August 2019

White Paper on the Security of Gizwits IoT Platform

V 2.0

Gizwits

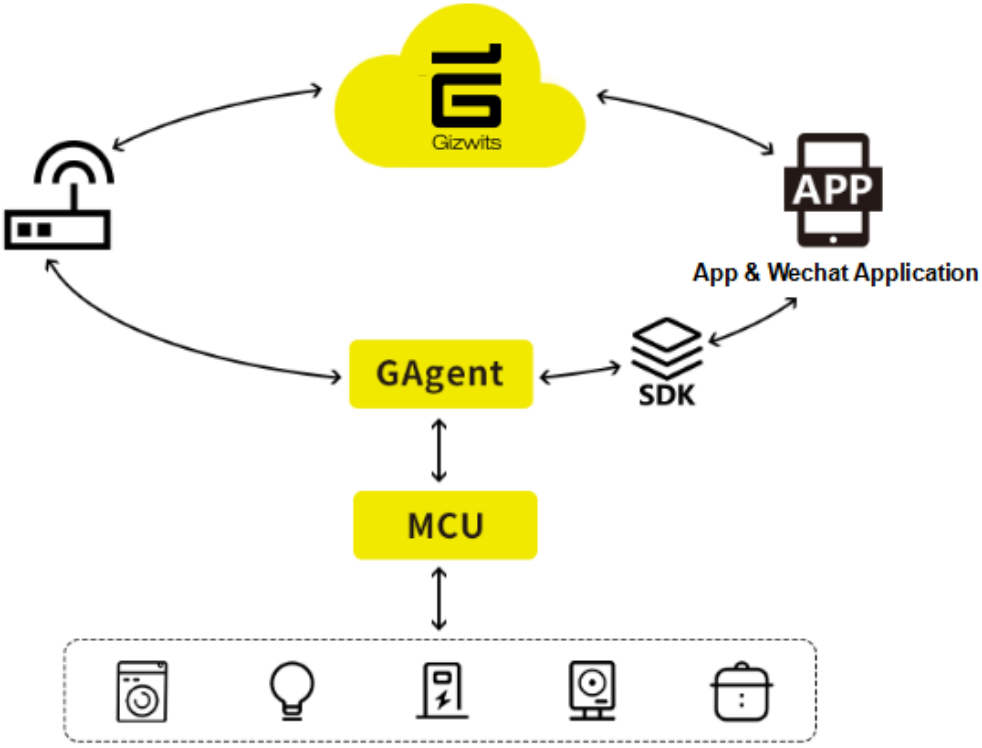
Table of Contents

1. About Gizwits

1.1. Introduction to Gizwits IoT Cloud Platform

Gizwits has deployed its services based on the cloud platform globally, with three major cloud service centers around the world, including Domestic cloud, US East cloud, and European cloud, which are committed to providing clients worldwide with secure, stable, reliable, and fast cloud services based on a platform compatible with access of heterogeneous network, multi-protocol, and multi-platform device thanks to the processing capacity of Gizwits that is large enough to accommodate tens of millions of concurrent connections (single machine) and the capability to provide uninterrupted services with 99.95% service availability.

The platform provides the ability from product definition, device development & debugging, application development, production testing, cloud development, operation management, data service and other aspects covering intelligent hardware access to the full life cycle service of operation management, providing developers and manufacturers with self-service intelligent hardware development tools and open cloud services, and reducing the technical threshold of hardware development of IoT through automated self-help tools, perfect SDK and API service capabilities so as to decrease the cost for research and development, improve the speed of putting products into operation, help developers and manufacturers upgrade their hardware intelligently, and thus to better connect and serve the final consumers.



