Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 2, November 2021, pp. 780~788
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i2.pp780-788

A cloud based 3-tier data security framework for industrial internet of things

Mirador G. Labrador[1], Abegail Bordios[2], Weiyan Hou[3]
[1]Center for Engineering, Science and Technology & Innovation, Samar State University, Catbalogan. Philippines
[2]College of Education, Samar State University, Catbalogan, Philippines
[1,3]School of Information and Communication Engineering, Zhengzhou University, Henan, China

Article Info

Article history:

Received Jan 19, 2021
Revised Sep 12, 2021
Accepted Sep 17, 2021

Keywords:

3-tier data model
Cloud based security
Field control system
Industrial internet of things
Security framework

ABSTRACT

The convergence of microelectronics and micromechanical system within a sensing device, the proliferation of wireless communication, and the use of software-driven equipment are already changing the landscape of the manufacturing industries. This situation compels the industries to adopt industrial internet of things (IIoT) systems and processes with the main objective-to improve the processes and increase production. However, it is undeniable that despite IIoT advantages, it posed significant issues on the security and privacy on industry automation especially along data generation and control system. Hence, this paper proposes a cloud based 3-tier data security framework that performs two-level security verification processes. The framework has been tested and validated using an experimental industry automation system and has been found to be functionally effective with an acceptable handoff delay.

Corresponding Author:

Mirador G. Labrador
Center for Engineering, Science and Technology and Innovation
Samar State University
Arteche Blvd., Brgy. Guindapunan, Catbalogan City, Samar, Philippines
Email: labradormirador@yahoo.com

1. INTRODUCTION

Cloud-based storage and process has changed the very nature of information the way it can be shared and accessed, managed and delivered. It changes the landscape of wireless communication connectivity and the associated data access security. Some argued that cloud computing is a new technology but what is real is that it supports grid technology, utility, virtualization in computing, network technology and software applications [1]. In particular, cloud computing applicability is very diverse as it can be used in computing virtualization, in networking and software services, in distributed and in parallel computing.

On the other hand, the shifting of industry automation and control processes from wired to wireless system gives birth to industrial internet of things (IIoT). IIoT is an interconnection of sensing devices, instrument and other electronic equipment networked together in order to allow data collection, exchange and analysis to improve and make industry operations effective and efficient. At the macro level, IIoT is a networked infrastructure that requires self-configuring objects in highly intelligent way but has a limited storage and computing capacity. As a result, cloud computing can play a significant role as it can support intelligent processes and at the same time resolves the storage problem.

Hence, the complementing features of cloud based system with that of the 3-layer data operational and transactional process of IIoT becomes the motivational aspect of this particular study. In particular, the study aims to explore and apply cloud computing as one of the security mechanisms in IIoT addressing

the contraints of IIoT memory requirement without compromising transaction and data transfer processing time. Moreover, as industrial equipment and devices become connected, cloud computing can be integrated for it will provide new storage, processing, scalability, security and networking capabilities. Thus, this paper explores and proposes the cloud-based 3-tier data security framework for industrial internet of things. The framework deals on the application of 2-level security measures on the 3-key component of IIoT architecture and operations-the device, the channel and the associated services. The remaing section of the paper includes presentation of relevant and related studies, the cloud-based security framework-which is based on the complementing features of IIoT transacational and operational processes vis-à-vis 3-tier data implementation requirement, presentation of the experimental set-up and results.

2. RELATED STUDIES

IIoT is an extension of internet of things (IoT), this section explores security approaches governing IoT. Note that a significant numbers of research has been undertaken to address the security issues of IoT. Some of these security solution targets security issues at a specific layer, whereas, other approaches aim at providing a cut-across solutions [2]. Physical and data link layers security issues are considered as the lowest-level security issues [3]. Some of these issues includes: (1) jamming adversaries-an intentional disruption on wireless devices communication or transmission, (2) insecure initialization-a security issues that causes generatation and transmission of unverified or unathenticated data, (3) low-level sybil and spoofing attacks-an attack in a wireless networks where a node may operate in a fake identities, (4) insecure physical interface-factors associated to serious threats to proper functions of IoT devices, and (5) sleep deprivation attack-an attack that causes the sensor node to be always in active state which results to the depletion of battery [4]-[6].

