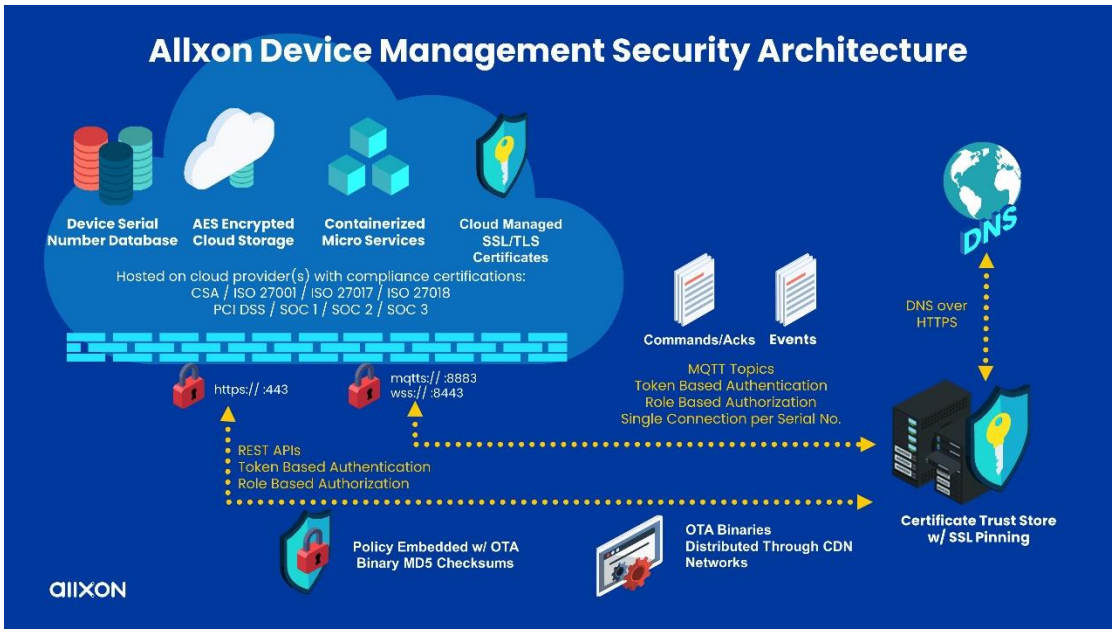
Allxon Security Whitepaper

2020 v.1.3

Contents

Introduction

Allxon is responsible for delivering high dependability and secure remote device management services. Allxon Cloud is a computing platform that allows customers to manage, monitor, and update their devices through a secure central portal system. Allxon Device Management Solutions (Allxon DMS) values and protects the integrity and confidentiality of their customers. A security by design (SbD) method is applied to the overall construction of Allxon's successfully robust AIoT infrastructure. Prior to the development of API and software, thorough research on potential and recurring cyber threats have been taken into account to construct a vigilant and up-to-date software system that consistently automates and regulates the security of its infrastructure. Allxon's SbD approach offers service integrators (SI) and managed service providers (MSP) a fully integrated cloud computing platform free from manual security configuration on cloud connections. Allxon's AIoT infrastructure and ecosystem, which comprises IHV, ISV, and SI/MSP, is built on multi-layered protection and defense security practices for secure data transfer and network capabilities. This article intends to explain the physical and operational security processes for networks and servers under the management of Allxon DMS.



Security in Connections

When data is transferred through the cloud from one location or network to the other, the data in transit becomes vulnerable to malicious cyber attacks. As a remote device management service, Allxon enforces the highest end-to-end encryption preventative controls to avoid threats when data is both at rest or transiting through their cloud system from portals to edge devices, and even from edge devices to control centers.