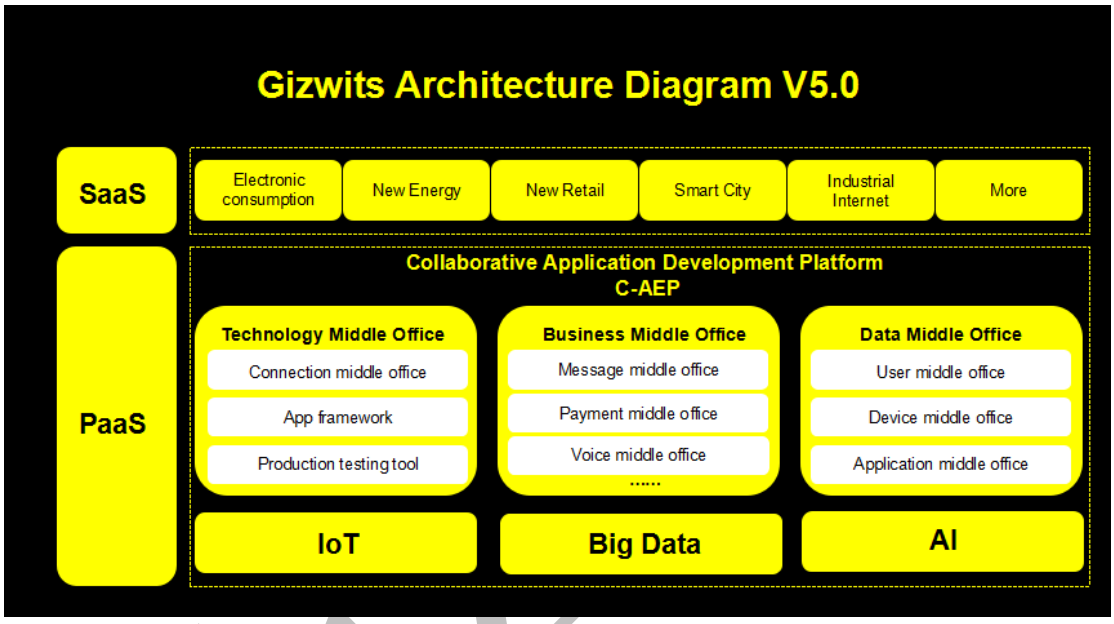
The platform maintains the cooperation with recognized domestic and foreign security agencies and the implementation and evolution of security applications, and at the same time also keeps the innovation and upgrading of service capabilities and technologies; Gizwits 5.0 provides developers and manufacturers with the platform for development of IoT-aided application and helps developers and manufacturers quickly implement applications and solutions in their industries. Gizwits C-AEP (collaborative application development platform) is a mid-platform architecture built by Gizwits for the attributes of the IoT industry, and it includes technology middle office, business middle office and data middle office.

The technology middle office provides an end-to-end technical framework of IoT and a set of convenient tools, including connecting middle office, APP frameworks, production testing tools, etc.

The business middle office provides formation services for common business of IoT device and users, which are used by various applications with IoT

attributes, and can quickly launch new businesses to achieve rapid IoT and meet changing business demands.

The data middle office carries out standardized modeling on the IoT data, with the device data and business data uploaded to the cloud and then stored in the theme database of the data middle office through data governance, including user middle office, device middle office, application middle office, etc.



1.2. Mission to Ensure Information Security

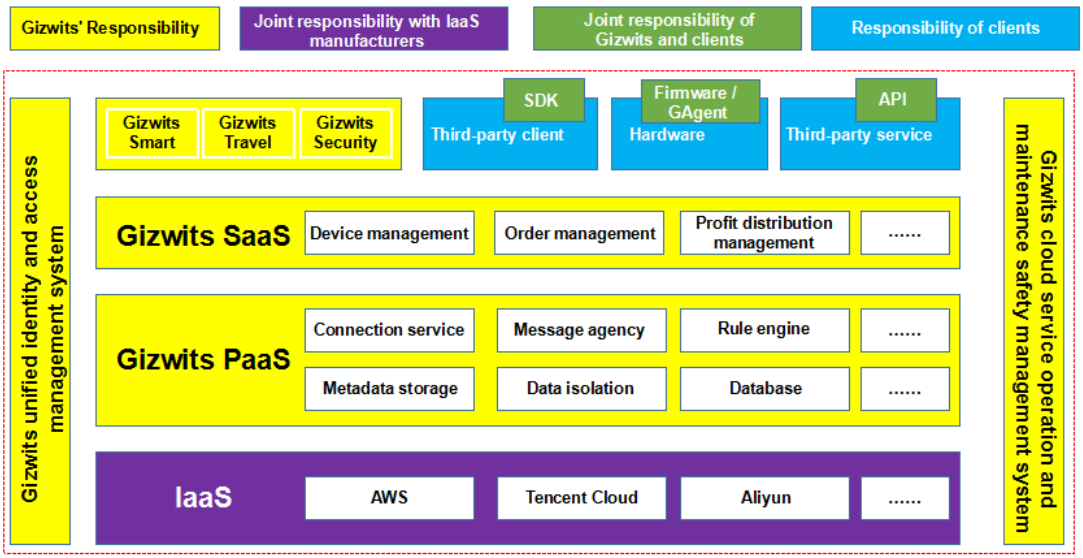
Gizwits provides clients with secure and reliable device interface services (GDCS) and industry SAAS services that comply with regulatory requirements, and makes every effort to ensure the reliability, confidentiality and integrity of the data for clients and their users. Gizwits promises that data protection and data security are above all else. While providing stable and available services, Gizwits will continue to build a comprehensive cloud platform security guarantee system, and take information security as one of its important development strategies.

