Imou Cloud Security White Paper

Hangzhou HuaCheng Network Technology Co., Ltd.

Legal Notice

Copyright Statement

Without the prior written permission of Hangzhou HuaCheng Network Technology Co., Ltd. (hereinafter referred to as "HuaCheng"), no one may copy, transmit, distribute or store any content in this document in any form.

The products described in this document may contain software copyrighted by HuaCheng and other third parties. No one shall copy, distribute, modify, extract, decompile, disassemble, decrypt, reverse engineer, lease, transfer, sublicense or otherwise infringe the copyright of the software in any form except with the permission of the relevant owner.

Trademark Statement

- IMOU、乐橙、IMOU 乐橙 are trademarks or registered trademarks of Hangzhou HuaCheng Network Technology Co., Ltd.
- Other trademarks or company names that may be mentioned in this document are owned by their respective owners.

Responsibility Statement

- To the extent permitted by applicable laws, in no case will the company compensate for any special, attached, indirect and secondary damages caused by the relevant contents and products described in this document, nor for any loss of profits, data, goodwill, documents or expected savings.
- The products described in this document are provided "in accordance with the status quo". Unless required by applicable laws, the company does not provide any express or implied warranties for all contents in the document.

Export Control Compliance Statement

HuaCheng complies with applicable export control laws and regulations and implements requirements related to the export, re-export and transfer of hardware, software, and technology. With regard to the products described in this manual, kindly fully understand and strictly abide the applicable domestic and foreign export control laws and regulations.

About This Document

- The products, services or features you purchase shall be subjected to the company's commercial contracts and terms. All or part of the products, services or features described in this document

may not be within the scope of your purchase or use.

- If the operation is not carried out according to the instructions in this document, any loss caused thereby shall be borne by the user.
- If the obtained PDF document cannot be opened, please upgrade the document reader software being used to its latest version or use other mainstream reading tools.
- The company reserves the right to modify any information in this document at any time, and the modified content will be added in the new version of this document without notice.
- This document may contain technical inaccuracies, inconsistencies with product functions and operations, or typographical errors, subject to the company's final interpretation.

Foreword

Overview

The cloud security white paper aims to present the results of HuaCheng's research and practice of cloud security technology, so that users can understand the security capabilities of Imou Cloud more clearly.

Revision History

No.	Version	Revised Contents	Release Date
1	V1.0.0	First Release	March,2020

Table of Contents

1 Security-Cloud Trends

With the development of 5G and big data technology, "Internet of Everything" has become the development trend of future products, and the traditional security industry has gradually transformed into intelligent and digital. As an important infrastructure in the digital era, cloud computing, with its high efficiency, scalability, and convenience, provides the necessary conditions for the intelligent and digital transformation of the security industry.

Imou Cloud is an open, shared, and secure video cloud service platform that provides users with video-oriented public cloud, private cloud, and hybrid cloud services. Taking Imou cloud as the core, it aims to build a business ecosystem of “Three in One” with video intelligent hardware, video cloud, and intelligent technology, through the access to network cameras, smart door locks, robots, wireless detection sensors and other smart devices, build a smart, secure and rich IoT ecosystem for users.

Imou Cloud always adheres to the concept of "compliance, openness and transparency", upholds the original intention of providing users with efficient, secure and trusted video cloud services, actively faces the network security challenges in the process of intelligentization and digitalization, and continues to build security protection capabilities to ensure data security and privacy compliance on the cloud platform.

2 Cloud Security Threats

As a cloud service platform for video, Imou Cloud faces all kinds of network security threats like all cloud computing services. The 12 most serious cloud security issues raised by the Cloud Security Alliance (CSA) are exactly what we have been committed to preventing and solving, including:

- Data Breach

When a large amount of data, especially video-sensitive data is stored in the cloud, data breach may occur due to intrusion by an attacker or due to improper internal configuration management and other factors.

- Weak identity credentials and insufficient access management

The use of weak passwords, weak identity authentication mechanisms, incorrect key management and certificate management, and failure to properly configure the corresponding access control management mechanism may result in unauthorized data access and functional operations.

- Insecure API

The cloud service platform provides users with corresponding APIs to interact with cloud services. Insecure API design and implementation may lead malicious users to bypass the access control mechanism and illegally access data.

- System and application vulnerabilities

Cloud services are essentially a set of applications, the operating systems, components they rely on and vulnerabilities in the service itself may all be exploited, leaving the entire system facing significant security risks.

- Account Hijack

The identity certificate is stolen, which allows illegal personnel to access the key content of the cloud service, resulting in the destruction of the confidentiality, integrity, and availability of the service.

- Internal Threats

Threats inside the cloud service platform may come from malicious personnel inside. When they have access control rights and initiate malicious retaliation, they may cause devastating damage inside the enterprise.

- Advanced Persistent Threats（APT）

Advanced persistent threats infiltrate into cloud services, establish a foothold within systems, and steal data from them.

- Data Loss

Data stored in the cloud may cause accidental data loss due to malicious attacks and non-malicious human operations, force majeure factors, physical disasters, etc.

- Lack of due diligence

Before deciding to introduce cloud service providers and cloud computing technologies, detailed due diligence and technical route planning are required to clarify the relevant responsibilities of cloud service providers.

- Abuse and malicious use of cloud services

Cloud computing services provide users with rich and efficient computing storage capabilities. When these capabilities are used maliciously, they will cause damage to other normal business systems.

- Denial of Service

Denial of service attacks (DoS) consume large amounts of various resources of cloud services, resulting in slow service response and insufficient resources, which prevents legitimate users from using cloud services normally.

- Sharing technology vulnerabilities

Cloud service providers extend their services by sharing infrastructure, platforms, or applications. The underlying components deployed may not provide isolation performance for multi-tenant or multi-user applications, resulting in shared technical vulnerabilities and exploited by malicious attackers.

In response to the above problems, Imou Cloud adopted a threat modeling method based on the STRIDE model, continuously iteratively identified and evaluated cloud security risks, and formulated mitigation measures in a targeted manner. Through deep digging of security flaws, we have continuously improved cloud security guarantee measures, and at the same time, we have built an Imou Cloud security system to ensure security and meet compliance requirements from various aspects such as organization, process, and technology.