Intermediate-level security issues take place at transport and network layers. Different security issues on this level includes: duplication, buffer reservation, routing, sinkhole and wormhole, and sybil attacks [7], [8]. Duplication attacks is caused by fragmentation or insecure neighbor desovery. Other security issues include: authentication and secure communication, transport level security, session initiation and resumption, and cloud-based privacy violation. On the other-hand, high-level security issues take place in the application layers which include, but not limited to, insecure interfaces, insecure software and firmware, midde ware security issues and the security issues associated to constrained application protocol (CoAP) with internet [9]-[12].

In fact, it has been argued that IoT security needs to move from single products to end-to-end solution and eventually to the entire security architecture [13]. A survey paper which categorizes the different security issues into application, communication, and data are described and presented in [14]. The said paper discusses the different IoT threats based on hardware, network and application components. In particular, IoT hardware threats includes: tracking, disk operating system (DoS), repudiation and spoofing for radio frequency identification (RFID) based hardware, packet manipulation for Zigbee; eavesdropping and DoS for bluetooth; and DoS, exhaustion, unfairness and sybil for sensor node. For network components, threats includes, manipulation of data, extortion hack, rogue access points, and misconfigurations. While for threats associated in application components includes: DoS manipulation of information, costumer security, physical security, theft and loss, insider misuse, and unintentional actions. On the other hand, Granjal *et al.* [15] analyzes security issues based on IoT protocols. Succeding paragraphs outlines the different IoT security requirements versus security attacks, threats, and solutions.

In particular, the study of [16] proposes Blockchain mechanism for IoT security. The study emphasizes that blockchain is more effective when used at the lower layer of the communication model as well as at the application layer. However, the study also points out that in order to maintain IoT integrity, it is necessary that other security mechanism such as firewall, encryption and authorization must be combined with that of blockchain security.

In similar manner, blockchain technology was proposed as a security mechanism for internet of vehicle (IoV) in [17]. The study deals on the use of blockchain technology coupled with cryptographic services in the implementation of IoV and argues that the used of the said mechanism ensures communication privacy and data authenticity. In general, it can be viewed that blockchain is more effective and efficient when it is being paired with other security solution approaches when it is being used in IoT. In other words, literature indicates that existing IoT security mechanism including that of blockchain can still be improved if it is being coupled with another security approaches.

As such, considering the different security threats and issues in the different network layer of IoT as cited in the previous paragraph vis-à-vis the associated data requirement, the design of security framework based on the said constraints and requirements was explored and proposed on this paper. The primary reason of the proposed security framework is to improved existing IoT mechanisms and at the same time address the

different threats and security constraints as presented in the previous paragraph. Description of the proposed framework is presented in the succeeding section of this paper.

On the other hand, as cloud computing offers an scalabale and convenient network access, its actually enables a dynamic data integration from and across all connected IoT devices. Thus, several studies have been undertaken on the cloud and IoT integration which has been presented in [18], [19]. The integration deals on addressing the different security issues in IoT. Sharma *et al*. [20] proposed a mitigation architecture for security attacks that incorporate a highly programmable monitoring network based on cloud computing which is referred to as OpCloudSec architecture. OpCloudSec allows network control and monitoring in the cloud which has a very high detection and identification capability of IoT devices. Similar studies have been undertaken by [21]-[23]. Although the studies presented show that cloud computing has a very good security performance assessment, it can be viewed that the strategy can be still be improved by embedding selective sensing intelligence in the edge nodes with the integration of intelligent mobility management techniques for data generators. Hence, it is for this reason that the integration of cloud computing as an additional security processes for IoT and IIoT in particular is being proposed based the complementing characteristics of IIoT Inteleggent level manufacturing processes with that of the data requirements based on 3-tier model offered by the cloud computing as indicated in Figure 1.

3. CLOUD-BASED 3-TIER SECURITY FRAMEWORK

The complementing features of 3-tier data model and that of the three-level intelligent processes of a manufacturing industry becomes the fundamental basis of this proposed security model. Figure 1 shows the framework of a cloud-based 3-tier security model for IIoT. As indicated in Figure 1, the intelligent level of manufacturing plant includes the (1) enterprise resource planning (ERP), (2) the manufacturing execution layer (MES) and (3) the field control system (FCS). On this, a corresponding data and processes are being identified and being matched with that of the 3-tier data model. FCS involves the actual sensors and actuators functions such as actual data sensing and triggering of device/equipment for certain operation. Likewise, the said FCS defined processes is in conformity to the presentation layer of that of the 3-tier data model categorically referred to as device/user layer as indicated in Figure 1. This is because the FCS processes and the associated data generation and function on this level is virtually-tied with that of the device itself.