In order to achieve the objective and complete the mission, Gizwits strictly implements the whole process protection mechanism, and realizes security

protection at all levels, including security inspection, security defense, and security monitoring and auditing of all external services, so as to form a whole process protection network before, during and after the event.

1.3. Responsibilities for Security

Gizwits is responsible for the security management and operation of services and data interactions on the platform of Gizwits and also responsible for the security of the provided cloud service platform and infrastructure. Clients need to protect their applications and data, including hardware and app security compliance, when the APP or the hardware's embedded software (including the use of the SDK) developed by the client access the Gizwits cloud platform. The following figure shows the division of joint responsibility for information security among basic cloud service providers, Gizwits and clients:



1.3.1. Responsibilities of Gizwits for Security

Gizwits cooperates with global mainstream cloud computing platforms such as AWS, Microsoft Azure, Tencent Cloud, and Aliyun to ensure the security management and operation of infrastructure and physical devices. For example,

the security capabilities and responsibilities of cloud service providers Tencent Cloud and AWS are as shown in *Tencent Cloud Security Responsibility*, *AWS Security Overview*, etc.

Gizwits Security covers data security and cloud service security. Gizwits is committed promises to use the professional attack protection technology experience of security teams and well-known security service providers around the world to provide secure operation and maintenance and operation services of cloud platforms, effectively protect the security operations of Gizwits, and ensure the privacy of clients and users and the security of data, including but not limited to:

- Data security: Data classification, data access control, data desensitization, etc.
- Cloud service security: Security management of business-related application systems in the cloud computing environment, such as application, interface design and development, security specifications, release, and use.

1.3.2. Responsibilities of Clients for Security

Clients are required to strictly adhere to the requirements for the security specifications and interface of Gizwits cloud platform when using the solutions based on Gizwits cloud platform. At the same time, clients are required to ensure the security of the developed products and applications, including business background, client, and hardware product security design. For the firmware and SDK secondarily developed on the basis of GAgent and APP framework of Gizwits, only technical support will be provided by Gizwits, without any security guarantee. Gizwits will provide templates for clients' reference for data security compliance, privacy policy and other related information based on the public version of APP (including any micro-customization of functions) of Gizwits;

clients will be fully responsible for the specific online privacy policy statement and legal compliance; if related security solutions are involved, provided that the two parties have reached a consensus, Gizwits can provide solutions for reference and consulting services.

2. Security System

2.1. Data Security

As everyone knows, data protection is the basic requirement of enterprises, governments and individuals today. With a deep understanding of the importance in data security to client business and client privacy, Gizwits sets out from the perspective of data security life cycle to formulate corresponding data security management policies for each life cycle stage of data generation, data storage, data transmission, data usage, data extinction and others to ensure end-to-end data security.

2.1.1. Data Ownership

All data generated by using services provided by Gizwits shall belong to clients. As the processor of data, on the basis of compliance with laws and regulations and Privacy Policy, Gizwits can help clients and users ensure the privacy, integrity and security of data under the authorization of clients and users.

2.1.2. Data Classification

Gizwits provides security protection for data of all users and enterprise clients. According to the data stored and used, the data level protection strategy is implemented, and the data level is divided according to the data value and

sensitivity degree. According to the classification of data security, corresponding protection policies and requirements are formulated to protect the safe data storage for users and enterprises.

2.1.3. Data Access Control

Gizwits provides security for data access of enterprises and users. Accesses to data used by all APP/business clouds are strictly controlled. Any third-party application accessing and using enterprise or user data must be authorized by the enterprise or user, and the operation will be recorded in the corresponding operation log for subsequent tracing and auditing.

2.1.4. Data Desensitization

In order to avoid the leakage of sensitive data, Gizwits desensitizes and encrypts sensitive data of users and devices to realize safe storage, and prevents attackers from acquiring sensitive information through static analysis of firmware/acquiring documents after logging in to devices, etc.

