Workgroup: Industrial Internet of Things
Internet-Draft:
draft-tang-iiot-architecture-00
Published: 2 November 2020
Intended Status: Informational
Expires: 6 May 2021
Authors: C. Tang
Chongqing University
H. Wen
Chongqing University
S. Ruan
Chongqing University
B. Huang
Chongqing University
X. Feng
Chongqing University

IPv6 and 5G based Architecture for IIoT

Abstract

As the foundation of the current new round of industrial revolution, the Industrial Internet of Things (IIoT) based on Cyber-Physical Systems (CPS) [smart-factory] has become the focus of research in various countries. In the entire development stage of IIoT, one of the key issues is the standardization of the IIoT architecture. With the development of intelligent manufacturing technology, the number of the IIoT devices will increase sharply, and a large amount of data will be generated in the industrial manufacturing process. However, traditional industrial networks cannot meet the IIoT requirements for high data rates, low latency, massive connections, interconnection and interoperability. The current IIoT architectures also have various limitations: mobility, security, scalability, and communication reliability. These limitations hinder the development and implementation of IIoT. As a network layer protocol, IPv6 can solve the problem of IPv4 address exhaustion. As a high-speed, low-latency wireless communication technology, 5G has great potential in promoting IIoT. In order to solve the above problems, this draft proposes an IIoT architecture based on IPv6 and 5G. It can provide high-speed, low-latency communication services, provide massive connectivity, mobility, scalability, security and other features for industrial device. And the architecture can provide generalized, refined, and flexible network services for devices outside the factory. And an information model is defined to standardize the representation of information in IIoT. Finally, the draft discusses security challenges and recommendations in IIoT.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 May 2021.

Copyright Notice

Table of Contents

1. Introduction

IIoT is an industry and application ecology formed by the comprehensive and deep integration of the Internet, information technology and industrial systems, and IIoT is a key information infrastructure for the development of industrial intelligence. Its essence is based on the network interconnection between machines, raw materials, control systems, information systems, products, and people. Intelligent control, operation optimization and production organization reform will be achieved through comprehensive in-depth perception of industrial data, real-time transmission and exchange, fast calculation processing and advanced modeling analysis. The IIoT foundation is the system architecture, this is the interconnection and intercommunication of the entire industrial system through technologies such as the Internet of Things and the Internet to promote the full circulation and seamless integration of industrial data.

The communication technology in the industrial network interconnection architecture needs to meet the following major requirements:

*High communication rate. More and more manufacturing activities, such as real-time monitoring of all production factors and the entire production process, and the application of cloud computing, edge computing, virtual reality and augmented reality in the manufacturing industry, will generate a large amount of manufacturing data, which needs to be stable and uninterrupted data rate exceeding 25 Mbps [iiot-5g] .

*High coverage. The goal of the IIoT is to establish "ubiquitous communication." In other words, any area of the manufacturing plant should achieve 100% networking coverage. However, in actual factories, due to the complex production environment, such as electromagnetic interference and obstacles, the current communication technology cannot meet the requirements of high coverage.

*Low latency. Advanced manufacturing activities, such as human-machine cooperation, machine-machine cooperation, and remote real-time control, have higher requirements on communication delays, and generally require lower delays (about 1 ms). Although the current wireless communication technology has made great progress, and the end-to-end delay is about 20-100 ms [iiot-5g] , it still cannot meet the urgent need for low delay in IIoT communication.

*Massive connections. Compared with traditional manufacturing, because of the interconnection of all things in IIoT, data

collection in the entire process and will inevitably lead to an exponential increase in the number of communication nodes. Taking into account the current communication technology, wired communication cannot meet the requirements of massive node connections due to its difficult to arrange lines, and wireless communication cannot meet the requirements due to the limitation of the number of access nodes.

*Interconnection. In the development of industrial networks, there are many different communication protocols. Such as fieldbus protocols: PROFIBUS, Modbus, HART, etc. Industrial Ethernet protocols: Ethernet/IP, PROFINET, Modbus TCP, etc. Industrial wireless protocols: WLAN, Bluetooth, WirelessHART, etc. Because these protocols use different technologies at the physical layer, link layer, and application layer, the interconnection and interoperability are not ideal, which affects the expansion of the IIoT to some extent.

The main work of this architecture is introduced as follows:

Combining the actual scenarios of factory intelligent manufacturing and the requirements of IIoT for communication technology, an industrial network interconnection architecture based on IPv6 and 5G communication technology is designed, which can provide high-speed, high-reliability, and low-latency communication services, including inside the factory The network provides functions such as massive connection, mobility, equipment registration and discovery, and security for industrial production-related equipment; the factory external network provides generalized, refined, and flexible network services for equipment outside the factory. In order to standardize the representation of information in IIoT, an information model is defined. Summarized the current security challenges in IIoT, and put forward some security recommendations.

2. IIoT Architecture

In the IIoT architecture, the network is the foundation, providing infrastructure for the comprehensive interconnection of people, machines, and things, and promoting the full flow and seamless integration of various industrial data. The industrial Internet network connection involves different technical fields with multiple elements and multiple subjects inside and outside the factory, with a large scope of influence and many optional technologies. There are various network connection technologies in the industrial field. These technologies are designed for specific scenarios in the industrial field, and have played a huge role and performance advantages in specific scenarios. However, in terms of data interoperability and seamless integration, they often cannot meet the growing demands of IIoT.

The overall goal of IIoT network connection is to promote the interconnection and intercommunication between systems, unlock data from isolated systems and networks, and make data play a greater value for applications within and across industries.

This chapter proposes an industrial network system architecture based on the transformation of factory IP network, including two major networks, the factory internal network and the factory external network, as shown in Figure 1.

The factory internal network is used to connect various elements in the factory, including people (such as production people, designers, external people), machines (such as equipment, office equipment), materials (such as raw materials, work in progress, finished products), Environment (such as instruments, monitoring equipment), etc. Through the factory internal network, it is interconnected with enterprise data centers and application servers to support business applications in the factory.

The factory external network is used to connect smart factories, branches, upstream and downstream collaborative enterprises, industrial cloud data centers, smart products, and users. The data center/application server in the smart factory is interconnected with the industrial cloud data center outside the factory, through the factory external network. Branches/collaborative enterprises, users, and smart products are also connected to the industrial cloud data center or enterprise data center through the factory external network. The data intercommunication in IIoT realizes the seamless transfer of data and information among various elements and systems, so that heterogeneous systems can "understand" each other at the data level, thereby realizing data interoperability and information integration. IIoT requires breaking information islands, realizing cross-system intercommunication of data, and fusion analysis. Therefore, the data interoperability connection layer supports the convergence of the underlying data generated by various factory elements and factory products to the data center on the one hand; on the other hand, it provides access interfaces to the data of the multi-source heterogeneous system for the upper-layer applications to support industrial applications. And the factory external network also should support the rapid development and deployment of industrial application.