Manufacturing execution layer (MES) is the second level of industry plant operation. MES usually enables control of multiple element of FCS. In the same manner to which the application layer of the 3-tier data model performs processing of commands, makes logical decisions and control, and drives application core capabilities. Thus, the proposed model of Figure 1 will enable better control, management and control of FCS devices.

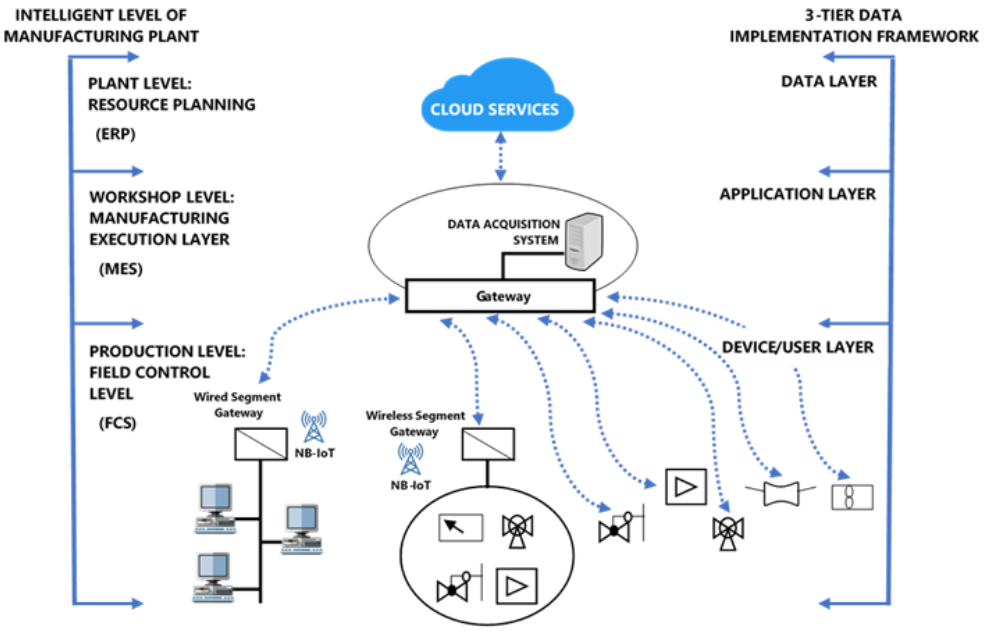

Figure 1. Industry operations and data requirement model

Meanwhile, ERP integrates all facets of an operation, including product planning, development, and manufacturing processes. In simple terms, it enables services for storage and access of data, processing of data and other forms of services relevant to industry operation. This functional ERP services requires efficient and effective data and service management which is being governed by that of the data layer indicated in Figure 1. Therefore, the binding mechanism of the industry plant operation with that of the 3-tier data architecture enables the possibility for the implementation of cloud-based 3-tier data model security approach as describe in Figure 2.

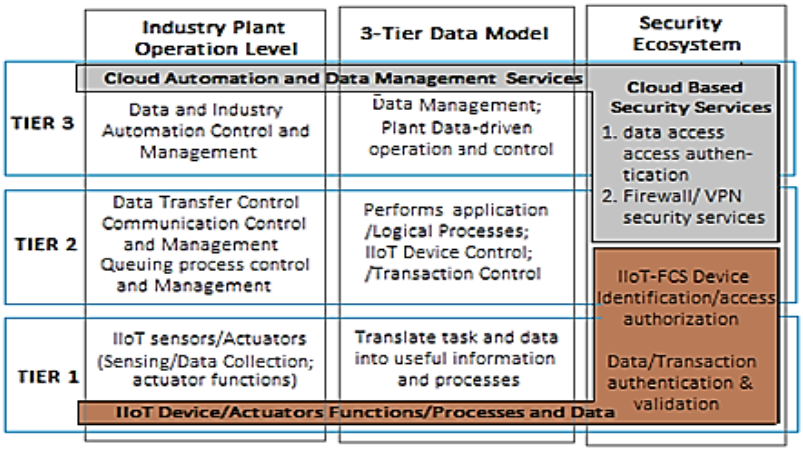

Figure 2. Industry operations and data requirement model

Note that IIoT devices has no capabilities to communicate directly with the cloud network. On this, IIoT devices requires external and interface communication facility via a specialized gateway collectively referred to that of data acquisition system (DAS) as indicated in Figure 1 and Figure 3. This specialized gateway serves as a relay station of data transmission and control operation between the FCS devices and that of the cloud system services. In particular, Figure 2 describe how a cloud based 3-tier security model can be implemented.

