Secure IoT Platform for Industrial Control Systems

AAmir shahzad
Department of Computer and Information Security,
Sejong University,
Seoul, South Korea
mail2aamirshahzad@gmail.com

*Young-Gab Kim
Department of Computer and Information Security,
Sejong University,
Seoul, South Korea
alwaysgabi@sejong.ac.kr

Abulasad.Elgamoudi
Department of Sciences, Computer Sience,
Al Zawiya University
Libya
Elgamoudi69@gmail.com

***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.**

Keywords—Internet of things, Industrial control system, Supervisory control and data acquisition, Programmable logical controller, remote terminal units, and Advance encryption standard Introduction

I. INTRODUCTION

Industrial control system (ICS) is an important term, which has been dedicating for monitoring and controlling of industrial infrastructures such as Oil, Gas, Manufacturing, Electricity and Transportation, and others, mainly combined with the most prominent control systems, such as the "supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS), often employed in several industrial sectors of current era. ICS mainly deployed in the industries to control the overall structure of production plant, or other employed equipment's, to produce the desired production goals as according to specifications and requirements, through employing of several control components, varies according to industries specifications and performance paradigms, that consolidated together for producing of output. The ICS, however, have been designed and networked to provision the controlling functions that are may fully automated in controlling of the overall structure of sectors, such a transportation controlling and other areas like oil industry, or these controlling systems are self-control by individual or human in case of manual operational mode[1-4]. Eventually, Industrial control system uses several control components and required network (or system) configurations and setting of sensors, actuators and programmable logic controllers (PLCs), also including system controlling loops, diagnostics and maintenance equipment, graphical interfaces or human machine interface (HMI) and proprietary and non-proprietary protocols such as DNP3, Modbus, TCP/IP , UDP and others. ICS deployed system is usually controlled by one or more controllers (or control loops), however, overall system information is manipulated bases on the system specified set points between various networked equipment or sensors, with the usage of proprietary or/and non-proprietary protocols and functional control algorithm that controls these set points[1, 2].

A. IoT and SCADA System

Internet of things (IoT), is another advance technology in IT sector, provides internetworking for numerous of devices such as sensors, actuators, PLCs and other electronic embedded smart devices and controls, and various software's' and provides systems network configuration and connectivity, which enables communication between these numerous devices for information exchanging [5-7]. Nowadays, IoT is one of the most advanced, efficient, and cost less technological solution which encompasses various hardware and software resources; and allows remotely connected sensing devices to sense with more capabilities, provides efficiency and can be monitored and controlled through deployed of existing systems or infrastructures, resulting the physical World integration with computer controllers (or systems). As IoT provides interconnectivity among various real-time sensing sensors and PLC and other intelligent devices, therefore this technology will be an entity indicated for the more advance cyber-systems encircling the significant developments, "such as smart grid, smart vehicle systems, smart medical systems, smart cities, and others smart systems." In early future, IoT has striven to provide advance or smart connectivity for variety of electronic and intelligent equipment's or devices, IT-based systems and the more advanced services through deploying of various traditional and real-time protocols, networks domains, and system software/hardware applications, which will be an work followed by machine-to-machine technological concept. Through interconnection of various devices and managing of

*Corresponding Author

978-1-5090-5140-3/17/$31.00 ©2017 IEEE

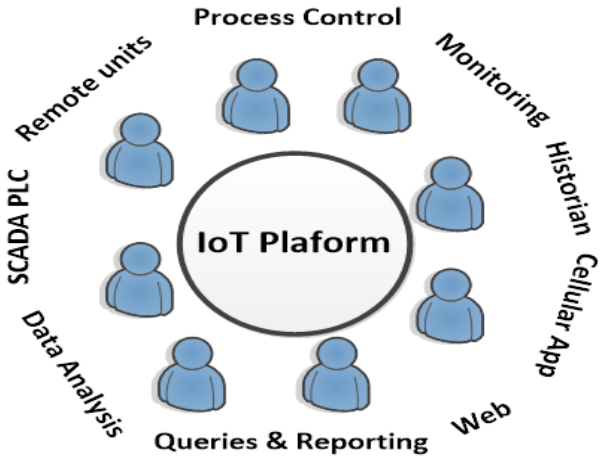

Fig. 1. IoT platform for SCADA system

applications for remotely monitoring and controller, the IoT becomes a tremendous development in the arena of industrial control systems (ICSs), or for real-time industrial infrastructures, including SCADA systems [7]. Figure 1 shows the typical IoT applications platform for SCADA system.