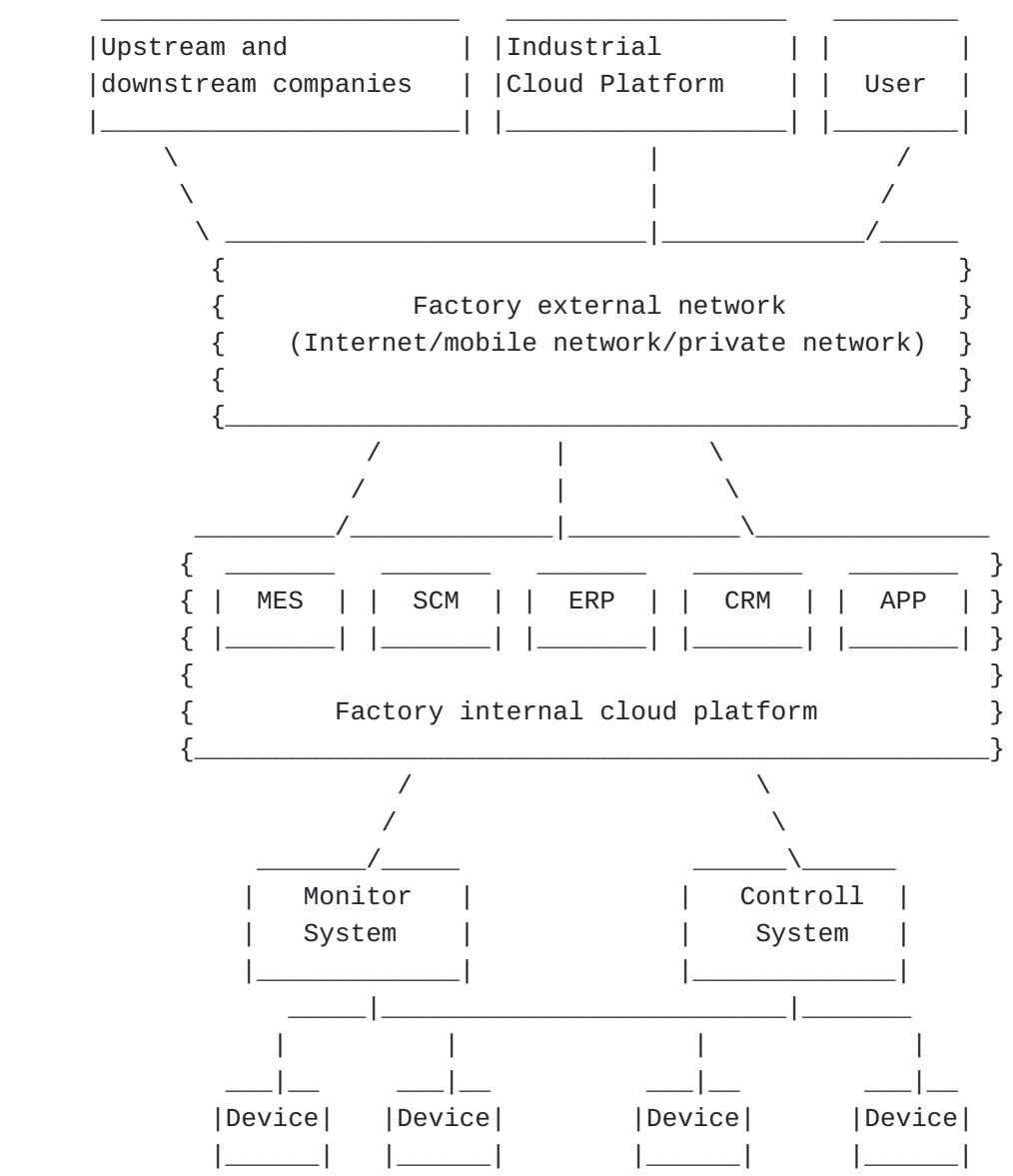

Figure 1: IIoT Architecture

Architecture advantages:

*High communication rate. The factory network adopts industrial PON and 5G technology, which can realize high-speed data transmission.

*Low communication delay. The Ethernet-based TSN network [tsn] and 5G wireless network can realize low-latency communication and ensure real-time industrial production.

*Massive connections. IPv6 [I-D.ietf-6lowpan-usecases] can assign an IP address to each industrial IoT device, and the 5G network supports the wireless access of a large number of IIoT devices.

*Scalability. When new industrial equipment joins the network, it can register with the edge server. When other industrial equipment has data and service requirements for the new industrial equipment, the new industrial equipment can be found on the edge server to access data or services.

*Mobility. After the device moves in multiple networks, it will register with the edge server again, and the device will obtain a new address from the edge server to perform subsequent communication.

*Localization of computing and storage. Use edge computing technology to perform computing or data storage services in edge servers close to industrial sites [edge-computing].

*Support multiple communication protocols. Use OPC UA protocol, support TCP, WebSocket, HTTP and other transmission protocols, which can realize device-to-device communication; support UDP broadcast, MQTT, AMQP and other protocols, and realize Sub/Pub communication [I-D.ietf-core-coap-pubsub].

*Cloudization of network services outside the factory. Based on cloud computing and enterprise dedicated line technology, the enterprise business system will be deployed to the cloud to facilitate external services. It can also provide segmented services for different scenarios such as public cloud and private cloud. Use network virtualization technology to improve the flexibility of network services, so that The factory external network will be able to quickly open services and quickly adjust services according to enterprise requirements.

3. The Factory Internal Network

3.1. Status and Development Trends

In the IIoT factory, on the one hand, the digitization of the factory requires that the digitization of many existing business processes be carried by the corresponding network. On the other hand, a large number of new networked devices have been introduced, such as AGVs, robots, mobile handheld devices, etc.; a large number of new business processes have been introduced, such as asset performance management, predictive maintenance, and personnel/ material positioning. The introduction of new equipment and business processes creates new demands on the network. As a result, the traditional two networks (production network and office network) in the factory will become multiple networks, which will

correspondingly cause changes in the network architecture in the factory.

In order to break information islands and improve operational efficiency, companies will deploy business systems that were originally deployed on various servers, such as MES, PLM, ERP, SCM, CRM, etc., to the data center/cloud platform in the factory. The data generated by each networked device and business process must be able to be aggregated in the data center/cloud platform in real time for joint analysis and rapid decision-making. Changes in business system deployment will also cause changes in network architecture.