2.1.5. Data Destruction

Users/enterprise clients have the right to delete sensitive data belonging to current users/enterprise clients through APP/business background, and can also contact the client service of official website to submit an application for deletion, which will be executed according to the process after authentication and verification of identity. Once executed, the data cannot be retrieved. When the memory and disk used by Gizwits to store client information need to be replaced, logical erasure and physical erasure will be performed first, and then the cloud service provider will demagnetize the storage media according to industry standard practices.

2.2. Application Security

2.2.1. Cloud Platform Security

2.2.1.1. Identity Authentication of Device

The focus of IoT security is on the hardware side of the device. Gizwits provides corresponding device identity authentication schemes for hardware devices at different security levels to meet the actual business demands of different device manufacturers.

- Pre-authorization authentication mode

For the devices at the ordinary security level or for the enterprises that have strict cost control requirements, Gizwits provides pre-authorization authentication mode to protect the identity security of the enterprise's devices. Pre-authorization are available in the following forms:

In the production testing phase of the device, the pre-authorization key generated by the cloud is burned to uniquely identify the legitimacy of the device. In the power-on registration process, the device must complete the registration process according to the pre-authorization key to obtain the unique number of the device generated by the cloud. The tools in the production testing phase need to be authorized before being provided to the enterprise for use.

Manufacturers provide codes that uniquely identify communication devices, such as MAC addresses of Wi-Fi modules or IMEI numbers of cellular modules, and provide these codes to Gizwits through the developer center or API of Gizwits before the device is connected to the cloud.

- Asymmetric authentication mode

For devices at a high security level or modules with strong hardware computing capability, such as Android and Linux, Gizwits provides asymmetric

authentication mode based on RSA1024 or 2048 bits. For some clients with special needs, Gizwits can also support the implementation of private encryption algorithms.

2.2.1.2. User's Identity Authentication

- The Gizwits platform has the following types of users:

  - Access provider user

Enterprises connected to the IoT platform of Gizwits, which develop and produce devices as developers, shall carry out R&D, debugging and production testing of devices, and provide after-sales service.

  - Operator users

Users using devices connected to Gizwits and supporting business systems to complete different types of services, such as after-sales service, shared leasing, and device management.

  - Consumer users

Users actually purchasing and owning devices, or using the devices in a shared service scenario.

- For different types of users, the platform of Gizwits provides different identity authentication methods:

  - Access provider users

Access providers mainly use the developer center of Gizwits. Gizwits provides two levels of personal account and enterprise account, and each level has multiple authorities such as owner, manager and observer. Key data can only be obtained by the owner, thus realizing data confidentiality at the account number and authority levels. At the same time, the personal account number can be added to the enterprise account number, providing high flexibility in the use of products.

  - Operator users

Operators mainly use various business systems developed based on Gizwits C-AEP, which are provided with necessary functions and data through enterprise API, SNoti, real-time big data, aggregated data, rule engine and other interfaces. Gizwits authenticates the business system by the method based on the access key and further ensures security through the white list.

When an operator's system interfaces with the platform of Gizwits, the access authority to data is strictly controlled, and data that does not belong to the operator is invisible. In addition, operators will have detailed records of their operations of key data for auditing purposes.

- Consumer users

The identity of the consumer users must be registered, providing email, mobile phone number, and third-party system account number, with strict password policies to protect the user's identity from random guesses. Random SMS and email activation shall be provided to confirm the authenticity of users. The user must successfully log in to perform business operations.

The platform of Gizwits provides OAuth/OAuth2 capabilities, which can be integrated with third-party OAuth ID providers, and can interface well with WeChat public numbers, applets, and such major third-party platforms as AWS, Google, Aliyun, Baidu, Miot, and IFTTT.

2.2.1.3. Matching between Device and User Identity

The Gizwits IoT platform provides IoT access services for devices and consumers of many different enterprises. The matching between the device and the user's identity is crucial.

Users operating devices: Gizwits only allows users who have the right to operate a device to operate the device. Only users who successfully bind or share binding rights can control the device.

Device data is forwarded to matching users: The system is equipped to forward the status and data of the device to the corresponding bound user mobile phone application.

2.2.1.4. Current Limiting Control at Application Layer

Access control at the application layer is a capability that the IoT platform must have to prevent business logic problems or other behaviors of access enterprises from affecting other users of the platform.

Reporting frequency control of device: The reporting frequency of each product device can be controlled to limit unreasonable request amount;

Access control for API time dimension quota: Provide a control mechanism for the total access limit of the time period dimension to prevent high-frequency service requests in a short period of time;

Access control for IP quotas: Provide access limit control for IP dimension;

Access control for quota application on consumer side: Provide access limit control for an application;

Access limit control for users at a single consumer side: Provides access control ability to a user.

