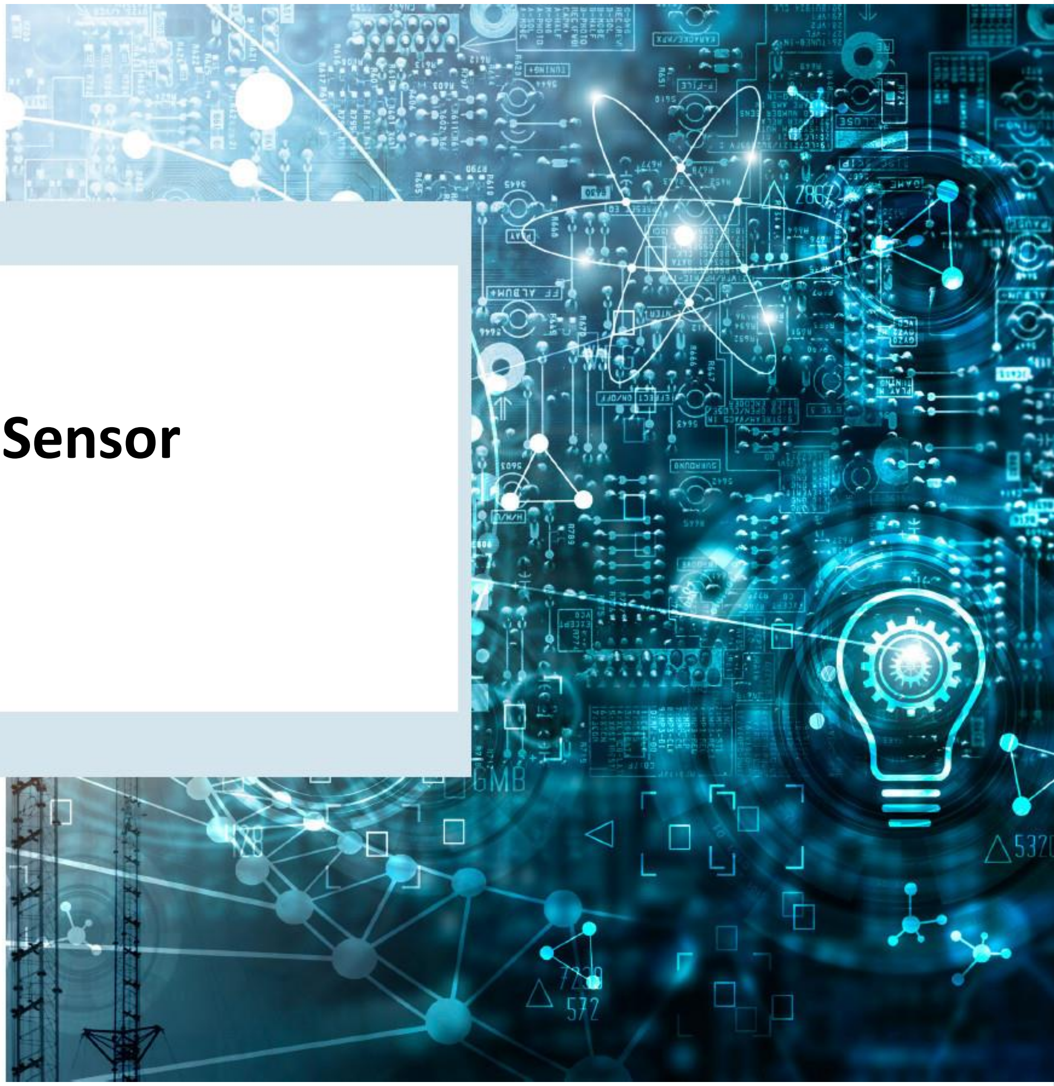
CHIPKIN

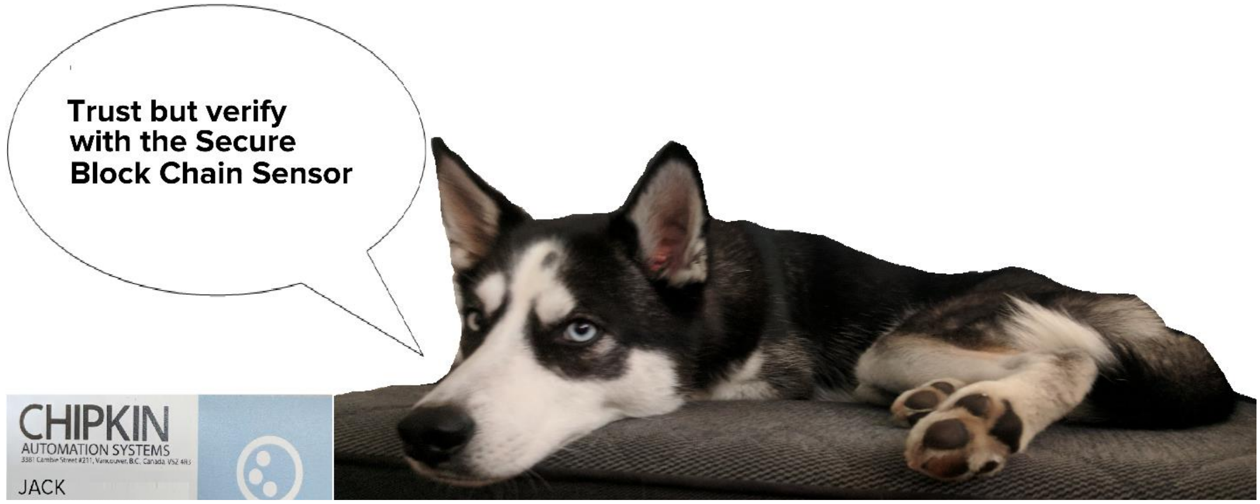


White Paper

Secure Block Chain Sensor

Abstract

What is the value of knowing a data objects's present value without having the measure of its quality. Many characteristics and attributes of data contribute to the evaluation of its quality and yet all too often data is treated as a simple scalar value – the present value is monitored or logged and the measure of quality not even considered.


Trust but verify with the Secure Block Chain Sensor
CHIPKIN
AUTOMATION SYSTEMS
3381 Cambie Street #211, Vancouver, B.C. Canada V5Z 4R3
JACK

This paper discusses the functional and physical components of a sensor that delivers data as an object with both a measure value component and a quality component. It's possible to avoid having to deal with the many measures of quality that are qualitative and subjective and still deliver data with higher quality. This is a valid endeavor.

One important measure of Data Quality is its 'Validity' and one component of 'Validity' is trust worthiness or provenance, to borrow a term from the antiques world. Provenance means "a record of ownership of a work of art or an antique, used as a guide to authenticity or quality."