The rest of paper is organized as follows. In Section 2, detail literature is conducted base on the existing IoT and SCADA systems applications, and relevant security issues. In Section 3, proposed IoT_SCADA system is networked with various functional nodes and security solution is implemented using cryptography. Performance results are computed, and discussions are made in Section 4. In the end, study conclusion and future work are discussed in Section 5.

II. Literature Survey

IoT is a system defines an environment that encompasses numerous of objects; sensors that connected with these objects are accessible over the Internet through employing of various networks connections, such wired or wireless. IoT can be able to carry information from various embedded sensors attached with the physical World, human and any inanimate object, and then transmit them to a system for further analyses. In early future, IoT will be able to connect almost components or parts of industrial infrastructures, smart medical telemonitoring systems, and smart transportation systems; and will provide the information sharing facilities in order to make systems and peoples always updated [7,8,9]. In existing, almost industrial systems were setup with the equipment's, having instrumentations heavily weighted, through massive size wired connection, much expensive deployed sensors, local system controllers, and wired system networked, that would not be upgradable or replaceable due to the higher cost requirements. However, in last two decades, there are changing taken placed in designing of IP-based industrial systems and now IOT is a solution to overcome the future cost relevant with industrial equipment's, sensors, system controllers, and systems communication, through sharing and transmitting of information with other connected similar objects, as part of IoT environment[7,10,11]. Further few ICS popular organizations, such as DNP3.org and Modbus.org, taken intentions on security mechanism requirements that to fight against the security challenges arising in IP-based communication and Internet communication [3, 7].

More advances of IoT toward the industrial systems, IoT is an important element of Industry 4.0 a new revolution in smart industrial sectors that provides advanced automation and sharing information facilities during manufacturing and is designed with the connectivity of IoT, cyber systems, and cloud computing. Through this, industrial systems will be networked by using of machines, or sensors, representing as smart, intelligent network systems that have the ability to communicate with other system nodes and control with self autonomously without interception of system operator's assistance and monitoring. A report by "Bosch, GE and Johnson," the smart design of an industrial system based on IoT concepts, the network devices can able to make predictions while some failure cases are occurring in part of machines, and would be efficient in step to take action independently of the issues without the involvement of system maintenance individuals. Further, self-organized management and administration is another feature of IoT. Therefore the system will smart enough to accommodate the sudden changes, such raw material or material inadequacy and blockage, arising in industrial automation and processes [8]. As a consequence, IoT is a sight for provisioning an efficient, scalable, and more important smart automotive environment for industrial productions, and anticipates the following connectivity values [8]:

I. Information Access: IoT provides the best way to improve the business, and its activities by connecting the industrial individual in order to update them with the right information, automation and processing information, machines performance, and system failures and alerts, which will be also accessible through cellular devices having industrial access application installed within, with lower service cost [3, 8].

II. Process and Functional Flow: In the start of each process, or considering the IoT platform, industrial manufacturers always require process visibility by their requirements, and base on supply chain issues; and might use other existing management ideas to initiate the development. If these cases happen, IoT platform can be prevalent to enable the manufacturers having with speedily information and analysis flows, and achieving potential market feedback in both system operations and software business tasks through devices connectivity. Moreover, machine-to-machine (M2M), also considering as 4th generation of SCADA system after 3rd generation called network based SCADA system, in industrial control systems can able to consolidates within IoT computing environment [8,12, 13].

III. Newly Data presentation: IoT is specifying a new concept regarding data, the newly types of data will be presented through employing of new equipment, replacing existing devices that networked in industries. Typically, IoT enables almost types of physical devices, such as sensors, PLCs, visual cameras, actuators, and other smart physical devices, to connect to the Internet and also with each other. When information collects from devices, then examine through IoT analytic tool, resulting as an insight for the users and industrial machines to make more appropriate and useful opinions about.

III. System Setup and Implementation

Nowadays, industrial systems and their automation are accessible and control through deploying of the IP-centric network, thus the information will be collected from anywhere, where the remote industrial stations are setup having various electronic devices, such as terminals units, PLCs, and intelligent sensors [14]. To design and model an Internet of thing based generic industrial control system, or IoT-SCADA system, few common parameters have to be considered:

- Efficient and smart network selection,
- Protocol selections for reliable communication,
- Efficient and scaled software's selection for information collection, monitoring, and control,
- Generic security mechanism for information protection,
- Smart network intrusion detection solution,
- Information analytics and performance monitoring,
- and Historian, respectively.

