca.2022.103414

Kumar, R., Singh, S. K., Lobiyal, D. K., Chui, K. T., Santaniello, D., & Rafsanjani, M. K. (2022). A Novel Decentralized Group Key Management Scheme for Cloud-Based Vehicular IoT Networks. *International Journal of Cloud Applications and Computing*, *12*(1), 1–34. doi:10.4018/IJCAC.311037

Kumar, U., & Venkaiah, V. C. (2022). An Efficient Message Authentication Code Based on Modified MD5-384 Bits Hash Function and Quasigroup. *International Journal of Cloud Applications and Computing*, *12*(1), 1–27. doi:10.4018/IJCAC.308275

Li, D., Chen, R., Liu, D., Song, Y., Ren, Y., Guan, Z., Sun, Y., & Liu, J. (2022). Blockchain-based authentication for IIoT devices with PUF. *Journal of Systems Architecture*, *130*, 102638. doi:10.1016/j.sysarc.2022.102638

Li, S., Qin, D., Wu, X., Li, J., Li, B., & Han, W. (2022). False alert detection based on deep learning and machine learning. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–21. doi:10.4018/IJSWIS.313190

Liao, R. F., Wen, H., Wu, J., Pan, F., Xu, A., Jiang, Y., Xie, F., & Cao, M. (2019). Deep-learning-based physical layer authentication for industrial wireless sensor networks. *Sensors (Basel)*, *19*(11), 2440. doi:10.3390/s19112440 PMID:31142016

Liao, R. F., Wen, H., Wu, J., Pan, F., Xu, A., Song, H., Xie, F., Jiang, Y., & Cao, M. (2019). Security enhancement for mobile edge computing through physical layer authentication. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 116390–116401. doi:10.1109/ACCESS.2019.2934122

Liu, J., Liu, Y., Lai, Y., Li, R., Wu, S., & Mian, S. (2021). Cross-heterogeneous domain authentication scheme based on blockchain. *Journal of Artificial Intelligence and Technology*, *1*(2), 92–100. doi:10.37965/jait.2020.0060

Liu, S., Chen, L., Yu, H., Gao, S., & Fang, H. (2023). BP-AKAA: Blockchain-enforced Privacy-preserving Authentication and Key Agreement and Access Control for IIoT. *Journal of Information Security and Applications*, *73*, 103443. doi:10.1016/j.jisa.2023.103443

Ma, W., Zhang, Q., Ma, J., Xue, H., Hao, X., Li, H., Jia, W., Meng, Y., Wen, Z., & Zhang, J. (2021, February). Lightweight identity authentication scheme for IoT devices based on blockchain. In Journal of Physics: Conference Series (Vol. 1812, No. 1, p. 012027). IOP Publishing. doi:10.1088/1742-6596/1812/1/012027

Madhu, S., Padunnavalappil, S., Saajlal, P. P., Vasudevan, V. A., & Mathew, J. (2022). Powering up an IoT-enabled smart home: A solar powered smart inverter for sustainable development. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–21. doi:10.4018/IJSSCI.300362

Raj, M. G., & Pani, S. K. (2022). Chaotic whale crow optimization algorithm for secure routing in the IoT environment. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–25. doi:10.4018/IJSWIS.300824

Rakas, S. B., Timčenko, V., Kabović, M., & Kabović, A. (2021, March). Industrial Internet: Architecture, characteristics and implementation challenges. In *2021 20th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-4). IEEE.