The block chain is essentially a provenance technology. Data provenance is less important when the data lives in a secure and controlled environment – like within a corporation. But that model is unavailable in the world of outsourced services and downstream suppliers.

Quality of Data

There are many ways of categorizing the quality components of data. The categorization below is one of many valid models.

The seven characteristics that define data quality are:

1. Accuracy and Precision
2. Legitimacy and Validity
3. Reliability and Consistency
4. Timeliness and Relevance
5. Completeness and Comprehensiveness
6. Availability and Accessibility
7. Granularity and Uniqueness

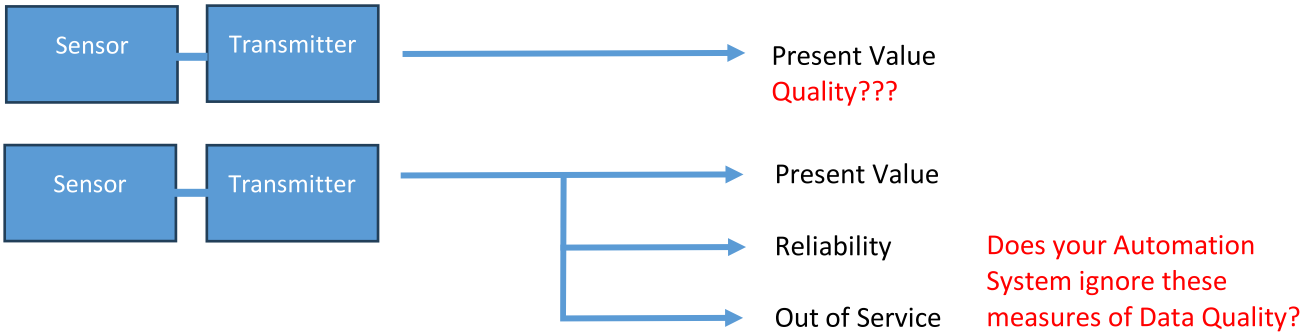
It's extremely important to understand that the intended use/application of the data has a powerful effect on how the attribute is defined/quantified. For example. Because of the slow response time of heating and cooling systems, even if 1% of a temperature sensor's readings were up to 50% inaccurate it would probably have no noticeable effect on the temperature of the space being heated or cooled.