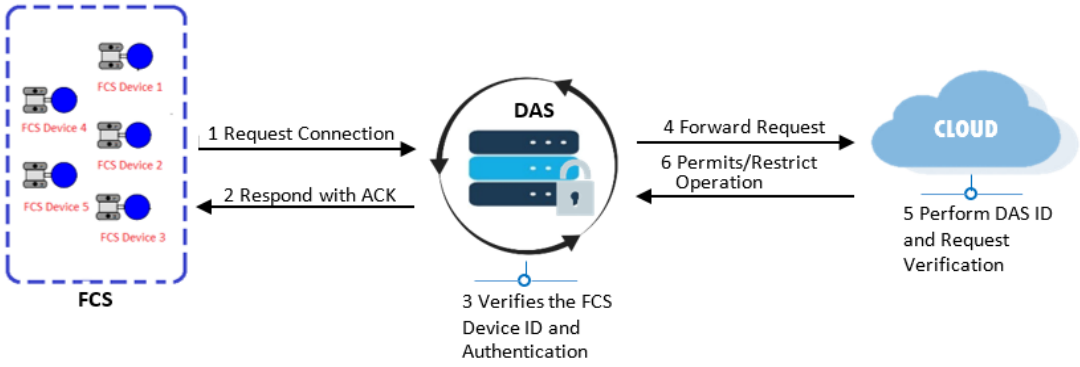

Figure 3. Binding security process

FCS devices and the DAS whose functions and characteristics describe in Figure 2 as tier 1 and 2 respectively establish a safe communication indicated in a security ecosystem of Figure 2 as identification, authorization and authentication. This security features binds both the FCS devices and that of the DAS. Moreover, tier 1 and tier 3 are security-tied together via the data access control and the issuance of trigger signal for specific device operation. The binding security processes as presented in Figure 3 are as follows:

– The FCS device requests a connection from the DAS. The DAS responds with acknowledge (ACK) signal. ACK signal is issued to the device via a handshake process. (In some cases ACK may not be issued if the DAS is busy. A transaction queiuing algorithm may be utilized).
– When connection is established, the DAS (via a server-side application) verifies the FCS device identification and authorization.

– DAS will forward device service/operation request and its corresponding ID to cloud server.
– Cloud server (via Cloud Services) performs DAS ID and request verification.
– Cloud-based Security permits or restricts operation request.

The process indicates the two-level security binding protocol of the proposed system. The first level identity, process authorization and transaction authenticity. While the second security level binds the tier 2 and 3 of industry operation, control and management. It ensures data privacy, and appropriate execution of FCS device operation. In general, the contribution of this paper is the integration of cloud computing services to strengthen the low-level security mechanism of that of IIoT utilizing the 3-tier data model concepts.

4. EXPERIMENTAL SET-UP AND RESULTS

4.1. Platform deployment, application and network scenario

This paper proposes the cloud-based 3-tier data security framework for IIoT. On this, a power plant system automation and management system was used as an experimental set-up. Figure 4 is the operational schema of the said system. In particular, the application scenario is divided into two level-(1) the DAS system services and (2) the power plant cloud-based services. Take note that security services are tied-up to the service functions of each functional level of power plant operation.

The power plant system automation is an example of an IIoT. Figure 4 ensures an appropriate automated FCS device control and operation. FCS device are sensors and actuators. Its main functions are to collect data (sensors) necessary as an input for an automated operation and the execution of function/operation (actuators). Data collected are transmitted to the gateway for processing via a low-power wide area access network (LPWAN) technology embedded as component of an FCS device.

On the other hand, the DAS and cloud services are both application programs. DAS services involve transaction queue management (in cases to which more than one FCS devices request service connection in a particular period of time). However, on this particular study, a simple first-come, first-serve (FCFS) queue model is used. Further, one of the major functionalities of DAS is to directly control the operation of FCS devices it is the one that issues trigger signal. Whereas, cloud services are ERP-based system. Services include data management and general plant operation management. ERP performs data processing. It notifies DAS to issue trigger signals to execute particular FCS device operations. Security functions and processes are integrated as part of the DAS and Cloud services defined in Figure 2 and Figure 4.

