IoT International

IoT INTL

rIoT Engine and SkyView Security

Role-Based Security
Access Control Based on the User Role

OAuth Framework
Token Based Security to Control Users' Access

TLS
Transport Layer Security to Protect Data in Travel and Maintain Data Integrity

Edge Data Integrity
Hashed and Encrypted Local Data at the Edge

The realtime IoT suite (rIoT) has three main components:

- Edge component or rIoT Engine: rIoT Engine is the actual integrated realtime communication module that is running on the edge. The Engine can run on both Windows and Linux platforms and is hardware agnostic. rIoT Engine can provide server interfaces to other systems to consume data locally. For example, the Engine can provide a DNP3.0 server interface to pass data to a local RTU, PLC or SCADA system, functioning as a realtime data hub.
- Time series is to receive, collect, save and serve time series data generated in the field. Time series can be an IoT platform such as Amazon, Azure, AT&T, IBM or just a SQL based database.
- SkyView: The presentation and configuration layer to configure devices, design and render HMI pictures, configure and render displays and charts, develop and publish interval reports, sequence of events, geo-intelligence, alarms and notifications.

Edge Security: Edge security is implemented where data is collected in the field.

Some of data communication protocols are more security mature compared to the other ones. rIoT Engine implements the security measures built into the protocol. In addition to the local data communication protocols, the rIoT Engine has the following built-in features:

- Local data saved in the Engine is seeded and hashed to ensure privacy and integration
- Local or remote configuration, debug and troubleshooting messages between the user computer and the Engine is implemented via a secure channel

Transport Security: Data in transport from the Edge to the Timeseries platform is secured by Transport Layer Security (TLS) protocol. Using TLS technology, the two sides negotiate a stateful connection by using a handshaking procedure. They establish a shared key which is used to encrypt the data in transport. During this handshake, the two sides agree on various security parameters.

IoT International

IoT INTL

Advanced Security Technologies

Two-Factor-Authentication

SMS Codes to Users' Mobile Devices to Authenticate the Users

Secure API's

Secure API's to Access Platform Data

Egress Only

Egress only, Data Diode Architecture to Send Data Unidirectionally

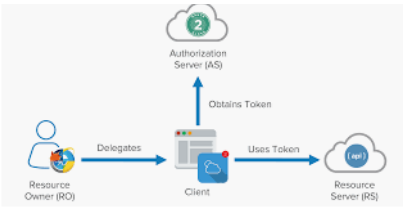
Role and Responsibility: SkyView implements Role Based security in accessing platform resources. In addition, by allocating the users to different roles, system messages and notifications can be routed to the right people. SkyView defines three level of access:

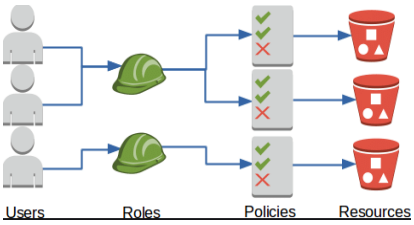
- Manager: Manger has access to the account level resources such as adding or removing an account. In addition, the Manager can add or remove the Admin users
- Admin: Admin users can add, modify or remove system artifacts and resources such as devices, HMI screens, charts, reports, etc. They can add, remove or modify regular users.
- Regular User: Regular users can only view the artifacts developed and added by Amin users. We can also allocate the users to different groups to filter the notifications they receive.

Data Integrity: It is paramount to be able to trust the data before relying on it. The Timeseries platform provides a long security key that is used by the Engine when it pushes data to the platform. If the key does not match with the information saved at the service, the data is not accepted by the platform.

User Authentication: It is important to make sure only authorized uses have access to the data. SkyView provides two-factor-authentication to authenticate the users. If the user opts in, they receive a SMS with a code any time they try to log in. Only after successfully entering the code they can log in the system. OAuth Authorization Framework is used to authenticate the user to the platform. Using OAuth, users are granted limited access to the system without exposing their credentials. OAuth is a token-based system i.e. the user asks for an Access Token from an Authorization Server. The token is then provided to the recourse server to access the resource. The token will expire with time or can be revoked.

Egress Only: For the majority of applications, an egress only scenario is preferred. In this architecture, data is sent to the cloud platforms unidirectionally. Any control command is to be initiated and executed on the premise. rIoT platform is a perfect fit for this situation, as the edge gateways need to have only an outbound port connection. In traditional systems that the data is concentrated on the premise, it is a huge challenge to secure the incoming connections to query the data and keep track of all the security patches and updates.





IoT INTL

IoT International

(443) 718-0240
10015 Old Columbia Rd
Suite B-215
Columbia, MD 21046
www.iotintl.net