2.2.1.5. Application Security Control of Web System

The Web vulnerability control mechanism is built into the external Web system and implemented in the technical framework:

SQL injection control: WEB system framework controls SQL injection.

Cross-site scripts: Prevention of cross-site script attack

Script file upload: Strictly control the upload path and file type to prevent attackers from uploading malicious codes and gaining control of the host.

2.2.1.6. Transmission Security

Gizwits uses TLS1.2 by default to provide encrypted transmission services for devices and applications to ensure the security of information in network transmission.

For devices at ordinary security levels, some modules can't use TLS1.2 from the cost point of view. By default, Gizwits provides AES128-bit symmetric encryption (or other encryption algorithm) to protect the transmission security from the device to the cloud and prevent data leakage. AES encryption (or other encryption algorithms) is at the service level. Gizwits provides a dynamic key update mechanism to make up for the deficiency of symmetric encryption.

2.2.2. Device Side Security

2.2.2.1. Program Code Security

The codes of the device and communication module are all written in C language, and the production files are based on compiled BIN files or HEX files, thus 100% avoiding source code leakage.

The product development process should follow a strict development process, including code specification management, code review mechanism and strict quality testing process, and Git should be used for code warehouse management to avoid product safety problems caused by code development.

Information in the device log needs to be printed hierarchically. Sensitive information (such as ID of the device and static password) should be replaced by asterisks to avoid information leakage caused by debugging information.

2.2.2.2. Data Storage Security

The cloud registration and pre-processing of the device all use AES 128-bit encryption algorithm for data encryption to ensure the security of data content.

Static sensitive data of the device, including the model password of the device, the local access password of the device, the pre-authorization password of

the device and the ID number of the device, should be stored in the flash of the device after confusion and encryption.

The offline log stored in flash by the device is the log code after confusion and compression, without any clear text log information, thus ensuring the security of the offline log.

The device supports restart and reset commands issued by the cloud, and can be operated remotely according to product requirements. When necessary, all data on the device can be destroyed.

2.2.2.3. Anti-counterfeiting of the Device

Gizwits supports various pre-authorization processes. Before a device is registered in the cloud, it must obtain a legal authorization key to correctly register in the cloud, thus eliminating the connection of illegal devices.

The authorization key supports burning during production, i.e. one code for one machine, to prevent device from embezzling the pre-authorization key.

In order to prevent the module from being improperly used by the firmware and verify the authenticity of the module firmware, authentication is required to be conducted after the module is started:

- After the module is started, it is required to read the production data from flash and extract the identity verification data. First, hash check is carried out on the whole production data to ensure that the identity verification information is correct. Then the identity verification ID is calculated by combining the version number of the module, mac and the encryption factor in the verification information. Finally, it is compared with the identity ID in the verification information in flash. If they are consistent, they pass, and if they are not consistent, they should be restarted.

2.2.2.4. Supports for Standard TLS and Custom Transport Encryption

The module supports TLS1.2 link layer encryption and AES128 bit data layer encryption.

The module supports transparent transmission mode. In this mode, the device can encrypt and transmit the device using a customized data encryption algorithm. At this time, the module acts as a data channel, and performs bidirectional forwarding of data under TLS encryption link. The device and the upper application are responsible for encrypting and decrypting the data layer.

2.2.2.5. Distribution Network Security

Gizwits supports the two distribution network methods of SoftAP and AirLink. The content of the distribution network is encrypted by AES and transmitted to ensure the security of the distribution network.

Gizwits supports Bluetooth distribution network, and Bluetooth point-to-point data communication between mobile phone and devices, with the content of the distribution network to be encrypted by AES to ensure the security of distribution network.

2.2.2.6. OTA Security

OTA is subdivided into modules OTA and MCU OTA to avoid the failure of firmware upgrade caused by OTA confusion.

The request process of OTA uses AES for data encryption to ensure data security.

In OTA files, MD5 is used for file verification, which avoids the problem of abnormal startup caused by device upgrade errors or incomplete files.

Sensitive information is removed from OTA firmware to obtain pure binary files, thus preventing information loss caused by device OTA file leakage.

OTA process supports continuous transmission at breakpoints to ensure the success rate of OTA device to the greatest extent and avoid safety problems caused by long-term failure of OTA device.