Ren, P., Xiao, Y., Chang, X., Huang, P. Y., Li, Z., Gupta, B. B., Chen, X., & Wang, X. (2021). A survey of deep active learning. *ACM Computing Surveys*, *54*(9), 1–40. doi:10.1145/3472291

Sadatacharapandi, T. P., & Padmavathi, S. (2022). Survey on Service Placement, Provisioning, and Composition for Fog-Based IoT Systems. *International Journal of Cloud Applications and Computing*, *12*(1), 1–14. doi:10.4018/IJCAC.305212

Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and opportunities in securing the industrial internet of things. *IEEE Transactions on Industrial Informatics*, *17*(5), 2985–2996. doi:10.1109/TII.2020.3023507

Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE Journal on Selected Areas in Communications*, *38*(5), 942–954. doi:10.1109/JSAC.2020.2980916

Tembhurne, J. V., Almin, M. M., & Diwan, T. (2022). Mc-DNN: Fake news detection using multi-channel deep neural networks. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–20. doi:10.4018/IJSWIS.295553

Tiwari, A., & Garg, R. (2022). Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–18. doi:10.4018/IJSWIS.306260

Tong, F., Chen, X., Wang, K., & Zhang, Y. (2022). CCAP: A complete cross-domain authentication based on blockchain for Internet of things. *IEEE Transactions on Information Forensics and Security*, *17*, 3789–3800. doi:10.1109/TIFS.2022.3214733

Vinoth, R., Deborah, L. J., Vijayakumar, P., & Gupta, B. B. (2022). An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical IoT environments. *IEEE Transactions on Network Science and Engineering*, *9*(5), 3633–3642. doi:10.1109/TNSE.2022.3176407

Wang, M., Rui, L., Yang, Y., Gao, Z., & Chen, X. (2022). A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network. *IEEE Transactions on Network and Service Management*, *19*(3), 2664–2676. doi:10.1109/TNSM.2022.3180357

Wang, X., Gu, C., Wei, F., Lu, S., & Li, Z. (2022). A Certificateless-Based Authentication and Key Agreement Scheme for IIoT Cross-Domain. *Security and Communication Networks*, *2022*, 2022. doi:10.1155/2022/3693748

Wollschlaeger, M., Sauter, T., & Jasperneite, J. (2017). The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Industrial Electronics Magazine*, *11*(1), 17–27. doi:10.1109/MIE.2017.2649104

Xiao, X., Guo, F., & Hecker, A. (2020, December). A lightweight cross-domain proximity-based authentication method for IoT based on IOTA. In 2020 IEEE Globecom Workshops (GC Wkshps (pp. 1-6). IEEE. doi:10.1109/GCWkshps50303.2020.9367500

Xie, F., Wen, H., Wu, J., Chen, S., Hou, W., & Jiang, Y. (2019). Convolution based feature extraction for edge computing access authentication. *IEEE Transactions on Network Science and Engineering*, *7*(4), 2336–2346. doi:10.1109/TNSE.2019.2957323

Yuan, C., Zhang, W., & Wang, X. (2017). EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system. *Arabian Journal for Science and Engineering*, *42*(8), 3275–3287. doi:10.1007/s13369-017-2447-9

Zhai, Z., Lai, G., Cheng, B., Qian, J., Zhao, L., Wu, J., & Wan, Z. (2022). Lightweight secure detection service for malicious attacks in wsn with timestamp-based mac. *IEEE Transactions on Network and Service Management*, *19*(4), 5299–5311. doi:10.1109/TNSM.2022.3194205

Zhang, H., Chen, X., Lan, X., Jin, H., & Cao, Q. (2020). BTCAS: A blockchain-based thoroughly cross-domain authentication scheme. *Journal of Information Security and Applications*, *55*, 102538. doi:10.1016/j.jisa.2020.102538

Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. *IEEE Internet of Things Journal*, *9*(22), 22501–22515. doi:10.1109/JIOT.2022.3176192

Zhang, Y., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. (2022). A lightweight authentication scheme based on consortium blockchain for cross-domain IoT. *Security and Communication Networks*, *2022*, 1–15. doi:10.1155/2022/9686049

Zhong, H., Gu, C., Zhang, Q., Cui, J., Gu, C., & He, D. (2023). Conditional privacy-preserving message authentication scheme for cross-domain Industrial Internet of Things. *Ad Hoc Networks*, *144*, 103137. doi:10.1016/j.adhoc.2023.103137

Tiantian Zhang, born in 1999, is currently pursuing her master degree in Software Engineering in Information Engineering College and Henan International Joint Laboratory of Cyberspace Security Applications at Henan University of Science and Technology, P. R. China. Her research interests include industrial Internet security, trusted computing, and authentication.