3 Cloud Security System

3.1 Sharing Security Responsibilities

Based on the cloud computing platform of the cloud service provider, Imou Cloud has built SaaS and open platform cloud services, and its security responsibility is shared by the three parties:

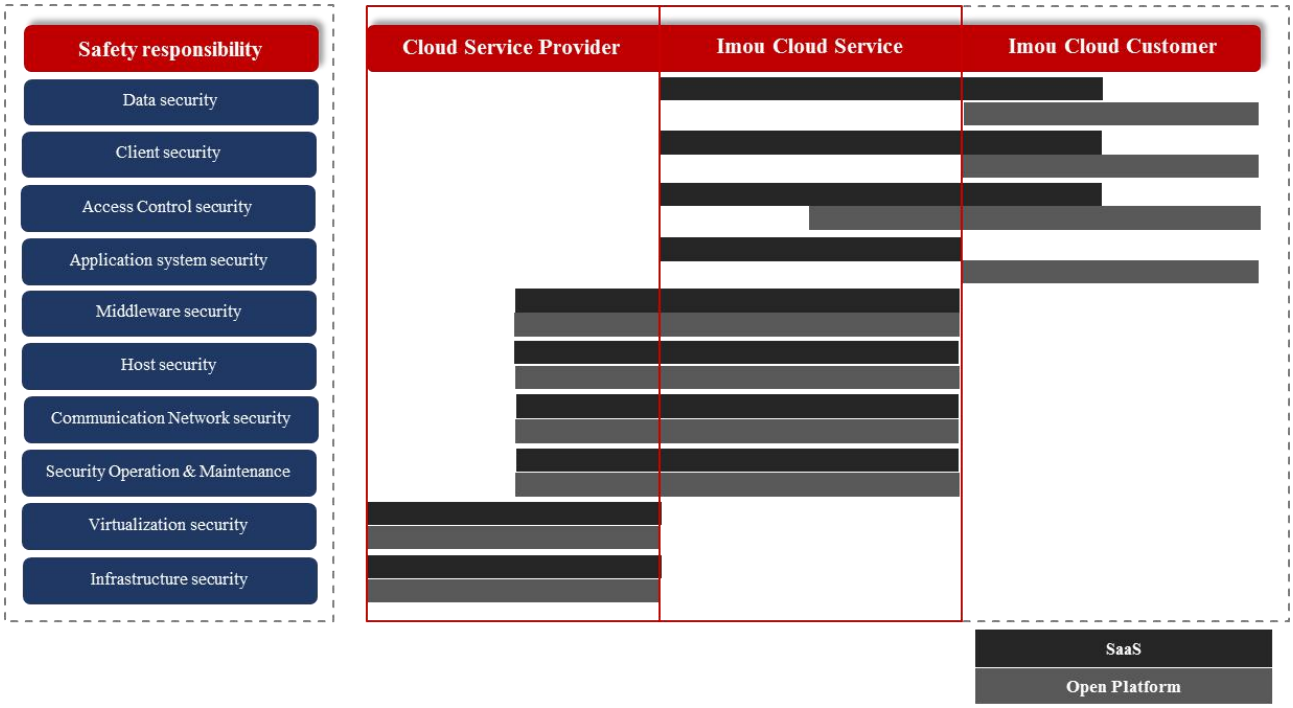


Figure 3-1 Cloud Security Responsibility Sharing Model

By choosing world famous cloud computing platforms such as Amazon Cloud and Alibaba Cloud, Imou Cloud inherits the cloud service provider's infrastructure security and virtualization security capabilities, as well as some operation and maintenance security, network communication security, host security and middleware security capabilities.

The professional operation and maintenance team of Imou Cloud is responsible for the secure operation and maintenance of Imou Cloud service, and combined with the construction of security standardization, together guarantee network communication security, host security and middleware security.

When providing open platform services, Imou Cloud only provides technical support and is responsible for the security of the open platform services (including access control security for users). For these projects develop and construct based on cloud platform capability, users are the one to take responsibility for these projects security, and security measures need to be taken to ensure project application security, access control security, terminal security and data security.

When providing SaaS services (including Imou APP), Imou Cloud will be responsible for building

application security, access control security, terminal security and data security capabilities. Users need to manage their own access control credentials, terminal access equipment and local personal data security, in order to better use the security capabilities of Imou Cloud.

3.2 Security Organization and Personnel

3.2.1 Security Framework

The company has established a security organizational structure and defined the security responsibilities of each organizational team.

The Cyber Security Committee is a cyber-security leadership decision-making body under the leadership of the board of directors, which implements comprehensive leadership, management and supervision of the company's overall cyber security work.

The Cyber Security Research Institute is responsible for the research and practice of security technology and emergency handling of security issues. It consists of 3 teams: security design team, security testing and incident response team, security solution design and development team. They lead the security group of each product line to jointly guarantee product / cloud security.

The Data Protection Officer (DPO) has extensive practical experience in the field of data protection and cyber security, and is responsible for data security matters within the group and related subsidiaries. And DPO is independent of each product line and reports directly to the company's cyber security committee.

The Security Compliance Team continues to benchmark industry-leading laws and standards, and uses proactive compliance and continuous audit strategies to improve the compliance and security capabilities of company-related products (including Imou Cloud).

The Cloud Security Group is responsible for implementing the company's cloud security strategy, responsible for the research, design and promotion of cloud security baselines, security solutions and key security technologies, and participating in security reviews of major cloud projects. Promote and support the security construction of the cloud product line.

3.2.2 Security Awareness Training

Before employees formally take up positions, we will carry out targeted security training activities according to different positions, including training on security coding, security testing, vulnerability management, and security development processes. Employees may formally take up positions after completing training and passing relevant examinations.