It supports the two methods of pushing OTA and checking OTA after power-on, and responds to OTA request as soon as possible to speed up OTA process.

2.2.3. Mobile Application Security

2.2.3.1. Storage Security

Storage security is a very important link in application security.

- In iOS, Gizwits stores sensitive data (Token, etc.) that need to be stored locally in "Keychain". In the storage process, two different AES-256-GCM tables are used to encrypt metadata and keys, ensuring the security of sensitive data.
- In Android, Gizwits uses "Keystore" to ensure data security. Keystore can protect the key from being used in a trusted environment. Keystore can prevent external access to keys from processes and devices and avoid unauthorized access to and use of keys.

2.2.3.2. Network Communication Security

- The mobile applications of Gizwits conform to App Transport Security (ATS) security mechanism to ensure secure network communication.

2.2.3.3. Application of Hot Update Security

- MD5 verifies the integrity of OTA packets
- When creating applications, keys are generated and stored in the cloud and App respectively, which are used to check the legality of OTA packets during OTA updates and prevent malicious push updates.

2.2.3.4. Application Uniqueness

- Application start-ups will perform integrity check to ensure that the application has not been tampered with or repackaged.

2.2.3.5. Code Security

- Gizwits is protected by a unique additional shell to protect App and prevent static reverse.

- Anti-reverse protection, code arrangement, code confusion, code slicing, false control flow, string encryption, control flow flattening and other technologies are used to ensure the security of the code.

2.2.3.6. Operation Protection

- Gizwits encrypts memory, local data and resource files to ensure the application security at runtime.
- Anti-information theft and anti-dynamic debugging technologies are used to prevent application data from being stolen from outside.
- Memory anti-dumping protection.

2.3. System Network Security

2.3.1. System Security

Gizwits cooperates in depth with Tencent Cloud and AWS, with the cloud service providers to be responsible for the physical and infrastructure security at the bottom of the whole cloud computing environment, providing security management measures including vulnerability discovery, patch repair, upgrade and update, audit monitoring, etc. Gizwits will also regularly entrust a third-party security company to conduct relevant security tests on operating systems, networks, middleware and applications, and make timely rectification to ensure that the system meets relevant security requirements.

2.3.2. Access Control

When accessing all systems that carry and store user and enterprise data, Gizwits must log in through a bastion machine. Access to data at a high-confidentiality level must be detailed to individuals, and there must be a secure login mechanism. Everyone's access shall have been authorized and

conforms to the principle of minimization, with all behavior log records to be complete and remote backup in line with the auditable requirements.

2.3.3. Network Security

2.3.3.1. Network Isolation

Gizwits has formulated strict internal rules for network isolation:

1) Physical and logical isolation between office network, development network, test network and production network. Private cloud, private cloud and public cloud are isolated through virtualization control access policies.

2) Access authority isolation. Unauthorized personnel are prohibited from accessing any internal network resources, and authorized personnel can only access relevant authorized networks after logging into a bastion machine through VPN network.

3) Cloud users are divided according to their authority. Access to the private data of the current personnel can only be conducted after authentication by security mechanisms such as identity authentication, certificate authentication, key authentication or interface token authentication.

2.3.3.2. Network redundancy

The data centers of Gizwits are located in many regions of the world, covering China, USA, Europe, Asia-Pacific and other places, and have built multi-physical computer rooms in the same city and a secure network in many centers in different places through the dedicated lines of cloud service providers, with the capability of disaster preparedness across regions, effectively reducing the continuous impact caused by public network failures of operators, ensuring that network services will not be interrupted due to single-point failures, and realizing the capability of disaster tolerance and even cloudy switch within the same city and across cities.

2.3.3.3. Intrusion Detection and Protection

Based on the proven network security architecture provided by well-known cloud service providers such as Tencent Cloud and AWS, Gizwits has realized all-round protection and has deployed security protection at all levels, including security physical examination (vulnerability scanning, horse-hanging detection, website back door detection, port security detection, etc.), security defense (DDoS protection, intrusion detection, access control to ensure data security and user privacy) and security monitoring and auditing, forming a whole-process

protection before, during and after the event to deal with various threats from the Internet.