The IIoT demand for flexible manufacturing and personalized customization requires the production domain to be flexibly reconfigured according to requirements, and intelligent machines may be adjusted and migrated between different production domains. This requires the network architecture in the factory to be able to adapt to the needs of fast networking and flexible adjustment.

The factory internal network proposed in this chapter can be understood from two aspects: functional view and network view.

3.2. Functional View

Functional view: According to the specific functions of the system and devices, and the location of the network, the factory internal network can be divided into device layer, control layer, and factory management layer, as shown in Figure 2.

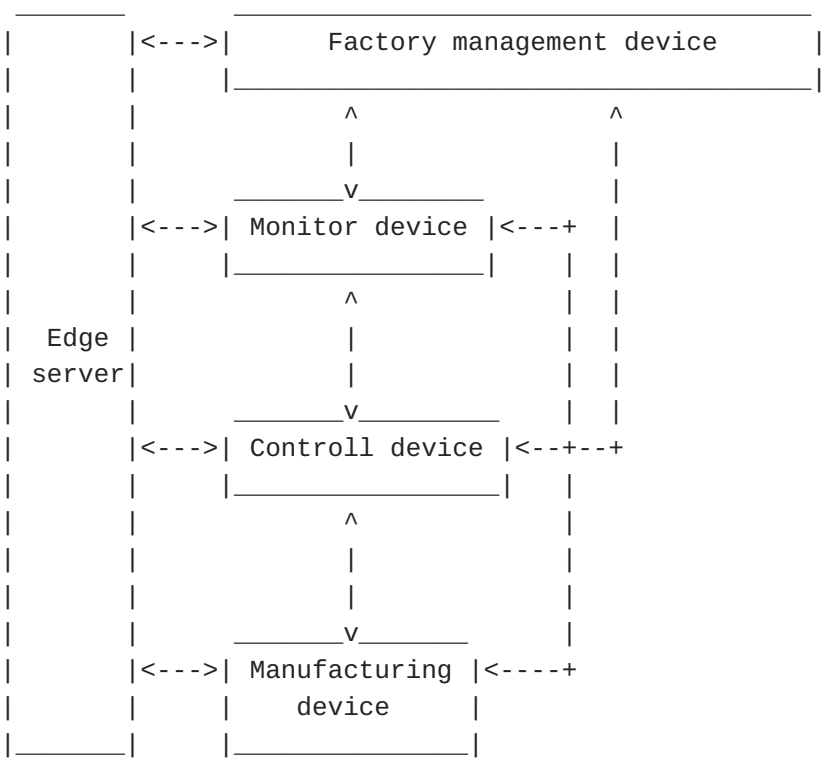

Figure 2: Functional View

(1) Device layer: realize the sensing and execution of the manufacturing process, and define the activities involved in the perception and execution of the manufacturing process. The time resolution granularity can be seconds, milliseconds, and microseconds. Various sensors, transmitters, actuators, RTUs, barcode scanners, RFID readers, and intelligent manufacturing equipment such as CNC machine tools, industrial robots, AGVs, conveyor lines, etc. run on this layer. These devices are collectively referred to as field devices.

(2) Control layer: Realize the monitoring and control of the manufacturing process, and define the activities of monitoring and controlling the manufacturing process. The time resolution granularity can be hours, minutes, seconds, and milliseconds. According to different functions, this level can be further subdivided into:

*Monitoring and control layer: With operation monitoring as the main task, it also has some management functions such as advanced control strategies and fault diagnosis. Visual data acquisition and monitoring system (SCADA), HMI (human-machine interface), DCS operator station, real-time database server, etc. run on this layer;

*On-site control layer: measure and control the production process, collect process data, perform data conversion and processing, output control signals, and realize logic control, continuous control and batch control functions. Various programmable control equipment, such as PLC, DCS controller, industrial computer (IPC), other special controllers, etc. run on this layer.

(3) Factory management: realize the production management of the factory and define the workflow/recipe control activities for the production of expected products, including: maintenance records, detailed production scheduling, reliability assurance, etc. The time resolution granularity can be day, shift, hour, minute, second. Manufacturing execution system (MES), warehouse management system (WMS), quality management system (QMS), energy management system (EMS), etc. operate at this layer.

In order to achieve the scalability of the IIoT (after a new device joins the network, other devices can access data or call related services), this architecture designs device registration and device discovery functions.

Device registration: When a new device is connected to the network, it will register its name with the edge gateway. The format of the registered name is /Service-Name/Gateway-Name/Device-Name, and the IP address of the device is stored and bound with the name.

Device discovery: When a device needs to access data in other devices or call services in other devices, it can be queried in the edge gateway. It can find the IP address of a corresponding group of devices based on the service name and gateway name, and based on Service name, gateway name, device name to find the corresponding IP address of a certain device. After finding the IP address, device can communicate with the corresponding device.

3.3. Network View

Network view: The factory internal network can be divided into three parts: edge network, backbone network, and factory cloud platform. They can be interconnected through industrial PON. As shown in Figure 3.

Due to the diversification of connected production factors, the edge network presents a variety of types: according to business needs, the edge network can be an industrial control network, office network, monitoring network, positioning network, etc.; according to real-time requirements, the edge network can be real-time network, non-real-time network; according to the transmission medium, the edge network can be wired network or wireless network; according to

the communication technology adopted, the edge network can be industrial Ethernet, 5G wireless network, etc.; the range of the edge network may be a workshop, An office building, a warehouse, etc.; each edge network is composed of edge servers, edge gateways, and field devices. Industrial enterprises can comprehensively consider business requirements and costs, and select appropriate technologies to deploy corresponding edge networks.

The backbone network is used to realize the interconnection between edge networks, cloud platforms/data centers in the factory, etc., requiring high bandwidth and high speed. Depending on the size of the enterprise, the backbone network can be large or small. It can be a cluster of fully interconnected routers, or it can include only one or two backbone routers.

For example, industrial device, control device, and monitoring device that need wired connections can be connected to switches that support industrial Ethernet protocols through optical fibers. The specific physical layer protocol can use industrial PON, and the data link layer protocol can use TSN protocol to form TSN Ethernet edge network.

Industrial device, control device, and monitoring device that need wireless connections can be connected to 5G base stations through 5G wireless connections to form a 5G wireless edge network.