3.3 Imou Cloud Security Architecture

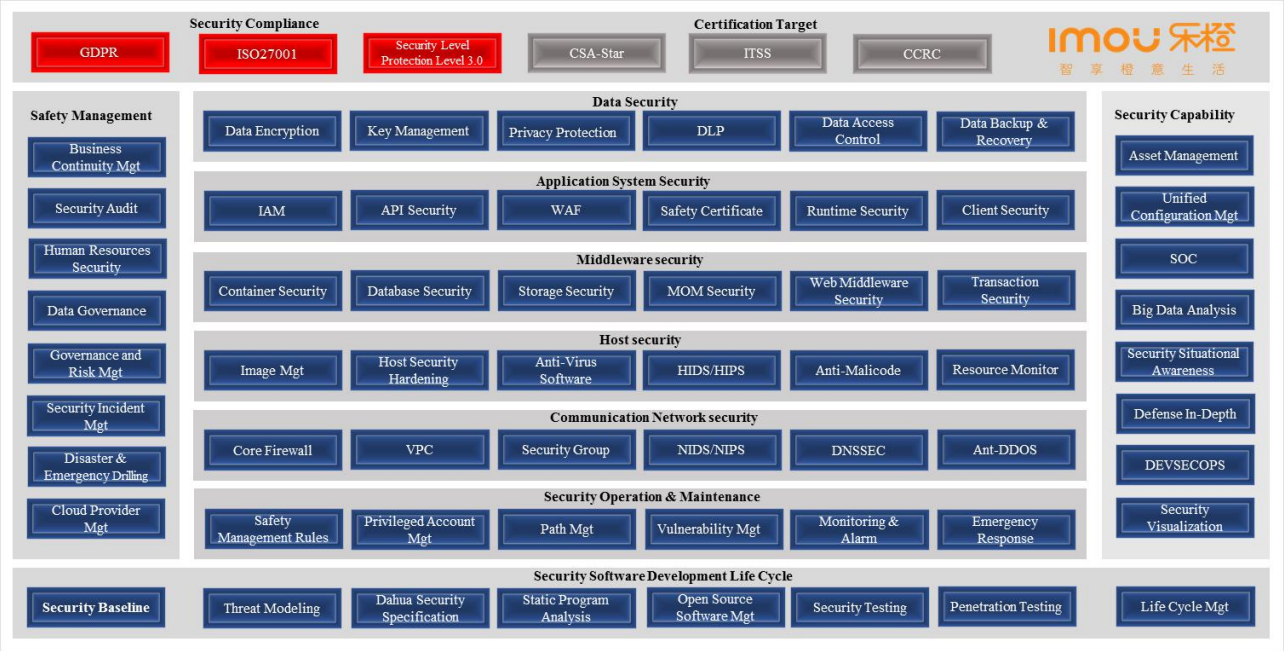


Figure 3-2 Cloud Security Architecture

According to the three dimensions of “Basic Security Unified Capability, Business Security Assurance Capability, and Global Security Support Capability”, Imou Cloud Security Framework integrates and guides the security system developing from sSDLC to sSDLC + DevSecOps. Take the CSA cloud model, security control and compliance mapping as the target, and the CCM cloud control matrix as the benchmark, combined with regulation and company business needs, starting from forward target guidance and reverse problem analysis to improve, integrate, and link the entire field of security ability to build a trusted, reliable, controllable, secure and visible Imoue Cloud security architecture.

4 Cloud Security Defense Capabilities

4.1 Security Concept

Imou Cloud is not satisfied with any single security protection software / hardware or control measures, but makes an overall security solution to the system from multiple levels and multiple dimensions, such as system architecture, network architecture, access control, permission management, etc. Achieve the purpose of "can't come in", "can't take away", "cannot understand", "can't change", "can't leave".

- Risk management. Good architecture design can prevent known and unknown vulnerabilities. Perfect security control measures can reduce the security risk to an acceptable range or even eliminate the security risk.
- Attack surface minimization. Reduce the number of exposed attack surfaces as much as possible. The attack surface includes code, interfaces, services, and protocols that provide services to all users.
- Defense in depth. Do not rely on a single security mechanism, but establish a multiple mechanisms, complementary support to achieve a progressive, interlocking defensive effect.

4.2 Cloud Platform Security

4.2.1 Infrastructure Security

Imou Cloud cooperates with well-known cloud service providers such as Alibaba Cloud, Huawei Cloud, Amazon Cloud, and Microsoft Cloud. Relying on the basic services provided by cloud service providers to build cloud products that meet user needs. The security of Imou Cloud's infrastructure is guaranteed by the cloud service provider. Imou Cloud will occasionally audit the security qualifications and security reports of each cloud service provider to ensure the security and reliability of the infrastructure.

4.2.2 Network Security

Imou Cloud uses a proprietary network VPC network deployment method instead of the classic network. The private network VPC can be 100% tenant isolation and 100% custom cloud private network environment, which can easily realize multiple security protection based on the host side and the network side. The VPC peer-to-peer connection function ensures the security of data

transmission between multiple regional nodes in Imou Cloud. Imou Cloud can defend against a variety of network attacks such as ARP attacks and MAC spoofing. Based on the cloud service provider's traffic cleaning capabilities, Imou Cloud can also better defend against DDOS attacks.

4.2.3 Host Security

Imou Cloud adopts the official security image of the cloud service provider, regularly updates the system patches, and periodically updates the host key. According to the official standards of Center for Internet Security (international organization) and industry best practices, the cloud server system is hardened. Imou Cloud host has realized a number of host security measures such as minimizing open ports, minimizing installation services, isolating management ports from business ports, and automatic warning of security events. Important business hosts have deployed anti-virus software, which will monitor the security status of the host in real time, and periodically take full-disk virus and Trojan scans of the host.

4.2.4 Middleware Security

In order to ensure the operation effect and user experience of the application, Imou Cloud integrates a variety of WEB middleware. Imou Cloud takes into account the balance between security and performance when selecting middleware. Even the performance is excellent, the middleware that does not meet the security control requirements will not be adopted. The middleware is upgraded to a newer version in a timely manner, and combined with CIS standards and industry best practices to strengthen the middleware, enable security functions, delete default pages, and disable unused components.

4.2.5 Database Security

Imou Cloud uses the cloud service provider RDS cloud database, and hardens the cloud database according to best practices. Cloud database login credentials minimize the authority and ensure the independence of credentials for different projects. All databases have implemented strict access control policies, and only the required hosts can access the database, requiring that all databases are not exposed on the public network. Imou Cloud regularly backs up the database and conducts regular recovery drills.

4.2.6 Application Security

Imou Cloud implements security enhancement measures in application architecture design and application deployment. Imou Cloud application complies with enterprise security standards during the development and testing process, and implements application security design and implementation from the dimensions of authentication, authorization, input verification, data

encryption, log auditing, and privacy compliance, and from code audit and virus Trojan detection , security scanning, penetration testing, risk assessment, compliance audit and other security activities to ensure the security and compliance of Imou Cloud application.