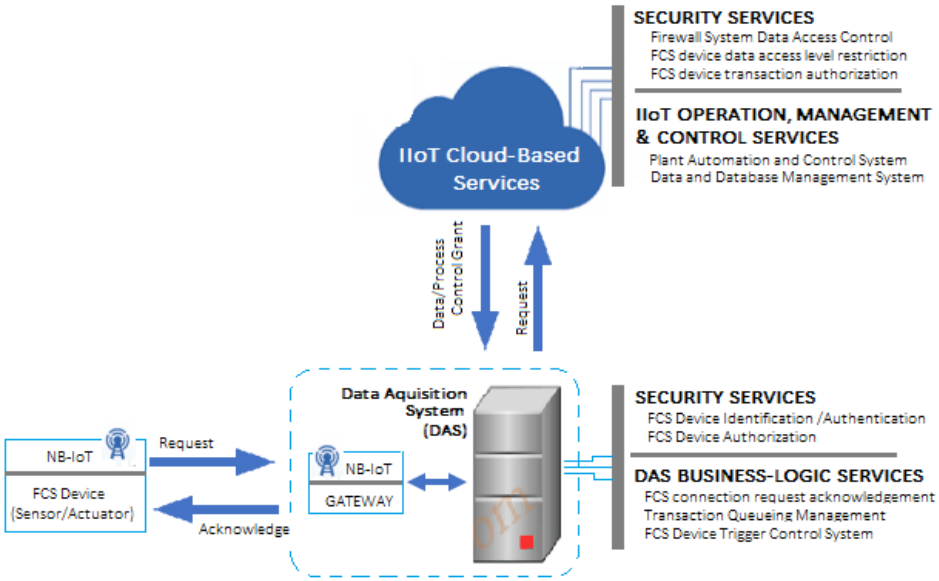

Figure 4. Application and network scenario

4.2. Security procedural processes and experimental results

In the experimental set-up the FCS device is tied-up to the DAS. In other words, FCS devices are paired up successfully by the communication capability of LPWAN. Pairing becomes successful when DAS-gateway issues an acknowledge signal to the device. After which FCS device will send its identification and

the associated data/request operations. DAS will perform device ID verification and authorization. In other words, DAS performs the first level security check. Once verified, DAS will forward the authorization request and its ID to the cloud server. Cloud server performs the second-level security check by validating DAS identification and device operation request. Cloud will permit or restrict request operations. Figure 5 shows the actual application program operation for DAS security verification process while Figure 6 shows cloud server successful line security verification procedure.