When one layers new applications on older installations it is possible that the quality does not meet the requirements of the new application.

Quality is engineered not accidental

An Analog Input data object in BACnet has a property called ‘Present Value’. The thoughtful designer of the protocol also added a property called “Reliability” and another called “Out of Service”.

Good engineering practice considers the state of both quality properties in making decisions on how to use the ‘Present Value’. Bad engineering practice ignores the quality and uses the ‘Present Value’ unconditionally. The presence of quality data does not automatically lead to quality data.



Does your Automation System ignore these measures of Data Quality?

Validity Issues for a Secure Sensor

The ‘new’ issue when it comes to data quality is its validity or trust worthiness. It’s not the scope of this article to discuss issues like repeatability, precision etc.

These are the 4 validity issues that a Secure Sensor can address.

1. Is this device still in the same location?
2. Is there a change to the operating conditions?
3. Is there a change to the ‘usual internal state’?
4. Has the data been altered in an unauthorized way?

Location

Accelerometer – movement:
An Accelerometer can be used to measure vibration, distance, and acceleration; a change in value could indicate possible damage, external or internal. Vibration and distance would indicate a change in environment, location or “outside temp etc” while acceleration would indicate a physical change.

GPS – rough grained location
A GPS can be used to constantly monitor the sensors’ location.

Strain Gauges – stress from removing from mounting, movement sensing may be possible.

A Strain Gauge is a sensor whose resistance varies with applied force. When external forces are applied to a stationary object, stress and strain are the result caused by external influences. Strain Gage measurements could be used to see if the sensor has been moved. The physical act of removing the sensor would cause a change in force, tension, and weight which would be converted into resistance.

Screws and Bolts

Tamperproof screws and bolts have security fasteners that provide an extra level of security, through their design, which prevents removal using ordinary screw drivers. Only people with the very specific screw drivers would be able to unmount the device.

Light Sensors
Light Sensors detect the current ambient light level. A change in light level could indicate an object nearing the sensor or a change in location of the sensor.

Change to Operating Conditions – External State

Temperature internal and external

A temperature sensor is a device that measures temperature though electrical signals and can be used to detect environmental changes. If the temperature fluctuates rapidly or changes by enough in a short amount of time, a signal can be sent notifying the 'owner?' that there has possibly been a change in the environment.

Infrared sensing – usual thermal context

A Passive Infrared Sensor is an electronic sensor that measures the infrared (IR) light radiating from objects in its field of view. It can be used to detect objects nearing the and possible damage approaching.

Noise sensor

A noise sensor could be used to detect whether an object or animal has approached or hit the secure sensor by picking up the noise around the sensor.

Pressure Pads

Pressure pads measure the forces exerted between any two objects. It consists of multiple sensing elements that are arrayed on or within a flexible cushion that maps forces between contacting surfaces. It could be used to detect if someone was to try and remove the device.

Passive Infrared Sensors (Motion Detectors)

A Passive Infrared Sensor is an electronic sensor that measures the infrared (IR) light radiating from objects in its field of view. This would help detect if any object was approaching.

Switches

Switches are used to detect the opening of a device, the breach of a physical security boundary, or the movement of a particular component. If someone tried to open the device, the owner would be notified immediately.

Circuitry

Flexible circuitry, nichrome wire, and fiber optics wrapped around critical circuitry or specific components are used to detect a puncture, break, or attempted modification. For example, if the resistance of the nichrome wire changes or the light power traveling through the optical cable decreases, the system can assume there has been physical tampering.

Usual Internal State

Power source monitoring
Power source monitoring could be used to act as a power supply alarm system that monitors all key functions and reports any changes.

Software diagnostics
Software diagnostics would help locate a problem within the software and/or hardware which would allow for accurate conclusions about possible changes in the sensor.

Unauthorized Alteration of the Sensor

Firmware hash verifications – firmware is what you expect it is.

Hash verification guarantees the integrity of the firmware; it ensures that the package contains the originally generated artifacts and has not been altered. The crypto hash of each element is stored in a file inside the firmware update package. At time of installation, all elements are extracted and their hashes is compared with the stored hashes. If any are different, the update process is aborted ensuring that all files are the same as before.

Identifier hashes – Serial numbers and other signature data from active electronic components are hashed.

If components have digital signatures, an unauthorized alteration with the sensor could be detected by a different hash being used to do so.