To fulfill the target goals of the study, IoT_SCADA system is setup where numerous of devices are connected with each other through secure channels. In figure 2, the IoT_SCADA system is modeled and setup, which encompassed six main functional parts, such SCADA main controller or control center with human machine interface, remote station, historian, reporting and maintains, data analytics, and user devices, connected through the internet of things (IoT) platform over the Internet. As mentioned, SCADA system is also connected to the Internet. Therefore many of its units or stations are networked at the geographical locations, and monitor and control from the control center. A terminal unit, in below figure 2, is connected remotely, setup to retrieves information from sensors that directly linked to the physical World. The carry information is continuously transmitted, and monitors at the control center, and detail information or data analysis is performed through employing of IoT analytic tools. At the same time, continuous receiving information is stored in historian and reporting will be carried out upon users' requests, end-users or/and cellular mobile users can also access the overall real time information of SCADA system as an authorized user through IoT. Each time, in IoT_SCADA system, communication will be initiated between the participated nodes (or parts), end-to-end cryptography mechanism, advance encryption standard (AES) algorithm, will deploy which provide a secure channel while information traveling over the Internet, or from/to participated nodes.

As mentioned, the IoT is a critical component for the industrial control systems (ICSs), or smart industrial manufacturing. The industries, such as oil, electric, water/waste water, and gas, have been achieving their productions through deploying of sensors and controlling from the computerized controller [14,15]. As most of industrial based systems, employing sensors, actuator, PLCs, and other controlling and monitoring facilities, were limited and not connected to the Internet. In SCADA system, typically, the hierarchical structure of the system is defined in advance. Therefore the overall system scope is limited as a part of industry uses, and disconnected with the advance and open IP networks that provide extensive connectivity with other network systems, over the Internet access. However, with the evolution of IT and Internet-based technology and more advanced the IoT, industrial system have made tremendous advance changes regarding technology development and information transformation and controls. At the same time, the advance transitions of legacy systems toward the non-proprietary networks and deploying of Internet for information sharing and uses of smart IoT application and services, the industrial system, or SCADA systems, are facing several communication challenges, and the most important one is security. As almost industrial systems, and their employed protocols designs were designed without any security concerns in mind, but security has been a very critical issue, as these systems are naturally defined as critical infrastructures that information's are also critical as well.

As a consequence, to resolve the underlying security issues of IoT_SCADA system, advance encryption standard (AES) cryptography algorithm is considered against security issues (or attacks). The proposed security solution uses a single key, called symmetric/secret key, generated by AES algorithm with time_session. Numbers of secret keys are generated and distributed among the nodes statically that to avoid the requirements of the certificate authority (CA), and stored in historian using MySQL tool. Therefore, each time communication is occurring between the system nodes,

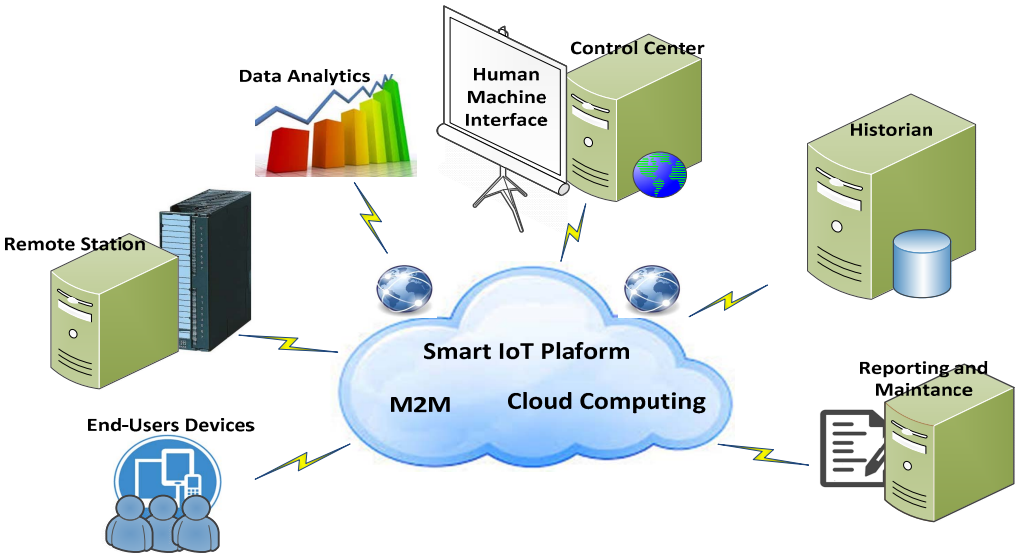

Fig. 2. Proposed IoT_SCADA system

encryption at receiving side and decryption at target side are performed using same key called secret key, with time_session, shared between participated nodes. The proposed security solution provided a secure solution against authentication and confidentiality attacks for IoT_SCADA system.