2.3.4. Operation and Maintenance Specification

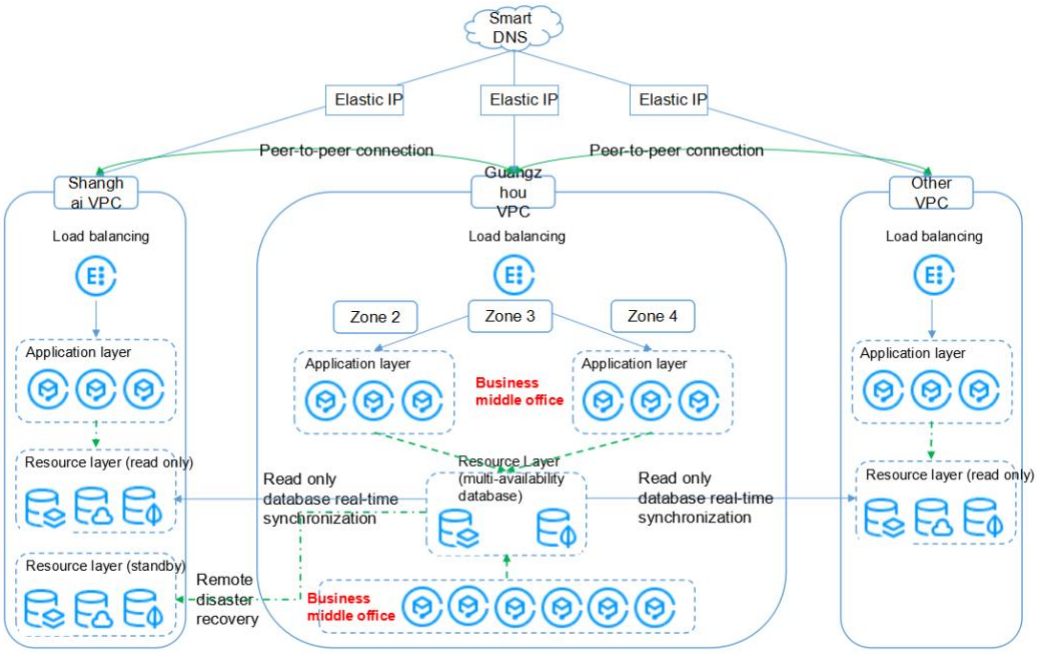
Gizwits ensures operation and maintenance safety through the strict internal management system in combination with automatic and instrumental O&M management platform.

- **Certification:** Operation and maintenance personnel must go through the Bastion Machine to access the production environment where client data is located, and all operation and maintenance accounts are equipped with a two-factor authentication mechanism.
- **Authorization:** When granting the authority, it is ensured that only the minimum authority required by employees to provide corresponding services is granted through fine granularity in the authority division, and all applications for additional authorization need to go through multiple reviews and approvals.
- **Monitoring:** The O&M team implements 7x24 hour emergency response duty mechanism. Once a security event occurs, it will be responded to and processed according to different event levels. Security events related to users and clients will be given the highest priority. The management of events includes the whole process of acceptance, notification, handling and summary after the event. The summary of events will fundamentally analyze the causes from multiple dimensions such as technology, process and consciousness, and implement the responsibility punishment to prevent similar events from happening again.
- **Audit:** Responses to all vulnerabilities and events are implemented based on a platform and in an online manner, with all records to be complete and queryable. Any internal personnel shall not touch the client's cloud business

data without the client's consent and authorization. The O&M team will regularly summarize and analyze all kinds of security data, and present and report them to the senior management of the Company.

2.4. Disaster Recovery and Business Sustainability

2.4.1. Multi-site and Multi-activity Architecture of Cloud Services



In order to promise and guarantee the service quality of the IoT platform, Gizwits formulates and strictly implements service level protocol. In order to prevent the interruption of business activities, protect business processes from major failures of information systems or natural disasters, and ensure their timely repair, Gizwits strictly implements disaster recovery and business continuity management requirements, mainly including:

- **Backup Management and Data Recovery:** The user data of Gizwits are copied and stored in multiple systems and multiple data centers, and

corresponding backup programs, frequencies and storage periods are set according to business requirements. Geographical locations of different data centers are distributed to achieve the effect of remote mutual backup. Backup media and recovery procedures will be checked and tested regularly.

- **A business continuity plan should be developed and implemented:** Gizwits maintains or resumes the operation of the business through the formulation and implementation of plans, and regularly tests, maintains and reevaluates the plans to ensure the availability of information within the required level and time after the interruption or failure of key business processes.
- **Disaster Recovery Drill:** Gizwits conducts regular disaster recovery exercise and implements complete drills to test that organizations, personnel, devices, facilities and processes can cope with disruptions. All drills will be recorded and summarized, and measures will be taken to improve them.