Zhiyong Zhang (Senior Member, IEEE), received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, P. R. China, respectively. He was ever post-doctoral fellowship at School of Management, Xi'an Jiaotong University, China. Nowadays, he is Director of Henan International Joint Laboratory of Cyberspace Security Applications, Vice-Dean of College of Information Engineering, and full-time Henan Province Distinguished Professor at Henan University of Science and Technology, China. He is also a visiting professor of Computer Science Department of Iowa State University. His research interests include cyber security and privacy computing, social computing and social intelligence, cyber-physical system and industrial Internet security. Recent years, he has published over 150 scientific papers in TDSC, TCSS, TBD, etc, and edited 6 books in the above research fields, and also holds 20 authorized patents. He is Chair of IEEE MMTC DRMIG, IEEE Systems, Man, Cybernetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Committeeman of China National Audio, Video, Multimedia System and Device Standardization Technologies Committee. And also, he is editorial board member and associate editor of IEEE Access (IEEE), Human-centric Computing and Information Sciences (Springer), Multimedia Tools and Applications (Springer), Journal of Big Data (Springer), and leading guest editor or co-guest Editor of Applied Soft Computing (Elsevier), Computer Journal (Oxford) and Future Generation Computer Systems (Elsevier). And also, he is Chair/Co-Chair and TPC Member for numerous international conferences/ workshops on cyber security and privacy computing, big data and artificial intelligence.

Kejing Zhao received her Master's degree in Mathematics at Henan University of Science and Technology, Luoyang, China. She is currently pursuing her Ph.D. degree in College of Information Engineering and Henan International Joint Laboratory of Cyberspace Security Applications at Henan University of Science and Technology, P. R. China. Her research interests include Industrial Internet security, industrial situation analytics, and industrial big data.

Brij B. Gupta is working as Director of International Center for AI and Cyber Security Research and Innovations, and Distinguished Professor with the Department of Computer Science and Information Engineering (CSIE), Asia University, Taiwan. In more than 17 years of his professional experience, he published over 500 papers in journals/conferences including 35 books and 11 Patents with over 24,000 citations. He has received numerous national and international awards including Canadian Commonwealth Scholarship (2009), Faculty Research Fellowship Award (2017), MeitY, GoI, IEEE GCCE outstanding and WIE paper awards and Best Faculty Award (2018 & 2019), NIT KKR, respectively. Prof. Gupta was selected for 2022 Clarivate Web of Science Highly Cited Researchers in Computer Science. He was also selected in the 2022, 2021 and 2020 Stanford University's ranking of the world's top 2% scientists. He is also a visiting/adjunct professor with several universities worldwide. He is also an IEEE Senior Member (2017) and also selected as 2021 Distinguished Lecturer in IEEE CTSoc. Dr Gupta is also serving as Member-in-Large, Board of Governors, IEEE Consumer Technology Society (2022-2024). Prof Gupta is also leading IJSWIS, IJSSCI, STE and IJCAC as Editor-in-Chief. Moreover, he is also serving as lead-editor of a Book Series with CRC and IET press. He also served as TPC members in more than 150 international conferences also serving as Associate/Guest Editor of various journals and transactions. His research interests include information security, Cyber physical systems, cloud computing, blockchain technologies, intrusion detection, AI, social media and networking.

Varsha Arya did Master's degree from Rajasthan University, India in 2015 and has been working as a researcher for the last 7 years. She published more than 25 papers in top journals and conferences. Her research interests include business administration, technology management, Cyber physical systems, cloud computing, healthcare, and networking. Currently, she is doing research at Asia University, Taiwan.