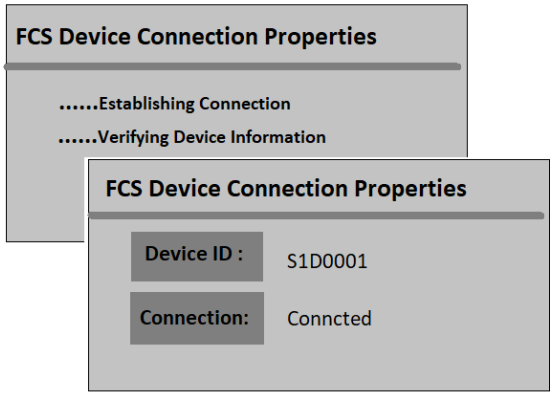

Figure 5. DAS FCS verification process

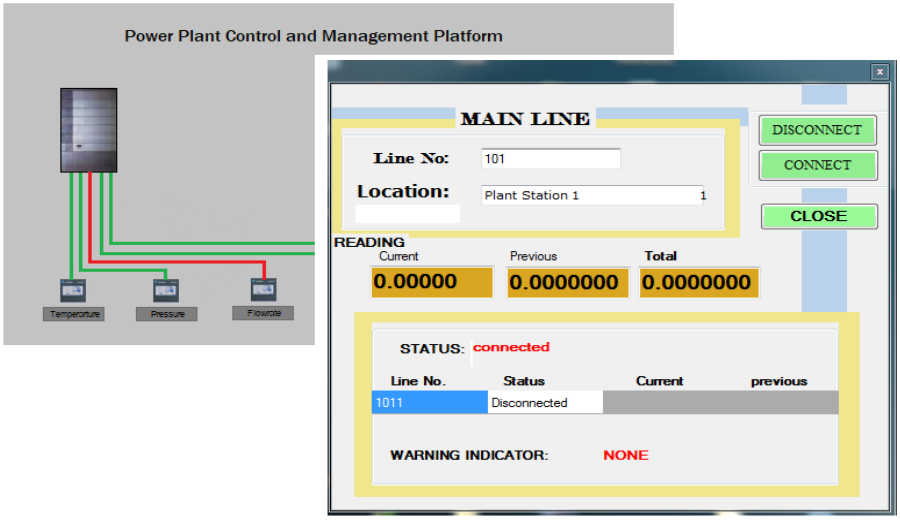

Figure 6. Cloud server successful security verification

As indicated in Figure 6, when a successful FCS device request verification is successful, line indicator changes color from green to red indicating that the connection from FCS device and cloud server control is established. Also, detailed FCS device information, properties and additional control are indicated in the new window. On the other hand, it is to be underscored that the 2-level security mechanism based on 3-tier data framework of IIoT could be influenced by few metrics such as the distance between the FCS device and the DAS. Hence, there are factors that will determine the efficiency of the proposed model. This includes FCS device active time, packet transmission ratio, and packet arrival rate. Packet transmission ratio is defined as the product of the FCS device active time and packet arrival time. Thus, proposed model performance depends on the said parameters.

Experimental results of the proposed framework utilizing the session initiation protocol (SIP) appear that FCS devices (wireless sensors) take advantage of the application layer signaling to provide DAS functionality. Its signaling suffers for additional delay due to processing delay at the application layer handoff. Figure 7 illustrates the associated call flows during a FCS device handoff in the network. Table 1

shows the experimental results involving handoff delay for SIP as reported in [24]. The handoff cases represent the movement from FCS device to DAS to cloud system. It shows that the delay associated with signaling and cloud for two cases with and without duplicate address detection. SIP-based mobility appears to suffer because of application layer processing.

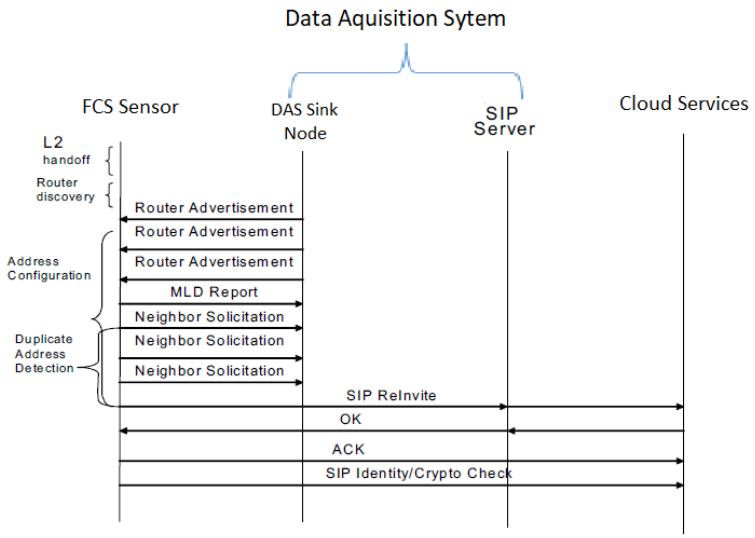

Figure 7. Cloud server successful security verification

Table 1. Sample handoff delay

Handoff Case	Signaling (ms)		Media (ms)	
	SIP (DAD)	SIP (NDAD)	SIP (DAD)	SIP (NDAD)
H12	3819	167.1	3861	415.8
H23	3924	155.6	4180,7	411.6
H31	1934.7	154.1	1931,4	404.4

4.3. Feature of the power plant automation management and control system

The power plant automation and management system a simple automation control system is an expanded and upgraded version of the developed system indicated in [25] which has been purposively utilized for purposes of simulating the proposed security framework. The system comprises of the different components and modules necessary in the execution of its operation as implied in Figure 6. critical to this are the FCS devices. This is because FCS devices are to be developed/constructed both with hardware and software components. Hardware components includes the integration of LPWAN, sensors, actuators and a microprocessor/microcontroller (pre-processing component). In particular, an ALT1250 NB-IoT chipset was used as wireless communication module, a PIC32MX as microcontroller chipset, and specific sensors/actuators (based on functions) among others. The FCS devices are virtually-connected to the automation and control management software as deployed separately on DAS and cloud server. At the cloud server is the over-all power plant control and management while on the DAS is the FCS device direct control and management.