2.4.2. Support for Offline Services

In the case that the device is completely disconnected from the network, devices of Gizwits support pure small loop control, which is a model especially suitable for some scenarios, such as the factory intranet environment that can 100% prevent data leakage.

The device supports direct access in hot spot mode without a router, and the mobile phone can connect the hot spot of the device to directly operate the device, which is convenient for use outdoor and in other environments.

When the device is connected to the cloud abnormally, it supports the storage of device logs to facilitate the troubleshooting of subsequent device problems.

When the device is connected to the cloud abnormally, the data generated by MCU can be saved and compressed. When the cloud replies, the data will be reported in time to prevent data loss caused by network problems.

3. Security Compliance

Gizwits complies with internationally recognized security standards and industrial requirements, and integrates them into the internal control framework, which is strictly implemented in the process of realizing the requirements of cloud platform, device side, APP, business background, etc.

At the same time, Gizwits also cooperates with independent third-party security services, consulting and auditing agencies to verify and ensure the compliance and security of the Gizwits platform.

At present, Gizwits has passed the certification by many agencies around the world and it is an IoT solution provider with multiple certifications.

3.1. Trusted Service of Industrial Internet Platform

Gizwits has passed the evaluation of the trusted services on industrial Internet platform.

The evaluation of trusted services on industrial internet platforms is organized by the industrial internet industry alliance, which focuses on trust and designs 24 indicators around "Have you made a real and standard commitment to the issues that users care about?". The platform services are evaluated through data review, technical testing and on-site inspection.

The evaluation of trusted services on industrial Internet platforms will help industrial Internet platform service enterprises establish industry service

conventions, so that users can safely use the platforms and competition can be more orderly.

3.2. ISO27001

Gizwits has been certified in accordance with ISO27001.

ISO27001 is a widely adopted global safety standard, which is based on the risk management as the core method to manage company and client information, and to ensure the continuous operation of the system through regular evaluation of risks and the effectiveness of control measures.

ISO27001 is a systematic and overall planned information security management system, which guarantees the security and normal operation of the organization's information system and business from the perspective of prevention and control. The ISO27001 system consists of two parts: Rules for Implementation of Information Security Management, which gives suggestions on information security management for personnel responsible for starting, implementing or maintaining security in the organization, and Specification for Information Security Management System, which explains the requirements for the establishment, implementation and documentation of the Information Security Management System (ISMS), and specifies the requirements for implementing security control according to the requirements of independent organizations.

The objective of ISO27001 Information Security Management System is to ensure the safety of enterprise information systems and businesses through the overall planning of information security solutions, and to maintain continuous normal operation.

ISO27001 certification is about the certification of information security management system. ISO27001 will effectively ensure the reliability of enterprises in the field of information security, reduce the risk of disclosure and better preserve key data.

3.3. ISO9001

Gizwits has been certified in accordance with ISO9001.

The ISO9000 quality management system is the foundation for the development and growth of an enterprise. ISO9000 does not refer to a standard, but a collective name for a class of standards. ISO9001 quality management system is one of the international standards formulated by the International Organization for Standardization (ISO) and has been recognized by more than 100 member countries and regions of the organization worldwide. ISO 9001 outlines a process-oriented approach for documenting and auditing the structures, responsibilities and procedures required to achieve effective quality management within an organization.

3.4. GDPR

GDPR (General Data Protection Regulation) was launched by the EU to curb the abuse of personal information and protect personal privacy.

GDPR requires that all people engaged in personal data processing must abide by its regulations and give some important rights to individuals whose personal data are being processed. Natural and legal persons involved in personal data processing, including companies and government agencies, are required to act in accordance with GDPR. Potential non-compliance can lead to high fines and the consequences of court proceedings and reputational damage.

Before GDPR came into effect, Gizwits had fully promoted data protection. Many requirements in GDPR all focus on ensuring effective control and protection of personal data. Gizwits provides clients with account deletion function, whereby clients around the world can destroy corresponding personal data by self-operation. All servers used by Gizwits to store the data of clients in Europe are located in Europe, specifically, Frankfurt.

3.5. VDE

VDE logo represents protection and security for electronic products worldwide. Through overall, neutral and independent testing of electrical products, VDE Institute is committed to their safety, electromagnetic compatibility and operational performance. In addition, VDE Institute provides support services for manufacturers to invest in the quality of their products.

Some clients who use the services of Gizwits have successfully passed through the relevant certification of VDE, and thus the services provided by Gizwits conform to the relevant security specifications of VDE.