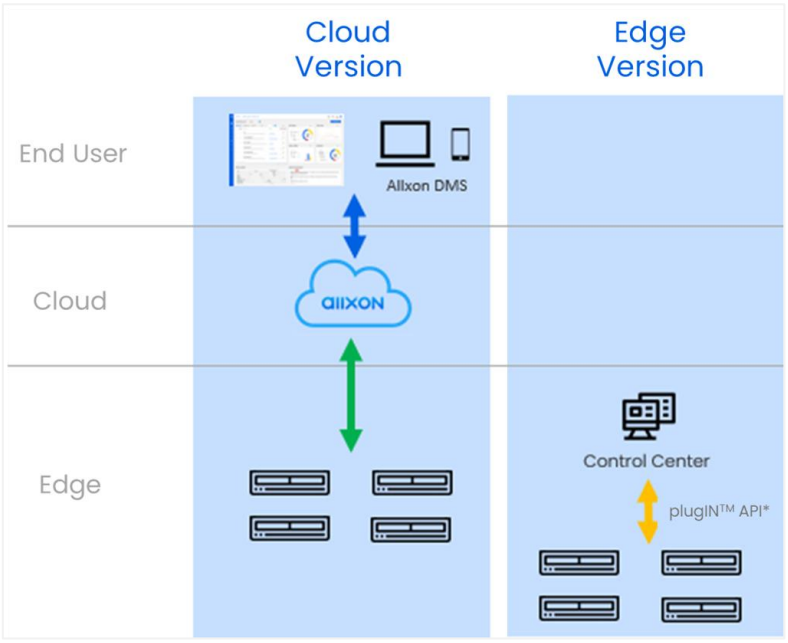


Figure 2. Allxon Cloud Architecture

Security between Allxon Cloud and End User

Allxon Portal makes it easy for users to access confidential information and remotely manage their devices with a user-friendly UI. Compatible with other ISV and cloud API versions, users can also incorporate Allxon Cloud as an invaluable tool to remotely manage their devices. Allxon Cloud is a fully encrypted network system with a robust underlying data protection infrastructure that withstands and prevents malicious activity and cloud data breaches. Allxon DMS uses a wide variety of security measures to put customers at ease while they handle digital information on Allxon Cloud.

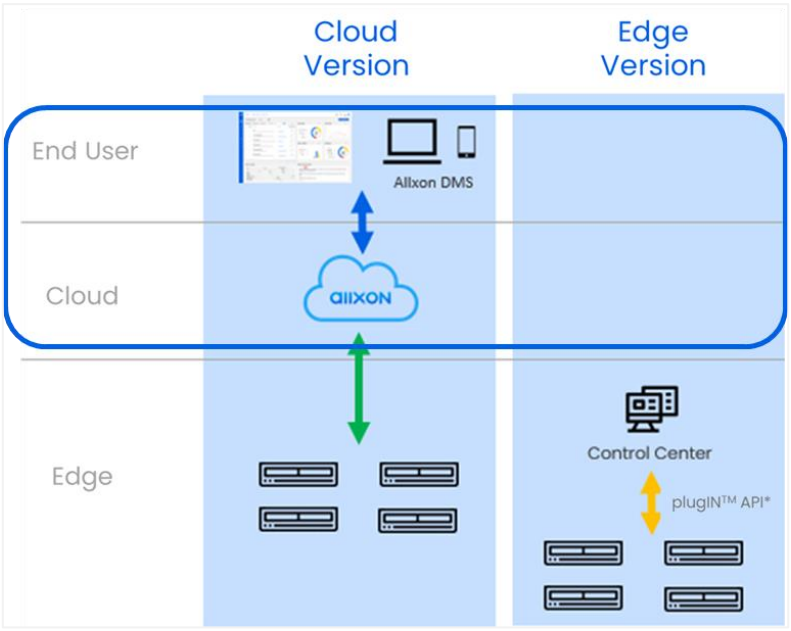


Figure 3. Security between Allxon Cloud and End User

Man-In-the-Middle Protection

Allxon ensures all cyber activity is monitored and operated on a securely encrypted network to prevent third party interventions such as man-in-the-middle (MITM) attacks. Allxon DMS uses cryptographic authentication to ensure communication between hosts are certified and consistent. Multi-factor authentication is implemented to prevent users from slipping onto an undetected network that may give away personal information and important data to cybercriminals.

Token Authentication

Allxon applies multi-factor authentication methods to secure the verification process when accessing cloud services. This additional layer of security is a token-based authentication process that requires users to insert a computer-generated code (a token) and the user's password before they are granted network entry. Multi-factor authentication methods create extra barriers to prevent cybercriminals from accessing private information possessed by the user and the organization.

Privileged Access Control

Allxon DMS uses a privileged identity management system to control network access from different users and groups. In a hierarchy security model, group administrators grant different levels of role-based access control (RBAC) rights to users according to the user's role in a group. In addition to individual permission, users have role-based access to their subset level, but never access to a level above or to other nodes in the same level. The enforcement of permission levels in hierarchy security models is a sophisticated RBAC management tool to help users and groups access and retain confidential resources, simultaneously regulating a vigilant security infrastructure.

Security between Allxon Cloud and Edge

Allxon is prepared for a wide coverage of interconnected devices to their cloud services. With potential exploitation and MITM attacks that are easily caused by multiple entry points, Allxon builds its cyber security foundation upon resilient communication channels. Allxon particularly focuses on enforcing robust cryptographic protocols for their own services such as Over-The-Air (OTA) updating, which is a time and cost effective solution for service providers looking to transfer new AI models to edge devices. Allxon implements the highest security measures to ensure data in transit is uninterrupted and safely transported to its desired location.

