Secure IoT Platform for Industrial Control Systems

ABSTRACT

Supervisory control and data acquisition (SCADA) systems, are part of industrial control system (ICS), have been playing crucial roles in real-time industrial automation and controls. Through the evolution of 3rd generation, or networks based system, SCADA systems are connected to almost types of networks such as wired, wireless, and cellular and satellite communication, but security is still a big challenge for SCADA system while communicating within. Internet of things (IoT) is a ubiquitous platform, a new advance enhancement, for efficient SCADA system, where billions of network devices, with smart sensing capabilities, are networked over the Internet access. Deployment of smart IoT platform, SCADA system will significantly increase system efficiency, scalability, and reduce cost. Security is still a major issue for both-, as they were initially designed without any priority and requirements of security. This study modeled IoT-SCADA system and deployed a security mechanism, employing of cryptography based algorithm, which provided a secure transmission channel while each time communication occurred, between the field devices in the SCADA system. Proposed security implementation, and computed measurements analyzed as potential security building block against authentication and confidentiality attacks.

EXISTING SYSTEM

Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery. The operator interfaces which enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA supervisory computer system. However, the real-time control logic or controller calculations are performed by networked modules which connect to the field sensors and actuators.

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers allowing access through standard automation protocols. In practice, large SCADA systems have grown to become very similar to distributed control systems in function, but using multiple means of interfacing with the plant. They can control large-scale processes that can include multiple sites, and work over large distances. It is one of the most commonly-used types of industrial control systems, however there are concerns about SCADA systems being vulnerable to cyber warfare/cyber terrorism attacks.Both large and small systems can be built using the SCADA concept. These systems can range from just tens to thousands of control loops, depending on the application. Example processes include industrial, infrastructure, and facility-based processes, as described below:

- Industrial processes include manufacturing, Process control, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electric power transmission and distribution, and wind farms.
- Facility processes, including buildings, airports, ships, and space stations. They monitor and control heating, ventilation, and air conditioning systems (HVAC), access, and energy consumption.

  However, SCADA systems may have security vulnerabilities.

DRAWBACKS

- Security problems are more.

PROPOSED SYSTEM

The manufacturing sectors or/and industrial sectors are very common sectors that develop to fulfill the demands of industries, such as Oil, Gas, Water/Wastewater, Electric, and others. In past two decades, there have been several enhancements accounted in term of remote information carries, and system monitoring and control, through integration with IP-centric network technology. Moreover, nowadays, the uses of Internet of things smart technology with the existing network-based industrial infrastructures, several enhancements have made that

enables more efficiency, system scalability, performance accuracy, capital saving and others, in industrial systems. With these enhancements, and employing of IoT and open IP networks, information security is a big challenge which has not been considered in the initial designing of industrial systems, including industrial protocols designing, as well security is also not a part of IoT initial designed. Therefore, by examining IoT potentials in areas of industrial sectors or especially in SCADA systems, this study first reviewed, the IoT and SCADA system as a part of industrial control system, or IoT-SCADA system, and then analyzed security issues that have been residing in. To overcome the security issues, a cryptography based security mechanism which implementation was significant in the protection of information while exchanging between several connected devices within the premises of IoT-SCADA system. The measured results were good enough to protect the IoT-SCADA system information while traveling over open networks or/and the Internet but limited to secure the IoT-SCADA system against authentication and confidentiality attacks.

ADVANTAGES

- Increase system efficiency and scalability.
- It reduces the cost.
- It provides security.

SYSTEM EQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X
- Programming Language : Java
- Java Version : JDK 1.6 and above