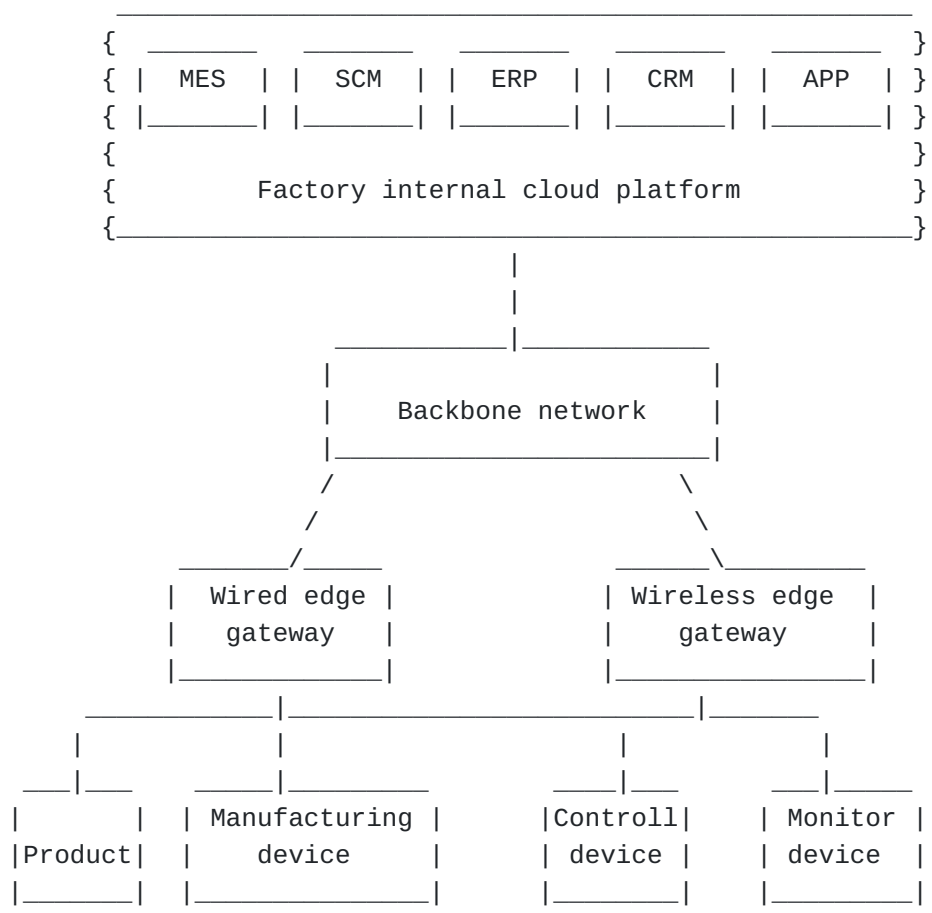

Figure 3: Network View

In order to realize the communication between edge networks of different protocols and the IP of industrial device, control device, and monitoring device, the IPv6 protocol can be used at the network layer. However, there are still a large number of devices and applications of the IPv4 protocol. In the transition phase to the IPv6 protocol, if the number of IPv4 devices and applications is large, the GI DS LITE tunnel technology solution can be used. If the number of IPv4 devices and applications is small, IPv4/IPv6 dual-stack technology solutions can be used

The backbone network is used to realize the interconnection between edge networks and cloud platforms in the factory, and requires high bandwidth and high speed. Depending on the size of the enterprise, the backbone network can be large or small. It can be a cluster of fully interconnected routers, or it may contain only one or two backbone routers.

The factory cloud platform can be upgraded to a TSN network on the basis of the original standard Ethernet, which can meet the requirements of industrial cloud platforms for high bandwidth and

low latency. TSN also has excellent upper-layer support compatibility and can support a variety of upper-layer communication protocols. For example, TSN and OPC UA can solve data intercommunication problems in the factory, and extend OPC UA data collection and cloud services to the field level. Our architecture will realize all-round real-time data collection and real-time operation in the production environment.

3.4. Way of Communication

The relationship between the functional view and the network view: the communication between the device layer and the control layer can be realized in the edge network; the functions of the factory management layer can be deployed in the factory cloud platform; the backbone network is responsible for the communication between the device layer, the control layer and the factory management layer.

(1) Communication between device and device: The one-to-one communication between devices can adopt the C/S architecture in OPC UA, and support the transmission protocols of TCP, WebSocket, and HTTP. OPC UA server and client are separately deployed in the two devices. When device need to access data or send instructions, it can use its own client to initiate communication with the other's OPC UA server. As shown in Figure 4.

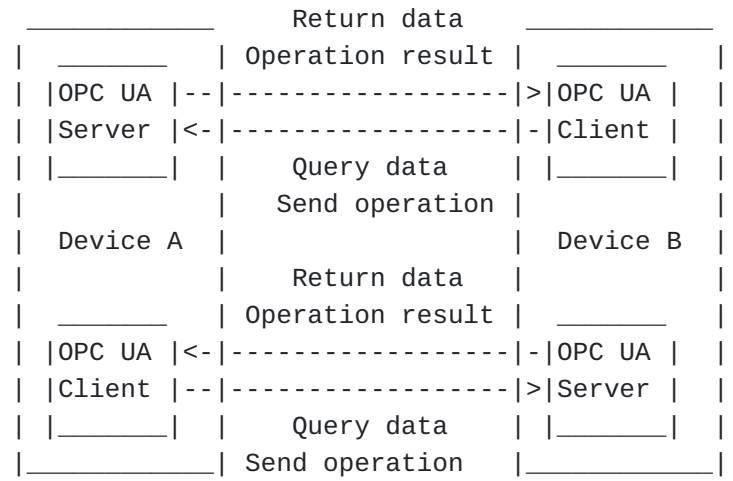

Figure 4: The C/S Architecture in OPC UA

The communication between one-to-many devices can use the Pub/Sub mechanism in OPC UA, and supports multiple mechanisms such as UDP broadcast, MQTT, AMQP, etc. If multiple devices have requirements for the data in one device, multiple devices can subscribe to this device. This device will publish this data to multiple devices when it collects or detects data changes. As shown in Figure 5.

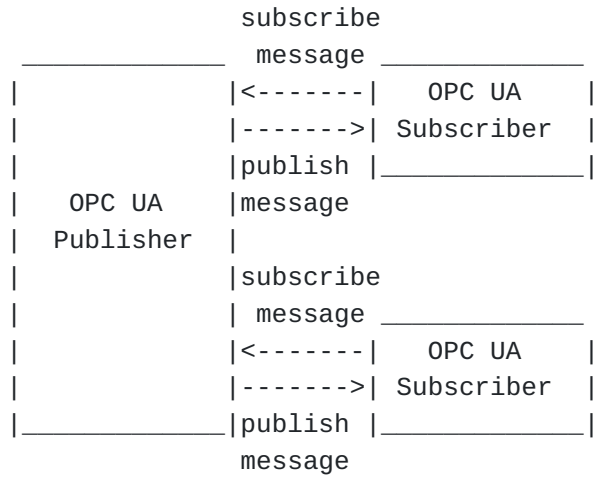

Figure 5: Pub/Sub mechanism in OPC UA

(2) Communication between device and edge server.