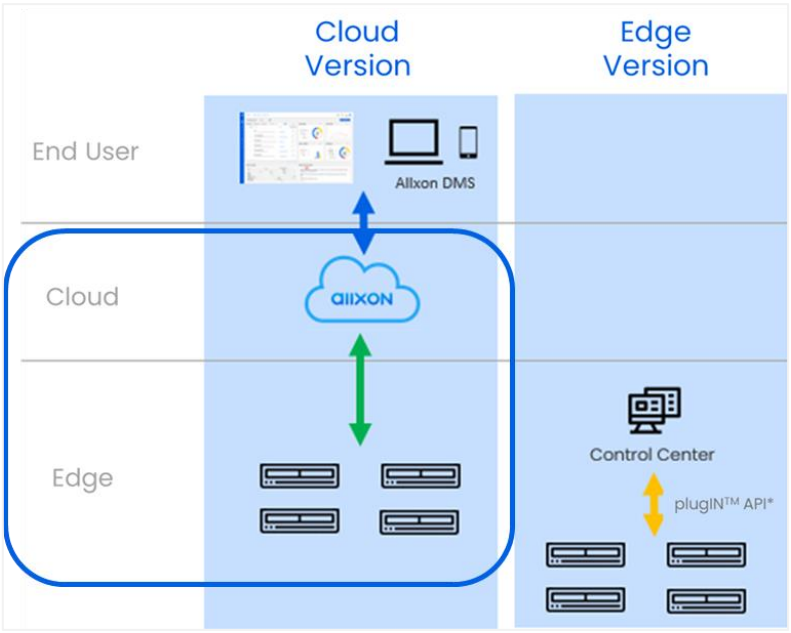


Figure 4. Security between Allxon Cloud and Edge

Secure Communication Tunnels

Allxon uses MQTTS and HTTPS for greater communication security. Allxon enforces secure channels to ensure messages and data in transit are fully encrypted and further secured by trusted certificate authorities (CA). This ensures communication and requests are sent and received by their intended hosts. Allxon uses TLS with HTTP/MQTT to verify servers, clients, and encrypted data. TLS certificate pinning is a method applied to enhance the process of authenticating certificates that are configured on the server. This method of application adds a layer of security during the TLS handshake. TLS certificate pinning is an end-to-end security measure that verifies the identity of the client and the server before completing and establishing a connection. A CA is also enforced to further authenticate all digital certificates issued by SSL and TLS to validate the entities behind certificate requests.

Allxon implements DNS over HTTPS (DoH) to increase user privacy and to secure communication channels. DoH uses TCP to transmit and receive DNS queries from clients. Data transiting between the DoH client and the DoH-based DNS resolver is encrypted via an HTTPS connection on port 443, making it impossible for even ISP to collect personal information related to a client's browsing history or personal

information. Allxon's enforcement of DoH authenticates the origin of DNS data and ensures that sensitive information has not been tampered, eavesdropped, or manipulated in transit by MITM attacks. Using the most vigilant methods to authenticate, verify, and validate credentials, Allxon has built impenetrable communication tunnels for clients and servers to connect, communicate, and exchange data.

Secure Data in Transit

Allxon Cloud enforces SSL/TLS security technology to use public key encryption to secure all data. All digital information that passes through Allxon Cloud is encoded to remain hidden and inaccessible to unauthorized users. With key pairing that is validated by the CA, messages and data are encrypted with public keys and can only be decrypted by private keys holders. Encrypted texts make it impossible for unauthorized users or entities to read the messages. Encrypted texts are only reversible by private key holders.

Allxon also monitors all data activity by using hash-based verification to ensure that important files have not been corrupted. Hash-based verification is an advanced security measure that runs important files through a hashing algorithm to generate a unique string of characters, to ensure all information is accurate and has not been modified during transit. The code serves as a digital signature that is irreversible and only readable by the sender and the recipient.

Security between Edge Device and Local Control Center

Local control centers that operate on a restricted local area network can also remotely manage and connect to their devices using Allxon's plugIN™ API solutions. Allxon offers an SDK that makes it easy for developers to securely set up a connection on their server to their edge devices without needing to share their IoT infrastructure with unauthorized users.