4.3 Security Standardization

4.3.1 Cloud Security Baseline

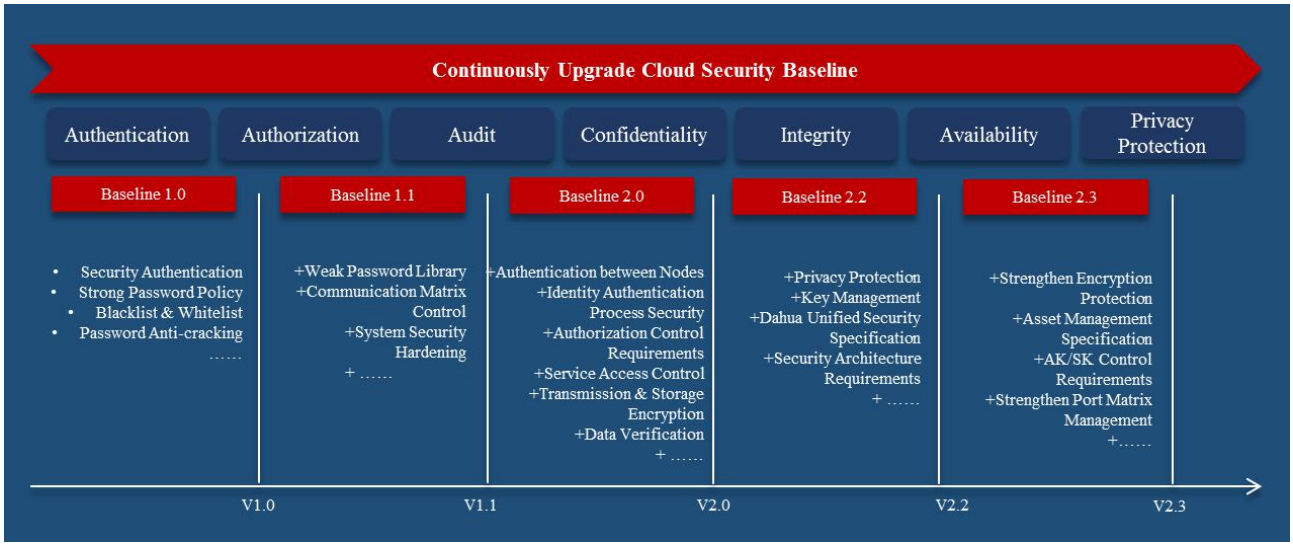


Figure 4-1 Cloud Security Baseline

Imou Cloud has independently implemented the "security baseline" for many years, adheres to the core principles of "Security by Design" and "Security by Default", and deeply cultivates cloud security technology to provide users with sufficient security guarantees.

The security baseline is based on and implements the design principles of security and privacy, constructs the "AAA + CIA + P" security element layout, and forms a systematic protection framework covering system security, application security, data security, network security, and privacy protection.

The layout of "AAA + CIA + P" security elements is as follows:

- AAA: Authentication, Authorization, Audit
- CIA： Confidentiality, Integrity, Availability
- P： Privacy Protection

4.3.2 APP Security Baseline

The APP mobile client is the key component of Imou Cloud and also the direct entrance for users to use Imou Cloud. Abiding by the core elements of “GBT35273-2020 Personal Information Security Specification for Information Security Technology”, GDPR, “Self-Assessment Guidelines for The Collection and Use of Personal Information By App Violations”, and “OWASP Mobile Application

Security Control and Design Principles TOP 10", we designed an App security baseline that meets the following major security objectives:

- Comply with laws and regulations
- Comply with industry security standards and specifications
- Protect user privacy and data security
- Sensitive information (video, images, and personal information) not be leaked during transmission and storage
- Prevent reverse client source code
- Prevent abuse of authority

4.3.3 Security Hardening Scheme

HuaCheng takes the CIS hardening standards, cloud service provider best practices, and industry experience as the source of demand. After analysis and refinement to form security hardening guidelines, including operating system hardening guidelines, middleware hardening guidelines, and database hardening guidelines. Promote and apply in various systems of Imou Cloud. Security hardening is guided by standard security concepts, reducing the attack surface of Imou Cloud and enhancing defense capabilities.

4.3.4 Key Technical Framework

ModSecurity is an open source cross-platform web application firewall (WAF) engine. ModSecurity focuses on HTTP traffic. When an HTTP request is sent, ModSecurity checks all parts of the request. If the request is malicious, it will be blocked and recorded.
OpenRASP is a security protection engine based on runtime application of self-protection (RASP) technology. OpenRASP runs the protection system inside each application, and has the characteristics of resisting unknown vulnerabilities, standardizing application coding standards, and low false alarm rate. Compared to ModSecurity's doorkeeper model, OpenRASP is a housekeeper model.
Combined with the characteristics of OpenRASP and ModSecurity, continue to optimize the protection rules and security strategies, and verify the effect by simulating external attacks to further ensure the protection effect.

4.3.5 Cryptographic Algorithm Specification

With reference to the international authoritative standards of BSI, NIST and FIPS, HuaCheng has formulated the enterprise standard "HuaCheng Cryptographic Algorithms Usage Specification". Each system of Imou Cloud followed the standard to correctly use the cryptographic algorithm, and only using the recommended Hash algorithm, symmetric encryption algorithm, asymmetric encryption algorithm, digital signature algorithm, key negotiation algorithm, etc.

4.3.6 Personal Data Classification and Grading Specification

Based on the National Personal Information Security Regulations and the GDPR Act, HuaCheng has determined the "Personal Data Classification and Grading Regulations" to classify personal data and clarify the protection requirements for different levels of personal data. No requirements for low-level personal data; access control and authority management are required for medium-level personal data; additional transmission encryption and storage encryption are required for high-level personal data; processing of severe-level personal data is prohibited in principle. In case of extremely special circumstances, it needs to be jointly reviewed by multiple departments and protected by the highest security measures.

4.4 Business Security

4.4.1 Authentication Security

Imou Cloud authentication mainly includes client authentication and device-side authentication:

- Client identity authentication can be divided into three authentication scenarios: before login, during login and after login:
    - Before login authentication: based on the AK and SK issued by the platform, to prevent malicious attacks on interfaces such as user registration and password recovery;
    - During login authentication: identity authentication with signature verification based on user name and user password;
    - After login authentication: identity authentication based on the user name and the token generated by the platform.
- Device-side identity authentication is to prevent illegal devices from accessing the platform. The platform issues different AK / SK for different devices.