Use the server/client mode in OPC UA, which is suitable for application scenarios such as larger data volume and industrial automation control. For example, in the scene of machine vision product quality inspection, device uses a camera to collect machine vision pictures of the product after the product is manufactured or assembled, and the picture is sent to the edge server's intelligent detection algorithm for analysis and processing through the OPC UA protocol. Then the edge server returns the detection result to the industrial equipment, and the industrial equipment performs the next step according to the detection result.

Use the subscription/push mode in MQTT, which is suitable for communication between devices with small data volume, low bandwidth, and low hardware resources and edge servers. For example, in the scenario of factory temperature intelligent adjustment, the energy-saving management program in the edge server needs to automatically turn on or control the adjustment device according to the change of temperature and humidity. The energy-saving management program in the edge server can first subscribe to the edge gateway with the theme of temperature and humidity. After the sensor device in the factory periodically collects the temperature and humidity data, it publishes relevant messages to the edge gateway with the theme of temperature and humidity. Then the edge gateway pushes this message to the energy saving management program in the edge server, and then realizes the automatic adjustment function.

(3) Communication between device and cloud server: A variety of production management applications are running on the factory cloud platform, which realizes data collection, process monitoring, industrial device management, quality management, production

scheduling, and data statistical analysis for the entire production process, so as to realize the informatization, intelligence and flexibility of the smart manufacturing management. In order to realize the communication between device and cloud server, you can use OPC UA protocol to deploy OPC UA server on device and deploy client on cloud server, so that cloud server can read real-time production data on device and send it control instruction. Or the cloud server first subscribes to the device for data, and when the data is ready, the device sends the data to the cloud server, and the cloud server sends instructions or data to the device.

4. The Factory External Network

The factory external network is designed to support various activities in the entire life cycle of the industry and is used to connect the upstream and downstream of the enterprise, the network between the enterprise and the product, and the enterprise and the user.

4.1. Situation

Due to the different levels of informatization development in different industries and fields of industry, the breadth and depth of the development and utilization of industrialized data and information are not the same, so there is an uneven network construction and development outside the factory, and some industrial enterprises only apply for ordinary Internet access. There are still islands of information between different areas of some industrial enterprises.

4.2. Development Trend

With the development of industrial networking and intelligence, the systems and applications in the factory are gradually expanding outward, and the industrial Internet services outside the factory are showing a trend of generalization, refinement and flexibility.

Network services outside the factory are universal. The traditional network outside the factory mainly provides the communication of commercial information, and the information systems of the enterprise are also deployed on the network inside the factory. The network outside the factory has few connection objects and single service. With the development of cloud platform technology, some enterprise information systems (such as ERP, CRM, etc.) are being externalized, and more and more IT software is also based on the Internet to provide services on the cloud. With the development of the remote service business of industrial products and device, the remote monitoring, maintenance, management, and optimization of

massive device will be carried out based on the network outside the factory in the future.

Refined network services outside the factory. The factory external network will realize the ubiquitous interconnection of the entire industrial chain and value chain. The complex and diverse connection scenarios promote the refined development of services. On the one hand, the connection demand of massive device has promoted the construction of mobile networks outside the factory and the rapid development of wide-coverage services; on the other hand, the shift in enterprise Internet demand to cloud demand has promoted the refinement of private line services. Provide segmented services for different scenarios such as enterprise Internet access, business system cloud access, public cloud and private cloud interoperability.

Flexible network services outside the factory. The development of network virtualization and softwareization has improved the flexibility of network services, so that the network outside the factory will be able to quickly open services and adjust services according to enterprise requirements; the application of a large number of mobile communication network technologies has improved the convenience and convenience of network access. The speed of deployment provides a more flexible way for enterprises to achieve extensive interconnection.

4.3. Enterprise Dedicated Line

The wide-area Internet business requirements of industrial entities mainly include the following aspects:

The Internet access requirements of industrial entities, the interconnection and isolation requirements between industrial entities across regions, the interconnection requirements of industrial networks and hybrid clouds, and the differentiated requirements (QoS, security/protection, etc.) of the industrial Internet for wide-area bearer networks.

At present, to meet the above requirements, the widely used carrier private line services mainly include: MPLS VPN dedicated line, and OTN-based optical network dedicated line.

MPLS VPN virtual private network builds enterprise virtual private network on the public MPLS network, to meet the needs of safe, fast and reliable industrialized communication between branches in different cities (international and domestic), and can support multimedia services that require high-quality and high reliability, such as office, data, voice, and images.

The MPLS VPN dedicated line is based on IP and high-speed label forwarding technology. Through the setting of QoS bits, the distinction of service levels and quality service guarantee can be realized.

The intelligent optical network based on OTN (Optical Transport Network) is an ideal solution for large-particle broadband service transmission. If the main dispatching particle of the external private network of an enterprise reaches the Gb/s level, the OTN technology can be considered as a priority for network construction.

With the increase in enterprise network application requirements, large enterprises also have large-particle circuit scheduling requirements. The introduction of OTN technology can realize the flexibility of large-particle circuit scheduling. Compared with MPLS VPN, OTN technology can realize an end-to-end physical private network, which is more attractive for specific enterprises that require large bandwidth (above Gbps) and require higher data and service reliability and security.

In addition, emerging technologies such as SD-WAN and CloudVPN can complement existing technologies, integrate various dedicated line resources, and open the call platform through a unified capability to form a transparent, integrated, and shielded part of the technical complexity for users. The factory's extranet solution can more economically meet the rapidly changing needs of enterprises for private line services.

(1) The CloudVPN cloud dedicated line is new generation enterprise private line network solution redefines enterprise interconnection centered on cloud services, simplifying business deployment to the greatest extent. CloudVPN can reduce the time of opening and adjusting VPNs traditionally on a weekly or monthly basis to the minute level, thereby providing convenient and flexible business options and realizing enterprise interconnection on demand.

The CloudVPN cloud private line solution includes the basic network equipment layer, management control layer, collaboration layer, and user interface. The operator's private line access capability is encapsulated as a simple OpenAPI interface, which supports developers' applications to quickly order, activate, and adjust on-demand services such as enterprise private line services and Internet access private lines by directly calling the interface. CloudVPN dedicated line network can be opened on demand in real time and elastically expanded: it supports real-time adjustment of dedicated line network bandwidth in industrial environments such as distance education, data intercommunication, and video conferencing.