There are two mechanisms to which the power plant operation can be controlled. First is the FCS device driven operation. On this mechanism, the FCS device invoke an interrupt signal to the DAS. Interrupt signals is based on the current status of operation (i.e. if sensors were able to detect/collect data that is not within the preset standard). When interrupt signal is being received by DAS, it will establish connection to the cloud server for data analysis. Results of data analysis would then be the basis for an automated operation (i.e. automatic shutdown of FCS device, and activation of certain operations). Second is the management-controlled operation wherein the authorized personnel may enable activation/deactivation of certain FCS devices and/or processes based on the information displayed in the interface management system software. Figure 8 is the sample application program interface at the cloud server.

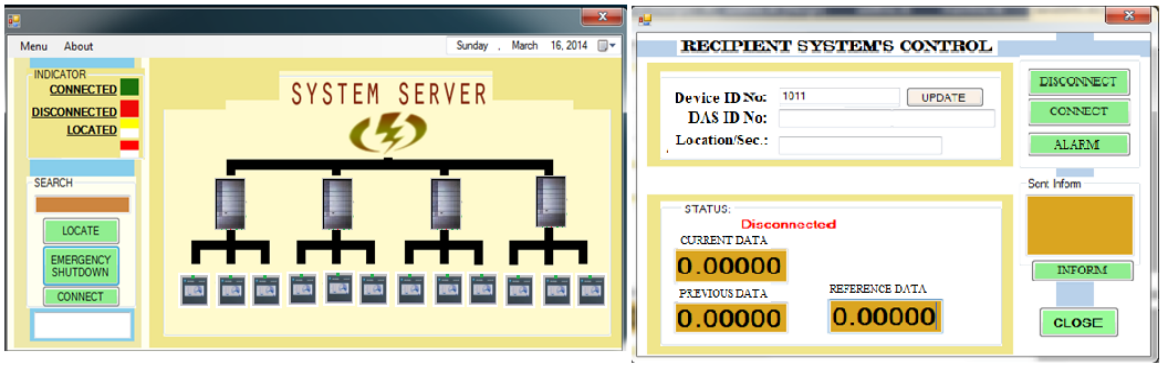

Figure 8. Cloud server automation control

5. CONCLUSION

This paper proposes a cloud-based 3-tier security solution for IIoT. The approach was based on the complementing features of both the 3-tier data model and that of the 3-level intelligent manufacturing processes of an industry. The proposed framework established a 2-level security verification processes implemented via the localized server functioning as data acquisition gateway and that of the cloud server. The proposed security framework has been validated as it is being tested in a developed industry-like automation system for power plant control. However, the study does not include performance analysis of the proposed model. On this, it is suggested that a comprehensive performance evaluation is to be undertaken and compared to existing security models.

ACKNOWLEDGEMENTS

This research is funded by the Samar State University-Center for Engineering, Science and Technology & Innovation, hence due recognition and acknowledgement is being accorded. Likewise, the authors also wishes to extend gratitude to Prof. Dr. Weiyan Hou of Zhengzhou University for the expertise and ingsights accorded which leads to the completion of the study.

REFERENCES

[1] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., and Wills, G. B., "Integration of cloud computing with internet of things: challenges and open issues," In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, pp. 670-675, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.

[2] Khan, M. A. and Salah, K., "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol 82, pp. 395-411, doi: 10.1016/j.future.2017.11.022.

[3] Minoli, D. and Occhiogrosso, B., "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1-2, pp. 1-13, 2018, doi: 10.1016/j.iot.2018.05.002.

[4] Labrador, M. and Hou, W., "Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicle (IoV) Scenario: A Blockchain Based Model," *Journal of Computer Science*, vol. 15, no. 2, pp. 249-257, 2019, doi: 10.3844/jcssp.2019.249.257.

[5] Lohachab, A., "ECC based inter-device authentication and authorization scheme using MQTT for IoT networks," *Journal of Information Security and Applications*,vol. 46, pp. 1-12, 2019, doi: 10.1016/j.jisa.2019.02.005.

[6] Yan, H., Wang, Y., Jia, C., Li, J., Xiang, Y., and Pedrycz, W., "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," *Future Generation Computer Systems*, vol. 95, pp. 344-353, 2019, doi: 10.1016/j.future.2018.12.061.