IV. Results and Discussion

In study, IoT_SCADA system and its parts, illustrated in figure 2, are all considered as nodes which are connected with each other's for communication or information exchanges. Each time, communication has been occurring between two or more nodes, a secure channel is used established by AES algorithm with the session. Meaning that, every time, shared key between sender and receiver nodes is encrypted/decrypted with specified session consolidated with, communication is performed. In figure 4, 50 times random size packets are transmitted between the IoT_SCADA system nodes (i.e., control unit and remote unit), and each packet is transmitted by encrypting with secret key having session (life session) of 20 seconds and at the target node used same shared secret key for decryption. In case, session of 20 seconds will be expired then the new secret key will generate that encrypt with existing

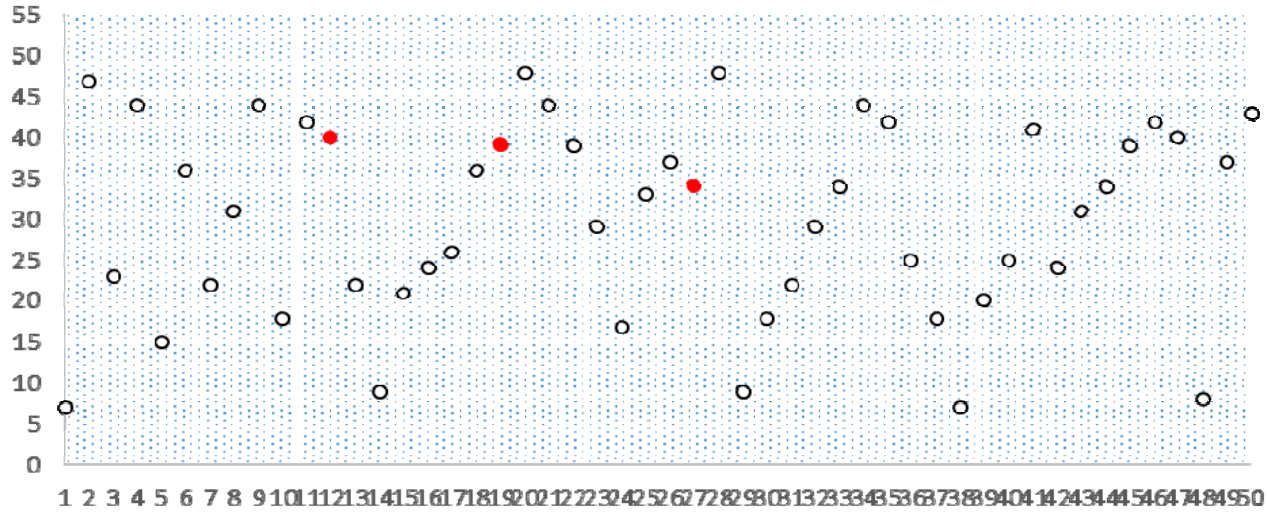

Fig. 3. IoT_SCADA system: Normal traffic with packet lost

```
<~~~ Main Controller
FIR(1) FIN(1) SEQ# 0
c0 c1 15 3c 02 06 3c 03 06 3c 04 06
<--- Main Controller
LEN(17) DIR(1) PRM(1) FCV(0) FCB(0) DEST(4) SRC(3)
05 64 11 c4 04 00 03 00 4e ef
c0 c1 15 3c 02 06 3c 03 06 3c 04 06 94 43
<~~~ Remote Unit
FIR(1) FIN(1) SEQ# 0
c0 f0 82 90 00
<--- Remote Unit
LEN(10) DIR(0) PRM(1) FCV(0) FCB(0) DEST(3) SRC(4)
05 64 0a 44 03 00 04 00 7c ae
c0 f0 82 90 00 43 a2
---> Main Controller
LEN(10) DIR(0) PRM(1) FCV(0) FCB(0) DEST(3) SRC(4)
05 64 0a 44 03 00 04 00 7c ae
c0 f0 82 90 00 43 a2
~~~> Main Controller
FIR(1) FIN(1) SEQ# 0
c0 f0 82 90 00
```

Fig. 4. Communication flow

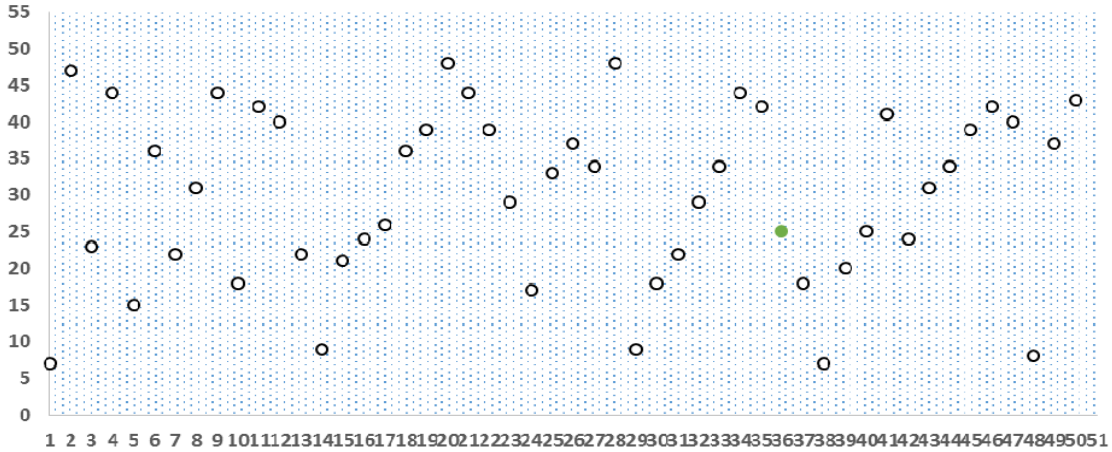

Fig. 5. IoT_SCADA system: Abnormal traffic

secret key in order to avoid the authorized entity inside the communication. However, in performance figure 3, only 3 times packets, from a total of 50 times, are lost. Meaning that transmitted 3 packets, having random bytes, are lost, or not fully received, due to network or configuration errors. Thus, the computed measurements shown in red colors are representing the lost packets, and the remaining showed the packets which transmitted successfully without any error. In figure 4, sample communication flow between the main controller and the remote unit is illustrated [14].

In performance figure 5, same number of experiments (e.g., 50 experiments) are performed, and attacks such "guessing shared key, brute force, eavesdropping, key cracking, and man-in-the-middle" are launched by employing of built-in attacks tools such as "cracking tools, sniffer, ethereal, key cracking tools, and ettercap," and attack tools [2, 14].