Imou client identity authentication features:

- Use standard HTTPS encrypted channel YTERWAXZ for identity authentication;
- Digest authentication based on multiple factors can prevent replay attacks, tamper proof, and password leakage;
- Client-side does not store user password.

4.4.1.1 Password Policy

Password requirements in identity authentication:

1. User passwords allow 8-32 characters in length；

2. Password allows characters: any visible characters except the five characters """, "" ",", ",": "," ";

3. Password composition must contain at least two character types (character types include numbers, letters and special characters, letters are case sensitive)；

4. Weak password library. The client establishes a weak password library. If a weak password library is matched, the password cannot be used;
5. Repeated characters in the password cannot exceed 5 consecutive times；
6. The password cannot be the user-name itself or the user name in reverse order.

4.4.1.2 Account Risk Control System

Imou Cloud IAM combines login password (strong password), SMS verification code, biometric code and other MFA (multi-factor authentication), etc. to improve the authenticity, legality and security of user accounts.

4.4.2 P2P Security

Imou Cloud supports P2P technology. P2P technology provides users with remote and secure access to devices deployed in the local area network through the public network to achieve device point-to-point services, improve resource utilization and access efficiency, reduce cloud service operating costs, and promote IoT interconnection capabilities. However, the use of P2P technology to enhance user experience and promote the characteristics of the interconnection of IoT nodes has also brought great challenges to ensuring the security of the P2P service architecture system. The following describes the P2P security defense system in terms of P2P background and technical principles.

4.4.2.1 Background

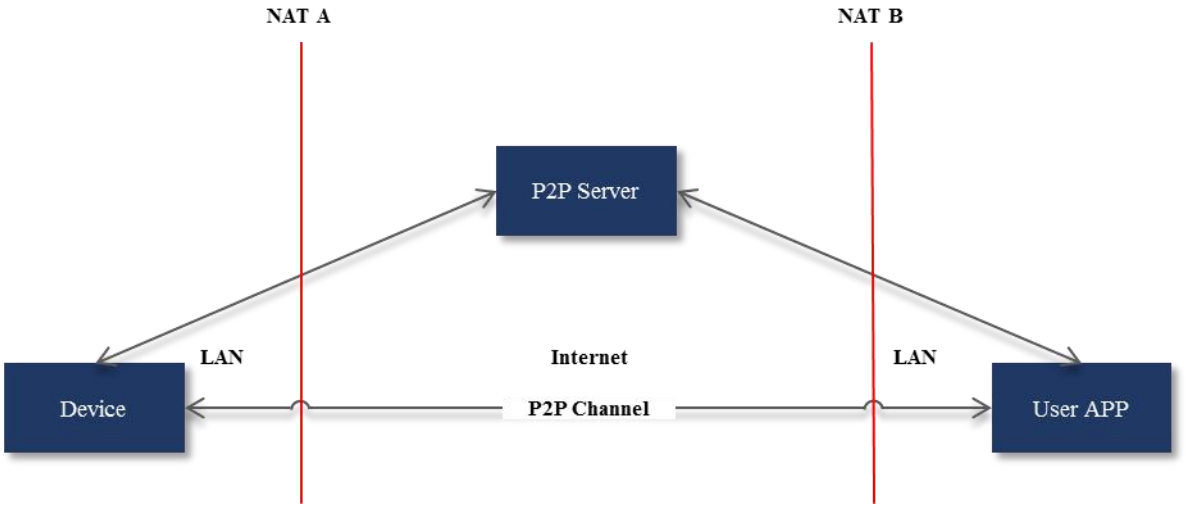


Figure 4-2 P2P Technology Principle

The P2P server uses UDP packet interaction to assist the NAT at both ends to achieve P2P (Point to Point) communication based on direct connection channels, the overall process is as follows:
1. Through the assistance of the P2P server, the device and the client obtain the public and private

network addresses of both parties and create a direct connection channel;
2. If the device and the client succeed in P2P communication through the direct connection channel, then transmit the code stream through the direct connection channel;
3. If the P2P communication between the device and the client fails through the directly connected channel, then the code stream is transmitted by forwarding.

4.4.2.2 Security Policy

P2P adopts digest authentication mode to ensure channel communication security. The P2P channel is equivalent to a transparent proxy transmission channel, and its security depends on the protocol of the application layer. In Imou Cloud, the media streams transmitted using the P2P channel have been encrypted and designed security control points in all links.

- Access control mechanism: The P2P cloud service extends the WSSE authentication mechanism to control access to devices and APP. WSSE uses HASH calculations such as time stamps, access credentials, and random numbers to achieve identity authentication while ensuring the non-replayability and confidentiality of messages.
- Relay point-to-point credential verification: P2P cloud service provides interactive security control and transfer capability. To avoid malicious attackers using this forwarding node to penetrate the NAT where the target device or APP is located, the Relay node has designed an identity credential verification mechanism to ensure P2P forwarding only legal users of the channel can realize data forwarding.
- DoS alarm notification: The P2P cloud service will monitor the service running status in real time. When the following (not limited to) abnormal conditions are found, the operation and maintenance personnel will be notified to ensure timely handling of service abnormalities: memory abnormalities, CPU abnormalities, and storage abnormalities , abnormal service, abnormal flow.
- Code fuzzification: in order to protect some protection logic mechanisms of APP from malicious attackers, we conducted code fuzzification on APP firmware to increase the cost of reverse attack.
- Data verification: The data interaction in the APP / device / P2P cloud service has strict data verification to avoid malicious attacks using illegal parameters to attack programs or services, and to achieve memory overflow, code injection and other attack modes.

4.4.3 Media Security

If the user purchases the Imou Cloud Storage Service, the alarm video generated by the Imou device will be stored on the Imou Cloud for users to view randomly. The video cloud storage service includes three processes: video upload, video storage and video download. Imou Cloud has corresponding security protection measures in the whole life cycle of video on the cloud.

- Video upload: Encrypt the content of the media stream and provide the transmission capability based on the HTTPS protocol;
- Video storage: Video data is encrypted and stored in cloud storage;
- Video download: The client must be authenticated before downloading the video.