[7] Kâafar, M. A., Benazzouz, L., Kamoun, F., and Males, D., "A Kerberos-based authentication architecture for Wireless Lans," In *International Conference on Research in Networking*, 2004, pp. 1344-1353, doi: 10.1007/978-3-540-24693-0_117.

[8] Shrestha, A. P., Choi, D. Y., Kwon, G. R., and Han, S. J., "Kerberos based authentication for inter-domain roaming in wireless heterogeneous network," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 245-255, 2010, doi: 10.1016/j.camwa.2010.01.019.

[9] Bersani F. and Tschofenig H., "The EAP-PSK protocol: A pre-shared key extensible authentication protocol (EAP) method," *RFC 4764*, 2007, doi: 10.17487/RFC4764.

[10] Clancy T, and Tschofenig H., "Extensible authentication protocol generalized pre-shared key (EAP-GPSK) Method," *RFC 5433*, 2009.

[11] Granlund D., Anderson K., Elkotob M. and Ahlund C., "A uniform AAA handling scheme for heterogeneous networking environments," *2009 IEEE 34th Conference on Local Computer Networks*, 2009, pp. 683-687, doi: 10.1109/LCN.2009.5355059.
[12] Zhang D., Fred Wang F., Burgos R., and Boroyevich D., "Common-Mode Circulating Current Control of Paralleled Interleaved Three-Phase Two-Level Voltage-Source Converters With Discontinuous Space Vector Modulation," in *IEEE Transactions on Power Electronic*s, vol. 26, no. 12, pp. 3925-3935, Dec. 2011, doi: 10.1109/TPEL.2011.2131681.
[13] *IoT Security White Paper: Evolving Security Architecture (2018)*, GIV 2025. [Online]. Avaliable: https://www.huawei.com/minisite/giv/en/.
[14] Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F., "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017, doi: 10.1016/j.jnca.2017.04.002.
[15] Granjal, J., Monteiro, E., and Silva, J. S., "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015, doi: 10.1109/COMST.2015.2388550.
[16] Labrador, M., and Hou, W., "Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicle (IoV) Scenario: A Blockchain Based Model," *Journal of Computer Science*, vol. 15, no. 2, pp. 249-257, doi: 10.3844/jcssp.2019.249.257.
[17] Arumozhiyaly R. and Baskaran K., "Implementation of a Fuzzy PI Controller for Speed Control of Induction Motor using FPGA," *Journal of Power Electronic*s, vol. 10, no. 1, pp. 65-71, doi: 10.6113/JPE.2010.10.1.065.
[18] Sahmim, S., and Gharsellaoui, H., "Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review," *Procedia computer science*, vol. 112, pp. 1516-1522, 2017, doi: 10.1016/j.procs.2017.08.050.
[19] Stergiou, C., Psannis, K. E., Kim, B. G., and Gupta, B., "Secure integration of IoT and cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 964-975, 2018, doi: 10.1016/j.future.2016.11.031.
[20] Sharma, P. K., Singh, S., and Park, J. H., "OpCloudSec: open cloud software defined wireless network security for the Internet of Things," *Computer Communications*, vol. 122, pp. 1-8, 2018, doi: 10.1016/j.comcom.2018.03.008.
[21] Mukherjee, B., et al., "Flexible IoT security middleware for end-to-end cloud-fog communication," *Future Generation Computer Systems*,vol. 87, pp. 688-703, 2018, doi: 10.1016/j.future.2017.12.031.
[22] Bittencourt, L. et al., "The internet of things, fog and cloud continuum: Integration and challenges," *Internet of Thing*, vol. 3-4, pp. 134-155, 2018, doi: 10.1016/j.iot.2018.09.005.
[23] Hussain, M., and Beg, M. M., "Fog Computing for Internet of Things (IoT)-Aided Smart Grid Architectures," *Big Data and Cognitive Computing*, vol. 3, no. 1, 2019, doi: 10.1016/j.iot.2018.09.005.
[24] N. Nakajima, A. Dutta, S. Das and H. Schulzrinne, "Handoff Delay Analysis for SIP Mobility in IPv6 Testbed," *IEEE International Conference on Communications*, 2003.
[25] Labrador, Mirador G., Miguel Lorenz D. Tabon, and Al-Benyashier M. Sahhibal., "Design and Development of GSM-Controlled Electric Consumption and Monitoring System," *International Journal of Electrical, Electronics and Computer Systems (IJEECS)*, vol. 16, no. 2, 2013.