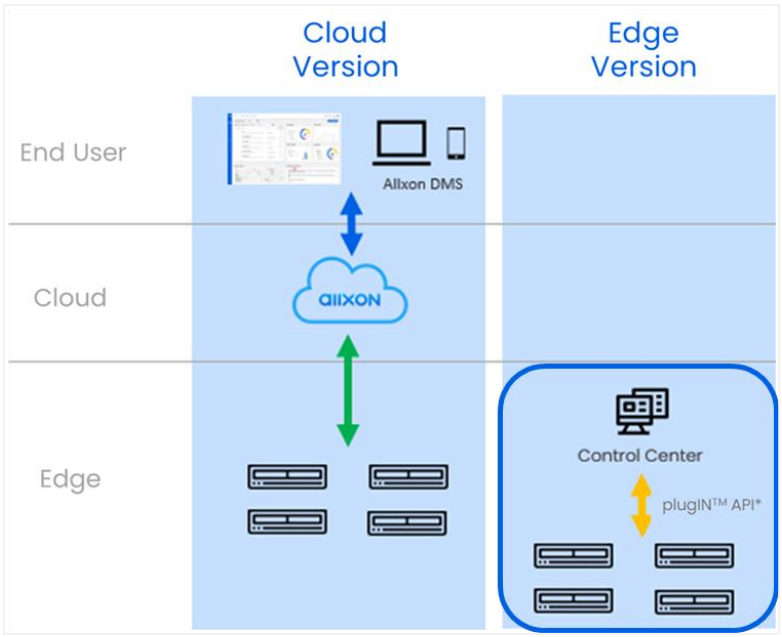


Figure 5 Security between Edge Device and Local Control Center

WSS

Compatible with HTTPS, Allxon offers WebSocket that is secured with TLS (WSS) to create bidirectional communication protocols for clients and servers to interact in real-time over a TCP connection. Developing real-time applications not only establishes bilateral communication, it also shows transparency by monitoring client progress and logins for an added layer of secure access management.

TLS with Client Authentication

Allxon provides TLS client authentication to restrict client access to servers. TLS issues unique client certificates and keypairs on the client's devices to authenticate and grant network entry. TLS client authentication helps secure and protect the IoT infrastructure of a local area network from unauthorized users. This cyber security enforcement makes it impossible for cybercriminals to replay attacks, and renders password or credential theft insufficient to penetrate the system.

Security in Allxon Cloud

As cyber security threats continue to evolve, Allxon ties together the best-in-class security practices to regulate and automate an impenetrable cloud computing system. In its design, Allxon is responsible for building a secure cloud network that is fully compliant with auditing regulations laid out by cyber security directives.

IT Security Standards

Allxon Cloud architects a sophisticated security by design computing platform that is built on cloud facilities and service providers, that uphold international compliance responsibilities, and are qualified with the following security standards:

- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- HITRUST
- MTCS Level 3
- FIPS 140-2
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- ITAR

Vulnerability Scan

Allxon DMS proactively keeps their security in check and reinforces its cyber walls by running a vulnerability scan every quarter. A third-party security provider is used to conduct a full vulnerability assessment that draws out a digital footprint and a precise picture of the network's threat landscape. The security application identifies and creates an inventory of all servers, devices, operating systems, software, open ports, credentials etc. that are connected to the cloud. The vulnerability scanner inspects each item on the inventory against one or more established databases to detect discrepancies and to classify system weaknesses that may be subject to exploitation.

Security at Edge

The hardware, firmware, and software at edge prove to be just as vulnerable as network connections are to cyber attacks. Allxon highly values security in edge devices and implements various verification tools, and runs several security programs to ensure that all digital information and devices are protected from malicious activity.

Hardware Binding Validation

Allxon databases store information on all devices that are connected to their network. Serial numbers (SN) and hardware specifications are used to identify and authenticate connections between servers to edge devices. To prevent data leakages, Allxon DMS software pairs and validates the two components on both ends before enabling any services. If SN and hardware specifications are incompatible, Allxon DMS refuses network access and device management services to edge devices.

Out-Of-Band Module Firmware Security

Allxon consistently creates a resilient computing system by releasing new updates to close security holes and to ensure proper functioning of hardware. While updates keep your Out-of-Band (OOB) module running on the latest firmware model, new cyber security findings and modifications are also taken into high consideration during the developing process of the firmware update. Though upgrading firmware on OOB module to the latest version is necessary to increase security, the data transfer during the updating process also poses potential threats. Allxon addresses this with multiple verification methods that assure firmware on OOB module updates can only be performed and initiated using a unique hardware button that is only accessible to authorized users.

Intrusion Detection

Allxon uses encryption software to prevent unauthorized access to digital information. All files run through a program that generates

checksum algorithms, that use cryptographic hash functions to detect data discrepancies and modifications. Running checksum algorithms is a resilient cyber security feature that detects the smallest changes made during data transmission or storage. Allxon also constantly authenticates the digital signatures of software to verify data integrity and to prevent tampering. In the event of data alteration, where checksums appear incompatible or inconsistent, Allxon runs cyber security software programmes that restores the software.