Logmore system security

Summary

This document describes the methods used to ensure security and validity of all data transferred and stored at Logmore system; web service and QR logger devices.

Description of data flow

Sensor data

Logmore's QR data loggers collect data into internal memory from sensor devices at set interval or based on set rules. Measurement data is stored in the memory until the memory is fully filled up. Once measurement memory is full, logger handles new data based on set mode. Default and most used mode deletes oldest data as new data needs space in the memory. Logging operation can also be configured to stop automatically once memory is full. Memory can be cleared with button press or mobile phone.

The stored data is directly read from the calibrated sensors. Data is scaled to set resolution during the saving operation. Resolution can be different for different temperature ranges. Logger's resolution and the temperature ranges are freely configurable with Logmore web service.

Data synchronization to the web service database

Data that is stored in the logger device's internal memory can be synced to the web service by scanning the QR code seen on logger's screen and by opening the link QR code contains. Measurement data is compressed and encrypted into the link. Data contained in the link can only be opened with secret encryption keys that are stored securely in the web service database. Only information that can be read from the link without encryption keys is the device's serial number. As each device has unique encryption key serial must be included in the link as unencrypted for web service to find encryption key for given device.

Data presentation in user interface and API

The data stored in the secure database can be presented at web service's user interface or API. To receive the data user must be authenticated and authorized to read the data. Unauthorized person or client can't read any information from the system it doesn't have access to.

Data validity

To ensure data validity several methods are used. These methods together make sure all data within the system is real data measured by the sensor and that the data has not been altered at any point of data flow within the Logmore system.

Encrypted incoming data

All data coming into the web service from logger devices is encrypted. Data can't be altered by editing the incoming data without encryption keys. If the data has been altered during logger and web service communication process the web service does not accept the incoming data block. Encryption keys are stored securely in the web service database.

Logger device encryption

Encryption keys are unique for every logger device. Encryption method used for communication between logger and web service is aes128-cbc. The encrypted link data is transferred to web service through encrypted HTTPS-connection. Device encryption keys are strongly random generated during manufacturing process and are securely moved between manufacturing location and web service database through encrypted HTTPS-connection. Encryption keys are only stored within the logger device and web service. In emergency cases person who has admin access to used loggers can request encryption keys from Logmore customer support to open logger's measurement data without connection to web service. In these cases it's user's responsibility to keep the sent encryption key safe.

Data validity in web service database

Once data is received into the web service from logger device the inbound data block is automatically decrypted, decompressed and validated. The measurement data is then saved into secure database system for storage. Stored measurement data is presented in the web service API and user interfaces for users that have access to the logger and it's data. Measurement data that is received into the system can not be edited or altered by users in any way. To ensure measurement data and authorization information security in the communication between user or client and web service the user interface and API always force encrypted HTTPS-connections for all users and clients consuming the data.

Web service infrastructure

The computation, storage and internet connection resources used to run the web service are acquired to Logmore from Amazon Web Services (AWS). AWS is the world's leading cloud computing provider. Resources are distributed across multiple AWS data centers for maximum availability, speed and to ensure persistence of all data in case of emergencies. In custom enterprise deployment cases where AWS is not suitable private instances of web service can be deployed to any data center running suitable hardware and software OS system.

To ensure data persistence in extreme cases where whole AWS becomes unreliable, system is backing up all data every night to non-AWS data center. Before the backup data leaves the secured Logmore AWS environment it is strongly encrypted using secure encryption key.

All the best security practices are used system wide to minimize security risks involved running system that's components are communicating through internet.

System is constantly monitored to prevent and notice performance issues, anomalies, invalid data or attacks.

Authentication

Users or system clients consuming data or user interfaces provided by web service are always authenticated. Authentication is implemented through Logmore account system that works through Auth0 identity provider platform. Auth0 system is ISO27001 and ISO27018 certified by a third party and has completed a full third-party SOC 2 Type II audit. Auth0 is also compliant with HIPAA BAA and EU-US Privacy Shield Framework and has achieved a Level 2 audit Gold CSA Star certification for its cloud service security capabilities

Software security and quality

Web service system is built in-house by Logmore's developers. All development takes place in Finland. Best development practices are used when developing the software to ensure the security and quality. System is constantly improving and every change is thoroughly tested to make sure system has no security vulnerabilities or quality issues.

In case of issues

Last additional layer of security comes from acknowledging that no system is perfect. Logmore's operations staff are monitoring the system around the clock and each person has been trained to act upon any issues occuring in the system.