SD-WAN is an extranet interconnection service formed by applying new SDN technology to WAN scenarios. This kind of service is used to connect enterprise networks, data centers, Internet applications and cloud services in a wide geographical area.

The technical features of SD-WAN include:

SD-WAN cloudizes the control capabilities of hardware networks through software, thereby supporting the opening of user-perceivable network capabilities;

The introduction of SD-WAN technology reduces the complexity and technical threshold of user-side WAN operation and maintenance;

SD-WAN technology has a high degree of self-service capabilities, and users can open, modify, and adjust private network interconnection parameters. The core concept of SD-WAN is the user's networking requirements and networking intentions, which can be translated and managed through the centralized control orchestrator provided by the communication service provider, shielding the complexity of the underlying network technology;

SD-WAN supports heterogeneous network (access can be done in many different ways including the Internet, other access methods such as OTN, other dedicated lines, etc.), the access equipment is generally on the user side, and the service differentiation point is on the user side; Support users to make flexible business adjustments through the self-service interface.

SD-WAN has the advantages of heterogeneous network and flexible operation, but because its virtual private network may be implemented based on Internet access, it may cause some hidden dangers in network attacks and data security, and end-to-end encryption needs to be implemented through encryption protocols.

4.4. Mobile Communication Network

With the development of the IIoT, the industrial production process is no longer limited to the factory, and gradually integrates industrial production with Internet business models, factories and products, and customers through the factory external network. In some production processes, the communication demand between the factory and the devices outside the factory has also increased significantly.

In these scenarios, mobile communication networks have been increasingly used in industrial production due to the characteristics of wide coverage, high speed, high network reliability and mature industrial chain, which greatly expands the connotation and extension of traditional industrial networks. Mobile

communication network has provided a good foundation for the development of IIoT.

3GPP's 5G defines three types of application scenarios: enhanced mobile broadband (eMBB), large-scale machine communication (mMTC), and high-reliability and low-latency communication (uRLLC). Among them, the eMBB scenario can support the gradual emergence of high-traffic services on IIoT, such as virtual factories and high-definition video remote maintenance. Large-scale machine communication scenarios are mainly aimed at massive field device communications.

The 5G network is a network that separates control and forwarding. The forwarding plane focuses more on the efficient routing and forwarding of business data. It has the characteristics of simplicity, stability and high performance to meet the forwarding needs of massive mobile traffic in the future. The control plane uses a logically centralized approach to achieve unified policy control, ensure flexible traffic scheduling and connection management. The centralized control plane realizes the programmable control of the forwarding plane through the mobile flow control interface.

The 5G core network supports various services with low latency, large capacity, and high speed. The core network forwarding plane further simplifies the sinking, and at the same time moves the business storage and computing capabilities from the network center down to the network edge to support high traffic and low time delay business requirements, and realize flexible and balanced traffic load scheduling function.

Main features and advantages:

The 5G network is a new type of network based on the separation of control and forwarding. It improves the overall access performance of the access network in complex 5G-oriented scenarios, simplifies the core network structure, provides flexible and efficient control forwarding functions, supports high intelligence operation, opens network capabilities, and improves the overall service level of the entire network.

The separation of the control plane and the forwarding plane makes the network architecture flatter, and the gateway device can be deployed in a distributed manner, thereby effectively reducing the service transmission delay.

Diversified business scenarios have diverse performance requirements and functional requirements for 5G networks. The 5G network has the ability to adapt to business scenarios, and provides appropriate

network control functions and performance guarantees for each 5G business scenario to achieve the goal of on-demand networking.

Applicable scene: 5G provides a more reliable, more open, and on-demand network for IIoT. The 5G network will better support the large-traffic services that are gradually emerging in the industrial Internet, such as virtual factories and high-definition video remote maintenance. The 5G network also supports a large number of equipment monitoring inside and outside the factory, such as remote monitoring and control of various device, remote control of wireless video surveillance, remote monitoring and reporting of environmental parameters and control machinery data, to meet the needs of the IIoT applications.

5. Information Model

Information model is a method used to define information representation, standardize data generated in industrial production, and facilitate communication between different devices and different applications. The information model should clarify three levels of content: (1) define which objects and the data contained in the objects; (2) how to organize these objects and data; (3) how to define the data format. The information of each device in the digital factory includes various parameters of the device itself, runtime data and data composition of the components in the device. This information is the object to be modeled.

The device information model can be divided into: static attribute set, dynamic attribute set and component assembly set. The data in a device is defined by attributes, and the collection of all information data contained in the device is called its attribute set. In the information model, information data is divided into static and dynamic. Static information represents information data that does not change or changes slowly after definition. In the device, it is mainly manifested as asset identification, order data, etc., such as material coding, processing device number, etc.; and dynamic information represents data that is generated, disappeared or changed in real time with the production process, generally device status data, part production process record data, such as working status, part processing size, logistics information, start and completion time and many more. According to the static and dynamic nature of information data, attributes are divided into static attributes and process attributes. Static attributes form a static attribute set, and process attributes form a process attribute set.

Each attribute set contains attribute data of several information objects. Information objects are described by attributes, and attributes are composed of attribute elements. This defines the

hierarchical structure of the information model as shown in Figure 6. The elements of information model are explained from small to large as follows in Figure 6.

Attribute elements: the basic elements that make up attributes, the basic units of attributes, such as attribute identification, name, data type, etc.

Attribute: the data describing the nature and characteristics of an object. Each attribute consists of multiple attribute elements, but not every attribute contains all attribute elements.

Information object: A body of information in the factory domain that describes a general, real, or abstract entity that can be conceptualized as a whole. Examples of information objects are the spindle of a machine tool, the processing route of a certain part, and the receipt of a certain material. The information object completes its digital definition and digital description through its attributes.