4.4.4 Open Platform Security

Imou Cloud Open Platform is dedicated to providing perfect solutions for video applications with the "trinity" of video intelligent hardware, video cloud and video technology. Open and share video cloud capabilities to third-party partners, helping partners have their own cloud video capabilities at a faster speed and lower cost, and share the ecosystem of the IoT based on video applications.
The open platform adopts the design of microservice architecture as a whole, providing users with standard RESTFul API interfaces, and implementing various control measures such as restricting access frequency, authentication, authority verification, parameter verification, etc. to these interfaces. The open platform team will also conduct security audits on application information submitted by users.

4.4.5 Data Backup Security

- Multiple data centers back up: Overseas Imou Cloud adopts a high-availability strategy, designs multiple data centers based on a distributed architecture, and all business data storage areas are in three major data centers: America Center, Europe Center, and Asia-Pacific Center. Provide corresponding data services according to the user's location.
- Multi-copy redundant storage: The user's audio / video and image data is stored in the object storage provided by the cloud service provider in multi-copy mode and the database is professionally hardened and configured with professional firewall protection and blocking illegal access and malicious injection from attackers. Together with cloud service provider best practices, Imou Cloud provides guarantee for the secure compliance storage and access of user data in the region.

4.4.6 Business Continuity

In order to prevent cloud service provider business transformation or acquisition / merger, causing business failure, Imou Cloud implements a multi-cloud strategy and cooperates with multiple cloud service providers such as Alibaba Cloud, Huawei Cloud, Amazon Cloud, and Microsoft Cloud. Imou Cloud supports business migration on different clouds and has a complete technical reserve. Imou Cloud deploys cloud services at multiple nodes around the world to ensure a good user experience.

- Flexible architecture: Imou Cloud architecture supports the application / recovery of cloud assets based on business needs, thereby ensuring the stability and overall service performance of Imou Cloud.
- High-availability architecture: Imou Cloud implements a high-availability architecture by deploying multiple service hosts for main service modules, equipped with load balancing systems, and deploying multiple service nodes. A server downtime does not affect the normal use of business functions.

- Self-starting when service is abnormal: Imou Cloud service can be automatically start up again when it crashes abnormally to ensure availability.
- Monitoring alarm: Imou Cloud automatically monitors alarms for the availability of individual service modules and service APIs.
- Data backup: Imou Cloud made a regular backup strategy for the database.
- Emergency drill: Imou Cloud regularly conducts emergency recovery drills to ensure that when an exception occurs, it can promptly recover business and data according to the established process.
- Shared responsibility: Imou Cloud and cloud service providers clarify their respective responsibilities and obligations in ensuring business continuity through contract.

4.5 Secure Operation and Maintenance

Imou Cloud is responsible for daily maintenance work by a professional operation and maintenance team, and responsible for the deployment, expansion, modify and monitoring of new services. Operation and maintenance security is a crucial link in cloud security, which involves security control measures such as personnel management, account management, and network management. Based on the concepts of pre-identity identification, permission identification and behavior management, and post-event security audit, Imou Cloud has developed an operation and maintenance security system and operation specifications to conduct overall security management and control of operation and maintenance behaviors and processes.

4.5.1 Asset Management

The large number and fast change frequency are the salient features of assets on the cloud, and good asset management is a prerequisite for secure operation and maintenance. To this end, Imou Cloud has established an automated asset management system that can complete the collection of Imou Cloud assets in a short period of time.

4.5.2 Management Plane Security

Imou Cloud management plane includes cloud service provider interface and internal management system. The cloud service provider interface inherits the cloud service provider's security management capabilities and implements strict role and permission management and control. The internal system management uses unified management of the bastion machine, and the server SSH port or business management background is only open to the bastion machine whitelists to achieve the purpose of centralized access control and auditing.

4.5.3 Account Security

Operation and maintenance personnel use the operation and maintenance account to access the

management plane of Imou Cloud. The operation and maintenance account has been bound to the employee ID to achieve independent audit and separate authorization.
Operation and maintenance account management has strict account life cycle management and authorization management processes, and accounts with different roles have different permissions and responsibilities.
Imou Cloud Operation and Maintenance Account Management System:

- The operation and maintenance account uses double-factor authentication, and the super-privileged account performs dual management (co-managed by two or more people)；
- Separation of operation and maintenance personnel accounts, assigning unique operation and maintenance accounts to each operation and maintenance personnel；
- Regular operation and maintenance account audits, and a dedicated audit team regularly conducts reasonable audits of the operation and maintenance account permissions to ensure that each account has the minimum required permissions and timely handling of invalid accounts；
- AD domain authentication and VPN tunnel, operation and maintenance login management plane, when developers log in to the development environment, they must first log in to the AD domain authentication server of the company's IT, and then connect to the Imou cloud bastion machine through the VPN network for management；
- The bastion machine manages the servers on the cloud in a unified manner. The server password and key are managed by the bastion machine to avoid the leakage of the password and key. Bastion machine login has double-factor authentication. Personnel operations have screen recording for easy post-event audit.

4.5.4 Security Monitoring and Alarm

Imou Cloud collects, analyzes and processes security logs and security events in cloud services through the SIEM system. The system integrates security logs of various services, including security logs of key services and operations such as user account blasting, application service attacks, network attacks, and operation and maintenance account behavior analysis. These logs are correlated and analyzed through professional analysis tools to perform notification or alarm handling. The security log in Imou Cloud Service is kept for more than 180 days and can be used for real-time query, audit and backtracking.

4.6 Security Management

4.6.1 Vulnerability Management

Imou Cloud has been doing network security in a proactive manner, with security activities covered before, during, and after the system goes online, including vulnerability scans, configuration checks, penetration tests, and code audits. The vulnerabilities collected through internal security activities

and reports from external security researchers form the basis of Imou Cloud's vulnerability management. The security liaison person of Imou Cloud is responsible for the analysis and identification of vulnerabilities, and assigns them to the corresponding R & D or O & M to repair. After repair, feedback to the vulnerability reporter for verification until the repair is confirmed. Imou Cloud Vulnerability Management strictly complies with the company's incident response SLA requirements.

4.6.2 Risk Management

Risk assessment includes activities such as asset collection and analysis, vulnerability assessment, threat modeling, configuration inspection, and operation and maintenance security assessment. Imou Cloud risk assessment standards are established based on the international standards for risk assessment, CSA Cloud Security Guidelines, CSA CCM, Level Protection 3.0, and ENISA Cloud Computing Security Risk Assessment. Risks from risk assessment are jointly discussed by multiple departments to determine the risk mitigation plan and continue to track the implementation of the plan.