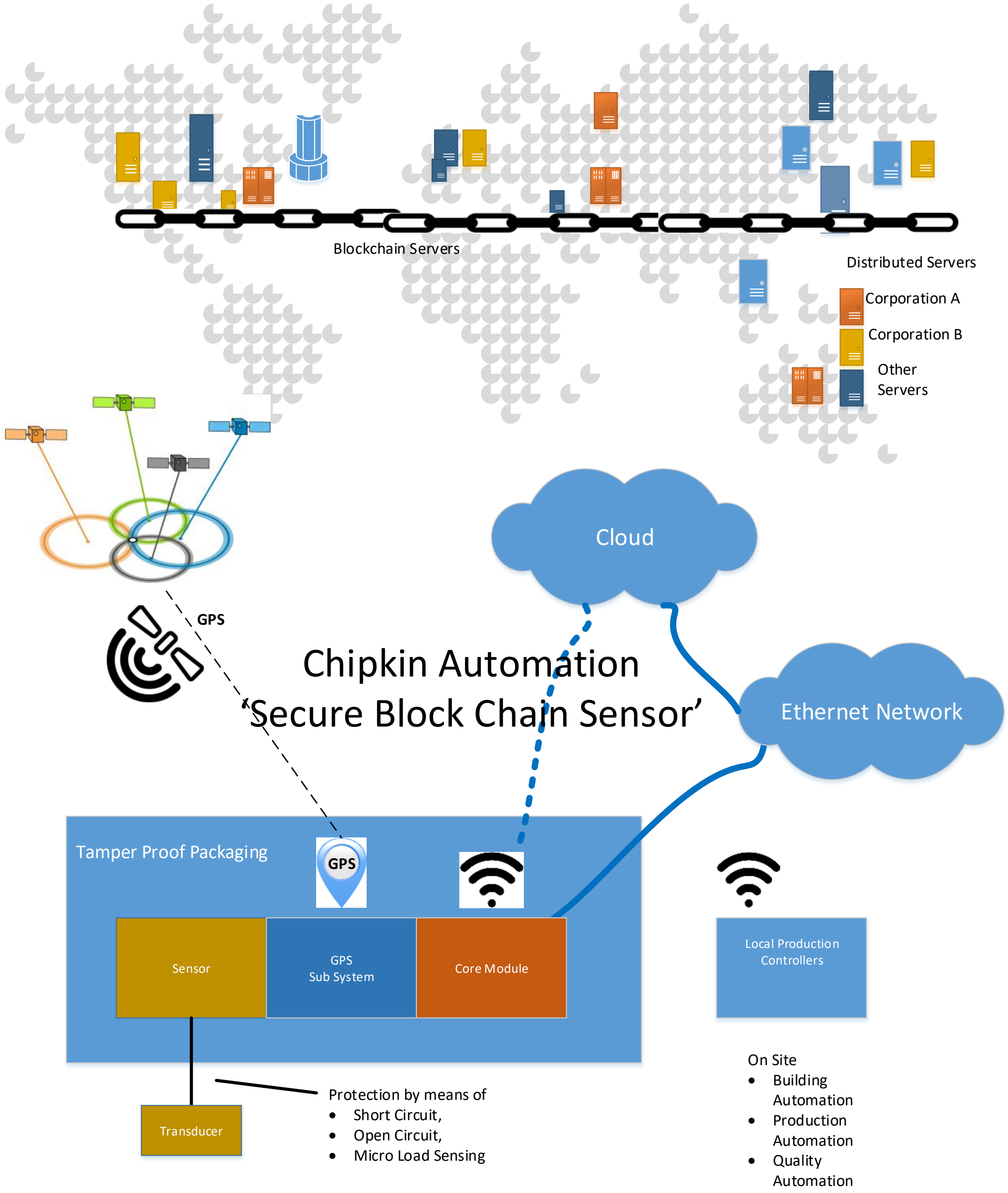
Unauthorized Alteration of the Data

Encryption
Encryption would keep all the data private and secure making it so no one without access could change any.

Initialization
To start the device, a specific code or hash would be needed making it impossible for anyone without the code to start the device up.

Authentication
Only certain personnel, who pass the user authentication, would be able to see and/or alter the data.

Secure Protocol – pull not push.
Using a secure protocol, the client would be able to periodically connect to the server to see all the recent events and in doing so would be able to see all data alterations.



Protection by means of

- Short Circuit,
- Open Circuit,
- Micro Load Sensing

On Site

- Building Automation
- Production Automation
- Quality Automation