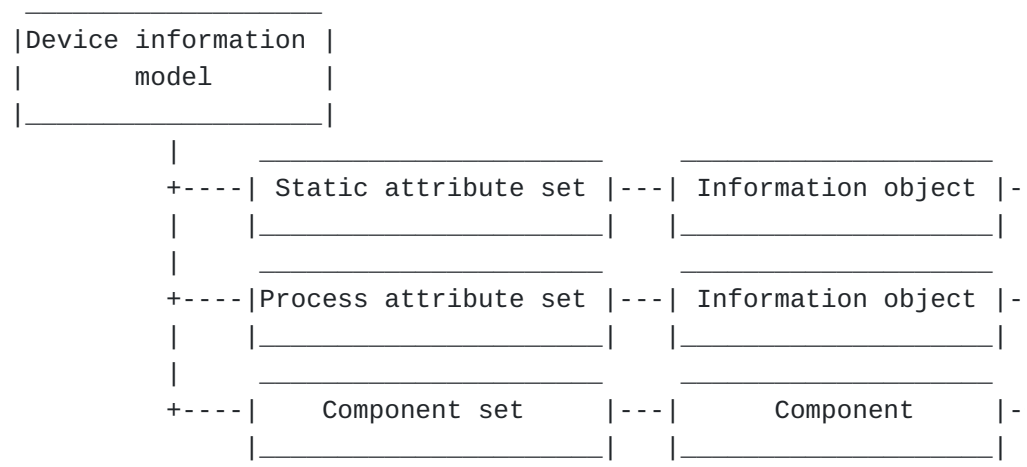

Figure 6: Information Model

Attribute set: A collection of a series of attributes. The attribute set can be composed of sub-attribute sets or the attributes of several information objects. According to the static and dynamic nature of information, the attribute set is divided into static attribute set and process attribute set.

Component: a physical object or logical object, which is a physical or logical part of the upper-level object, and its characteristics are described by the attribute set. Components can be nested, components can have their own subcomponents, and all subcomponents of the same object form a component set.

The device information model is an expandable tree structure that allows nesting between attribute sets and components. In the above definition, the attribute set and the component set are abstract structural elements that constitute the description of the factory information model. They are not a mapping of an actual object and do not contain actual content. They are only used for the framework and level of the organization model.

The device information model defined above is only an abstract framework. When modeling the information in the actual device and developing functions based on the information model, the actual device and function need to be based on the category and semantics of the frame. Various information model elements are filled to form an information model object with practical meaning. This process is called the instantiation of the information model. When the information model is implemented, it needs to be based on the specific description method and communication mechanism to realize the organization and storage of the instantiated information model. This section provides an information model implementation scheme based on the OPC UA protocol, as shown in Figure 7.

According to various information in the actual device, use the device information model to model, and use the OPC UA model generator to generate the corresponding XML file according to the established information model, and put it in the process model of the OPC UA server. The process model can obtain real-time data of the physical device through the data access module, save and update the value of the corresponding attribute in the information model.

The information model can be displayed through the address space of the OPC UA server, and the OPC UA client accesses the address space of the server to obtain the data and information defined by the information model. When the OPC UA client accesses or modifies the attribute information defined in the information model to the server, the UA service will access or modify the corresponding attribute information in the process model and return the result to the OPC UA client.

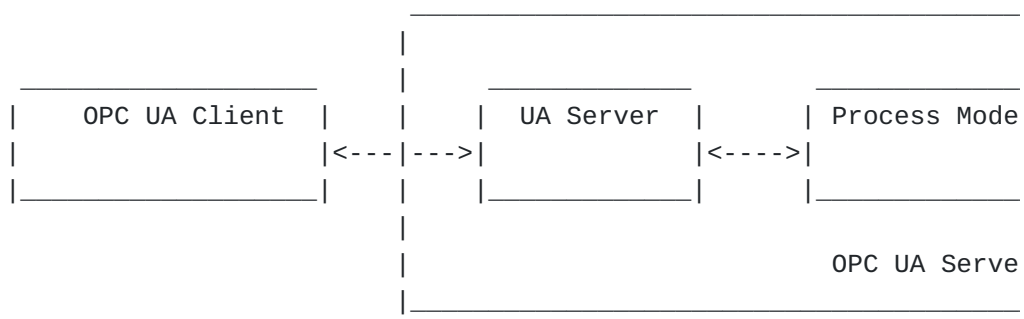

Figure 7: Information model realization scheme based on OPC UA protocol

6. Security Challenges and Recommendations

With the rapid development of sensor networks, cloud computing, artificial intelligence, and 5g technologies, the number of network devices in the future will rise sharply, and the corresponding market scale will also become larger, which will also cause corresponding security problems. Information leakage, virus proliferation, and even the destruction of public infrastructure, such as the impact of the national grid, communication equipment, servers, etc., before that, the security of IIoT has not attracted much attention, and the leakage of data collected by medical device has aroused widespread discussion in today's Internet era. People are becoming more aware of the importance of data security. With the recent extensive national-level management and control, more attention has been paid to the security of IIoT. It has also received attention from relevant agencies and enterprises in various countries. Regardless of life or technology, IIoT security will become a problem that must be solved for future development.

The current IIoT architecture is roughly based on the classic three-tier model, which is essentially logically divided into: sensing, transport, and application.

6.1. Sensing Security

The sensing layer is to realize the sense and collection of data in the physical world, use sensors, cameras, RFID and other smart devices to realize data collection, and realize the secure transmission of data through limited networks and wireless networks. Its key technologies are RFID technology and sensor networks. The IIoT sense front-end is responsible for real-time detection and collection of data, and uploads it to the cloud data center for processing through the transmission network, while the presenter of the sense terminal is vulnerable to various security issues such as virus intrusion, information leakage, tampering, etc. Therefore, for weak terminals with limited cost and performance, two-way

authentication, encrypted transmission, and remote upgrade capabilities should be met. Terminals with strong resource performance should meet stronger security capabilities, such as security certificate management, antivirus, and intrusion detection. For smart factory application scenarios, there are low latency requirements and fast response to services. Therefore, it is necessary to design efficient and lightweight security algorithms to deal with security threats, such as PRESENT block ciphers [PRESENT], DES lightweight ciphers, KATAN/KTANTAN lightweight ciphers [KATAN], and LBlock [Lblock] have all provided Different solutions.

6.2. Transport Layer Security

Consistent with the security requirements of the sensing layer, the task implemented by the transport layer is to re-responsibly transfer the data of the sensing layer to the application layer for processing. It also requires the transmission network and communication protocol, and the network node has been attacked by the network (such as man-in-the-middle, and counterfeit attacks), causing node paralysis, which may further cause the leakage of communication keys and affect the security of the entire network. At the same time, a large number of nodes and data can easily cause network congestion and cause denial of service attacks, which will also affect the transmission layer. Security puts forward higher requirements. Due to the need for communication between networks with different architectures in the transport layer, it is necessary to face security issues such as cross-network authentication, key negotiation, data confidentiality and integrity protection of heterogeneous networks. There are some confrontational security technologies, homomorphic encryption technology, secure multi-party technology, and anonymization technology.