4.6.3 Security Audit

The security audit is an independent third-party department (Corporate Legal Affairs, IT, Information Security Department, Network Security Department) who independently or jointly audits Imou Cloud. The audit content includes information security, network security, security operation and maintenance, and user privacy security. According to the auditing standards, conduct regular security audits, and continue to conduct security construction based on the audit results. It plays a key role in the security advancement.

4.6.4 Incident Management

Imou Cloud has established an event management process system and implementation strategy. Implement a graded evaluation system for incidents and classify incidents into four levels: critical, high, medium and low. Use detection, suppression, recovery, and eradication methodologies to provide technical support capabilities, and follow the SLA requirements for each level of event processing.

4.6.5 Incident Response

Imou Cloud has established a complete incident response process, including incident procedures and measures when encountering security events such as malicious programs, network attacks, security incidents, network interruptions, and data breaches. Imou Cloud formulates and carries out various emergency drills according to the importance and actual business conditions, providing

technology and capacity reserves for incident response.

5 Data Security

5.1 Data Lifecycle Management

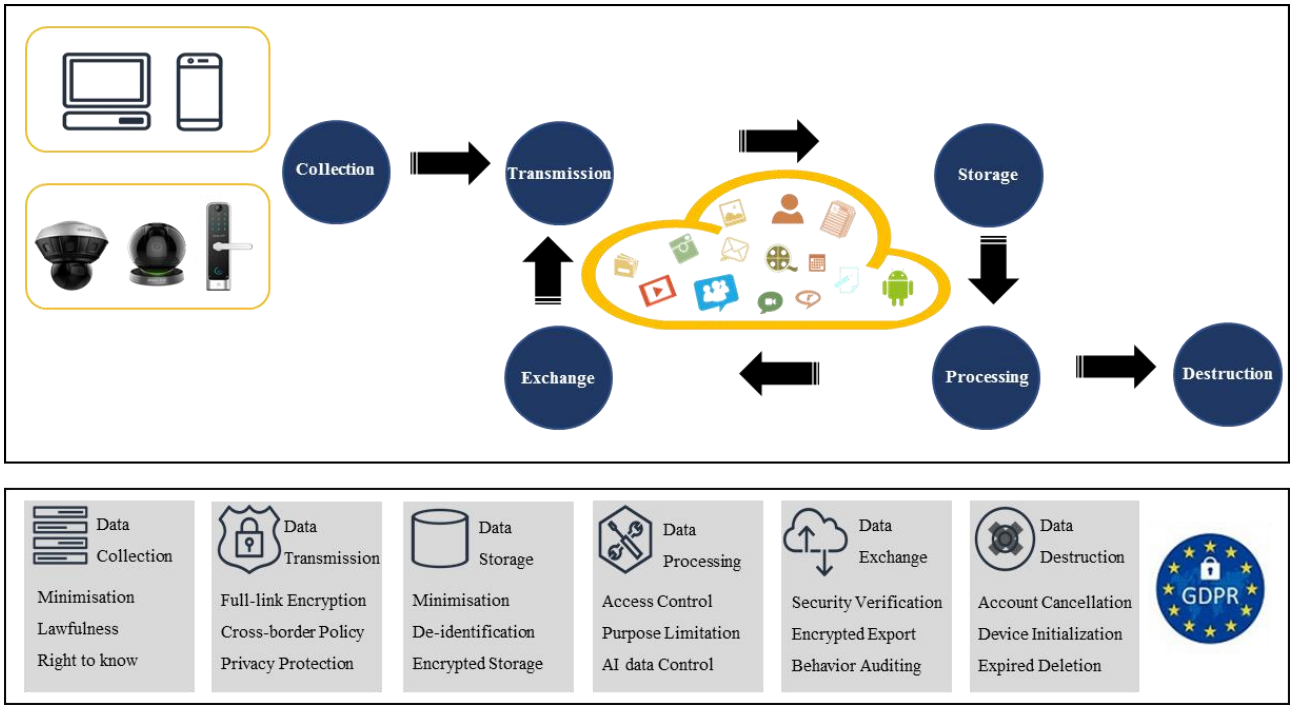


Figure 5-1 Data Life Cycle

Imou Cloud data security system manages and technically controls all aspects of the data life cycle (data collection, storage, transmission, exchange, processing, and destruction). While ensuring the safe and stable operation of the cloud platform, improve the confidentiality, integrity and security of data.

- Data collection: Imou applications and devices, including cameras (Imou camera, Imou NVR, etc.), APP applications, and PC client programs, etc. When collecting user personal information, strictly follow the principle of minimization and clearly inform the collection purpose through the privacy policy, and obtain the user's explicit consent and authorization.
- Data transmission: Imou Cloud uses a full-link encryption scheme to protect the network transmission of user data. Without affecting the business use, sensitive data needs to be encrypted before transmission. When data is transferred across borders, Imou Cloud Service combines with cloud service provider’s cross-border policies to comply with corresponding regional laws and regulations.
- Data storage: Imou Cloud combines with cloud service provider’s secure storage solution to provide users with secure cloud data storage, follow the principle of minimum storage period, and implement strict access control policies to prevent illegal access inside and outside. User data is stored after encryption, and the encryption key can be set by the user.
- Data processing: Imou Cloud uses data stream files to identify the business functions for processing personal information and sensitive information, and adopts fine-grained

authentication and authorization and access control strategies. When processing personal information, strictly follow the purpose stated in the collection or the scope of reasonable association. Handle AI feature data carefully, after using personal biometric information to implement functions such as identity recognition and authentication, delete the original image.

- Data exchange: through the secure export function of Imou client or contact the customer service of the official website, export the user's personal information as required. Media data is encrypted in the process of uploading on the device side, storing on the platform side, and downloading on the client side, while providing users with a custom password function to encrypt the media stream. It also supports user behavior auditing of users who initiate data export requests.
- Data destruction: Imou Cloud will delete the user's personal information or do anonymization when the account is cancelled or the data expires. Imou Cloud Service provides a corresponding interface and a simple and easy method for canceling accounts. Users can also submit feedback / contact official website customer service to clear personal data on the cloud. When using terminal devices such as Imou cameras, users can delete personal data stored in the device by restoring factory settings, increasing the transparency of data deletion processing.