Through the attacks scenario, the level of attacks is accounted to check the performance of deployed security algorithm. As a result, only one-time attack, represented in green color, is fully intercepted inside the transmission, but the remaining 49 experiments packets are securely transmitted between participated nodes. In performance figures 3 and 5, the x-axis shows the number of experiments performed to compute the measurements and y-axis show the number of random bytes contained in each packet. The measured results concluded that the proposed security solution has potential enough to secure the IoT_SCADA system against authentication and confidentially issues or attacks.

V. . Conclusion and future work

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.

In future, a generic model for IoT-SCADA system will be designed where numerous of devices will network in order to exchange information within secure channels, developing with cryptography mechanisms that will have potentials to fight against IoT-SCADA system insecurities.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R7115-16-0002, Wise-IoT)

REFERENCES

[1] S, J., K. K., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,” Recommendations of the National Institute of Standards and Technology, 2006

[2] M, S. A, “Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security,” Proceedings of the 7th International Conference, 2013

[3] S.A et al., "A New Cellular Architecture for Information Retrieval from Sensor Networks through Embedded Service and Security Protocols." Sensors 16, no. 6 (2016): 821.

[4] SCADA system, https://en.wikipedia.org/wiki/SCADA

[5] J.G., J.L, “SCADA communication and security issues. Security and Communication Networks”, 2013

[6] Internet of Things, https://en.wikipedia.org/wiki/IoT

[7] IoT and SCADA: Complimentary technologies for Industry 4.0.

[8] Lopez Research LLC, “Building Smarter Manufacturing With The IoT,” 2014

[9] R., P., J. L, "Securing the Internet of Things, in Computer,: vol. 44, no. 9, pp. 51-58, Sept. 2011.

[10] ICON LABS, “Secure the Internet of Things,” http://www.iconlabs.com/prod/internet-secure-things

[11] R.M et al., "Security in the Industrial Internet of Things," 2016

[12] Harbor Research, Inc., “M2m & Smart Systems,” http://www.windriver.com/m2m/edk/Harbor_Research-M2M_and_Smart_Sys_Report.pdf, 2014

[13] M.B et al. , Project Proposal, “Securing the Internet of Things,”https://sites.google.com/a/onid.oregonstate.edu/477-project/project-proposal, 2014

[14] S.A et al., “A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks,” Sensors 2016, 16, 322..

[15] L.A, A.I, G. M, “The Internet of Things: A survey,” Computer Networks, Volume 54, Issue 15, Pages 2787-2805, 2010