6.3. Appliacation Layer Security

The application layer is the logical highest layer of the architecture. The tasks implemented in it are very many and complex, and the number of application categories is also different, such as monitoring services, smart grid, industrial control, green agriculture, etc. The application layer needs to process effectively the data from transport layer. Taking into account the huge data and network node calculations of IIoT, huge storage and computing capabilities are required, and the use of cloud computing technology can carry these tasks at a significant cost-effectiveness. The current architecture is based on cloud computing, and cloud platforms realize applications. The processing response of business logic emphasizes the combination of IIoT and cloud computing. Therefore, there are also cloud computing and cloud platform security issues, including platform data storage, exchange, processing and other security issues, as well as data security and

interaction issues arising from the integration of different platforms. At present, the cloud platform uses WAF, firewall, and HIDS. To a certain extent, it has played a role in data protection, but further security technical support is still needed. The distributed structure based on edge computing can share the computing pressure, decrease response time, and to a certain extent limit security risks to a certain area. Reduce the security risk of the core network, so the application of edge computing will be a good opportunity. The cloud intelligent platform can deal with huge data. It is easy to have many abnormal data and abnormal behaviors. It is not easy to detect and exclude. Security has a strong impact, and the use of various emerging technologies such as data mining, machine learning, AI, etc. to analyze data can further detect data anomalies and improve data security. At the application level, it is relevant in many large enterprises those applications all collect a large amount of private data, such as health status, purchase behavior, travel routes, group contact, value orientation, etc., which also generate data privacy protection problems. Therefore, scholars have proposed homomorphic encryption algorithms. Blockchain also provides a new solution for this. For example, blockchain can realize an anonymous sharing method of IIoT devices [permissioned-blockchains]. Blockchain is widely used in the field of IIoT, which can effectively improve the lack of the traditional centralized data storage mode of IIoT. The full nodes of the blockchain network record complete data information to jointly maintain the data security of the IIoT device and reduce the traditional cost of maintaining a centralized database for the application of IIoT. The tamper-proof modification of the blockchain, the timing guarantee the security and traceability of the data of the entire network node, the use of block chain technology can ensure data privacy and security.

6.4. IIoT Security Solutions

Combining the security issues of the IIoT architecture, summarize the existing security issues and corresponding solutions, mainly including device protection, device identification, authentication mechanisms, secure communication mechanisms, data privacy protection, anomaly detection and intrusion detection security status, the corresponding solutions are as follows As shown in the Figure 8.

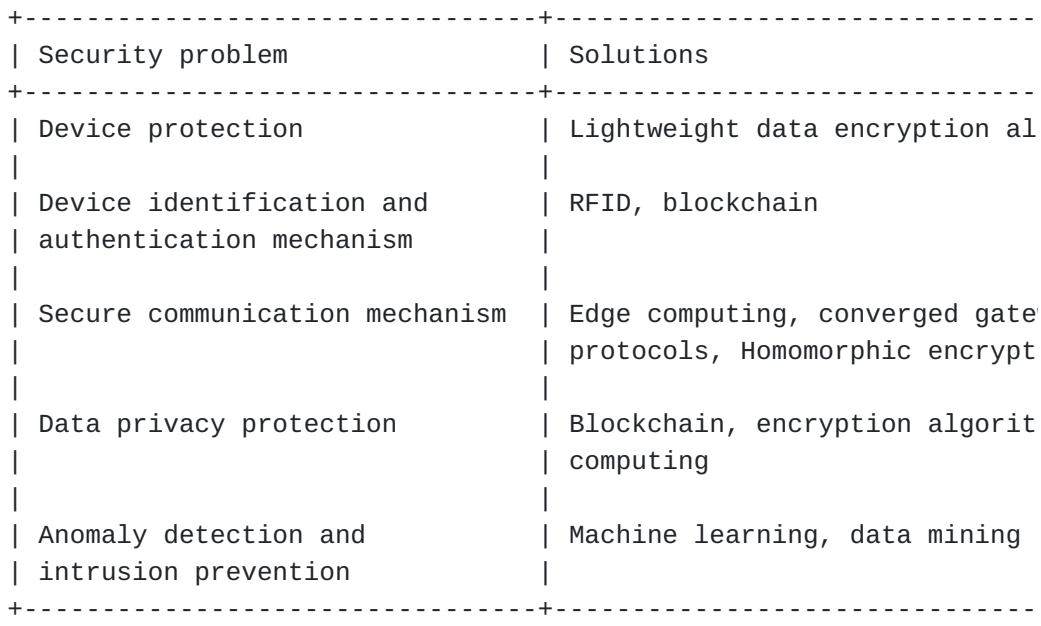

Figure 8: Security problems and solutions

7. Informative References

[smart-factory] Chen, B., Wan, J., and S. Lei, "Smart factory of industry 4.0: key technologies, application case, and challenges", 2017.

[iiot-5g] Cheng, J., Li, D., and W. Chen, "Industrial IoT in 5G environment towards smart manufacturing", 2018.

[tsn] DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking, detnet., "https://tools.ietf.org/html/draft-ietf-detnet-ip-over-tsn-03", 2020.

[I-D.ietf-6lowpan-usecases] Design and Application Spaces for 6LoWPANs, ipv6., "https://tools.ietf.org/html/draft-ietf-6lowpan-usecases-10", 2012.

[edge-computing] Mach, P. and Z. Becvar, "Mobile edge computing: a survey on architecture and computation offloading", 2017.

[I-D.ietf-core-coap-pubsub] Publish-Subscribe Broker for the Constrained Application Protocol, pubsub., "https://tools.ietf.org/html/draft-ietf-core-coap-pubsub-09", 2020.

[PRESENT] Bogdanov, A., Knudsen, L., and G. Leander, "PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems", 2007.

[KATAN] Canniere, C. and O. Dunkelman, "KATAN and KTANTAN -- A Family of Small and Efficient Hardware-Oriented Block Ciphers", 2009.

[Lblock] Wu, W. and Lei. Zhang, "Lblock: a lightweight block cipher", 2011.

[permissioned-blockchains] Hardjono, T., "Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains", 2016.

Authors' Addresses

Chaowei Tang
Chongqing University
No.174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: cwtang@cqu.edu.cn

Haotian Wen
Chongqing University
No.174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: wenhaotianrye@foxmail.com

Shuai Ruan
Chongqing University
No.174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: rs@cqu.edu.cn

Baojin Huang
Chongqing University
No.174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: baojin-huang@foxmail.com

Xinxin Feng
Chongqing University
No.174 Shazheng Street, Shapingba District
Chongqing
400044
China

Email: xxfeng@cqu.edu.cn