HuaCheng has formulated the "Personal Data and Privacy Protection Standards" based on security design principles, personal information security regulations, GDRP regulations and TÜV Rheinland standards. Restricting security compliance requirements, privacy policies, basic principles of personal data processing, user rights, etc., Imou Cloud strictly abides by this standard.

5.2 Enterprise Data Security

Imou Cloud logically prohibits mutual access to data belonging to customers of different enterprises, and processes customer data in accordance with customers' written instructions and contract agreements on the basis of compliance with laws and regulations. All data processing behaviors are transparent to customers and protect enterprises confidentiality, integrity, and security of customer and user data.

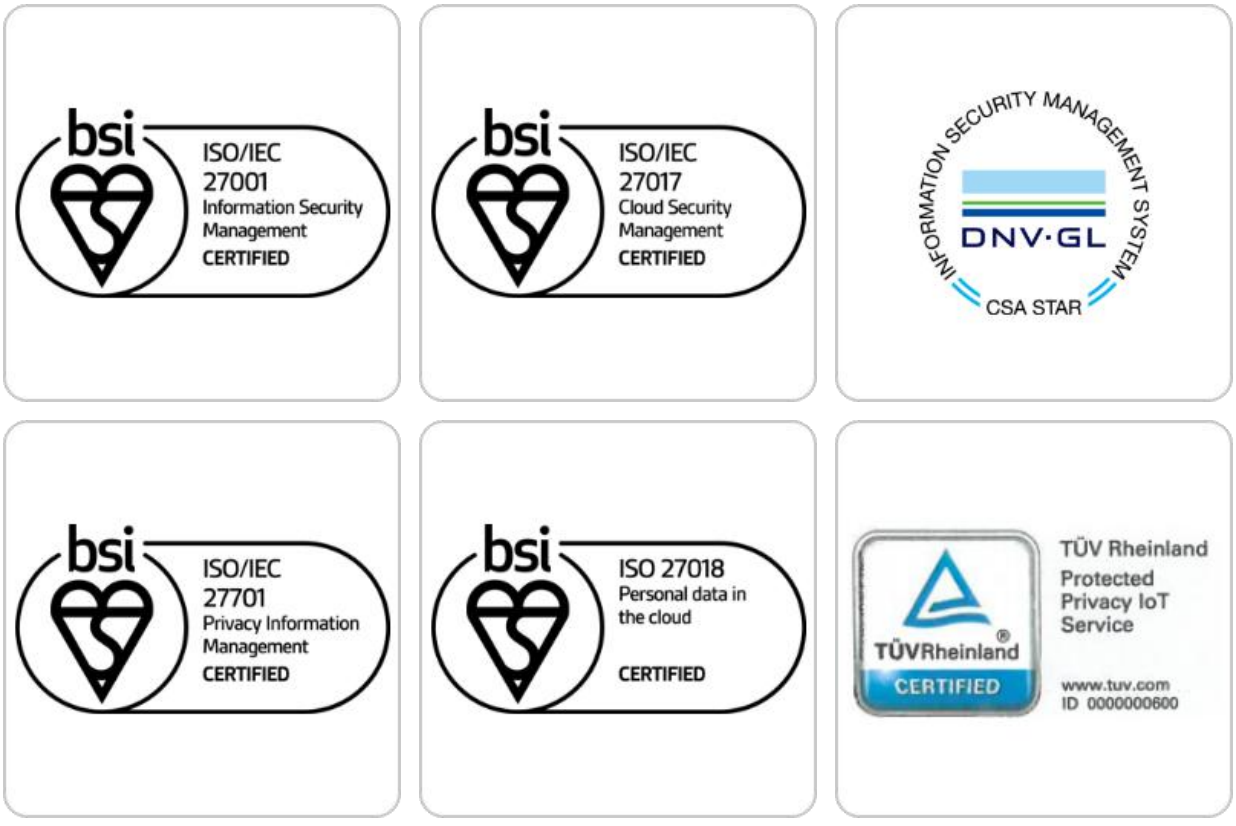
6 Security Compliance

Security compliance is the foundation of the development of Imou Cloud. According to domestic and foreign standards and industry practices, Imou Cloud integrates many compliance control points into the internal control management and product design of the cloud platform, and strives to create a cloud service that is trustworthy by users; at the same time, actively participate in the formulation and promotion of industry security standards, adhere to compliance as a service, and build and operate a secure and reliable cloud ecological environment.

In the field of privacy protection compliance, Huacheng complies with the GDPR Act and implements privacy and data governance practices. It has obtained the German TÜV Rheinland IoT service privacy protection certification and the British Standards Institute (BSI) issued ISO27701, ISO27018 certification.

In the field of cloud security control, Huacheng implements the CCM cloud control matrix and NIST SP 800-53 standards, and has passed the CSA STAR certification issued by Det Norske Veritas (DNV) and the ISO27017 certification issued by the British Standards Institute (BSI).

In the field of information security management,Huacheng follows the international authoritative certification system and has passed the ISO27001 certification issued by the British Standards Institute (BSI).



7 Security Commitment

HuaCheng has always adhered to the principle of customer first, and insisted on creating an Internet of things industry service provider and solution provider with video services as the core. Attach great importance to the security of users' personal information, and take all reasonable and feasible measures to protect the security of personal information. Strive to provide customers with a safer and healthier Imou Cloud environment.

HuaCheng has always regarded cyber security and privacy protection as one of the company's highest programs and has continuously invested special funds to comprehensively improve security awareness and capabilities aims at providing sufficient security protection for its products. HuaCheng has established a professional security team, which provides whole life cycle security management and control for product design, development, testing, production, sales and aftersales. While insisting on data minimization, service minimization, strictly prohibiting backdoor, removing unnecessary and unsecure services (such as Telnet, etc.), HuaCheng constantly introduce innovative security technologies, strive to promote and improve the product security capability, and better meet the security requirements of users in different scenarios.

HuaCheng established ISRC (Imou Security Response Center) to solve cyber security issues and provide reliable and secure solutions for global customers, including Security Advisories, Security Alarms, Vulnerability Report and Response Processes, and sharing Security Suggestions and Research Results, etc. For the latest and detailed security information.