Low-Cost Design and Implementation of Cloud SCADA System

Mohamed Y. M. Hashem[1], Fawzy A. Osman[2], Mostafa A. R. Eltokhy[1,] Ail S. Gab Allah[3]
[1]Electronics Technology Department, Faculty of Industrial Education, Helwan University, Cairo, Egypt
[2]Electrical Engineering Department, Faculty of Engineering, Banha University, Cairo, Egypt
[٣]Curricula, teaching methods and educational technology Department, Faculty of Education, Benha University, Cairo,Egypt
m_yusuf7@yahoo.com, fawzi.osman@bhit.bu.edu.eg, mostafaeltokhy2717@yahoo.com, alyzzz2000@gmail.com

Abstract
In Industries, it's always look forward to reducing their operational cost and their Critical infra structures. Therefore, companies search for solutions to reduce their cost and ensure the system efficiency. One of that solutions is the use of a Cloud computing system which offers the advantage of integrating CPSs such as SCADA systems. This paper proposed a cost effective, simple, reliable and secured Cloud SCADA system. The proposed Cloud SCADA System based on secured nodes was implemented, which connects each other through VPN channel "encrypted'' to ensure the isolation of our system form external attacks. The remote terminal unit (RTU) also connected to master terminal unit (MTU) through unit encrypted VPN channel, so in our system, when the end user need to connect to MTU the firewall of our system protect on MTU from un-recognized end point users. Comparing the cost of our system with pervious work, it's lower than Arduino + WI-FI method by five times and 13 times lower than Raspberry-PI method. Also comparing with other server options the proposed server is easy for using, available for adding new components and also has high security.

Keywords Cloud computing system, SCADA systems, IOT systems.

1 Introduction
SCADA (Supervisory Control and Data Acquisition) is defined as the business automation control system central to many modern industries, including, oil, energy, gas, power, transportation and water. Both public-sector providers and private enterprises use SCADA systems, and they can work well in various types of

Companies because they have the ability to extend from simple configurations to huge, complicated projects. SCADA systems organize manifold software and hardware components, which allow industrial institutions to gather, monitor, and process data, and also, cooperate with control technologies that are connected over Human Machine Interface (HMI) software and record events into a log file. Information of SCADA systems is collected from sensors or other manual inputs, and then sent to programmable logic controllers (PLCs) or remote terminal units (RTUs), from which this information is sent to the computers with SCADA software. Current SCADA systems have Ethernet connectivity to enable connecting with the functionalities of networking. Standard protocols include IEC 60870-5-101/104, IEC 61850 and DNP3. These protocols are standardized to operate over the TCP/IP model. Mod bus TCP Protocol is commonly supported in devices with Ethernet Connectivity. The main function of SCADA software is to analyze and display the data to help operators and other employees to decrease waste and improve efficiency in the manufacturing procedure.

Reducing operational cost and Critical infra-structures are important factors in industries. Therefore, companies search for solutions to reduce their cost for getting efficiency system. Using of a Cloud computing system is one of that solutions which offers the advantage of integrating CPSs such as SCADA systems. This solution leads to the concept of Smart Industrial Systems, SIS. The advent of the cloud combination has provided many benefits to the information technology, IT, industry that includes embedded security, cost reductions and an increase in redundancy and flexibility. CPSs can be described as smart systems including both physical and computational components that are basically integrated and interact closely to sense and monitor changing states in the real world. CPS applications such as smart transportation, smart medical technologies, smart electric grids and so on.

At a supervisory control system, the major task of SCADA systems is to monitor a system's processes and apply the appropriate controls accordingly. SCADA systems are basically CPSs used in industries which included in a wide number of application areas [1-4].This solution present in the industry is Web SCADA, which provides multiple benefits that include anywhere/anytime accessibility to the system through a secure web browser connection.

When the future Internet is considered, new technologies replace old technologies, hence, we can say that the integration of industrial business systems and the cloud concept has made the integrated SCADA systems more vulnerable compared with classical SCADA systems. In general, SCADA systems architecture contains a Human Machine Interface (HMI), hardware, software, Remote Terminal Units (RTUs), a supervisory station, sensors and actuators [5]. However, when these systems were exposed to the cloud computing and complex network environments, they became more vulnerable to cyber threats and attacks. The following section describes the journey of SCADA systems from first generation to the IoT-based SCADA systems being used up-to now [6].

2 Generation of SCADA

2-1 First generation of SCADA systems

- Mainframe is the main brain responsible for computing.
- These systems weren't inter linked architect us. These systems used mono politics software's with high cost and limited features.
- These systems were closed to wan protocol for communication with RTU's.
- Today's WAN protocol not dosed for communicating (limited).

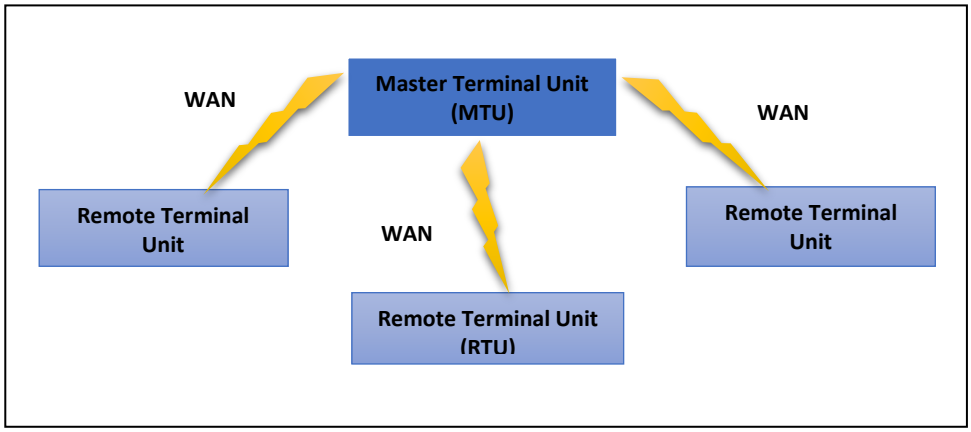

Fig. 1 First generation monolithic SCADA systems

2-2 Second generation of SCADA systems

- These systems used (LAN's) technology for inter connecting.
- These systems architecture become thy and less expensive than first generation
- These distributed systems increased performance and reliable and also redundancy, became available.
- Protocols used for (LAN's) mostly become monopolistic (limited)

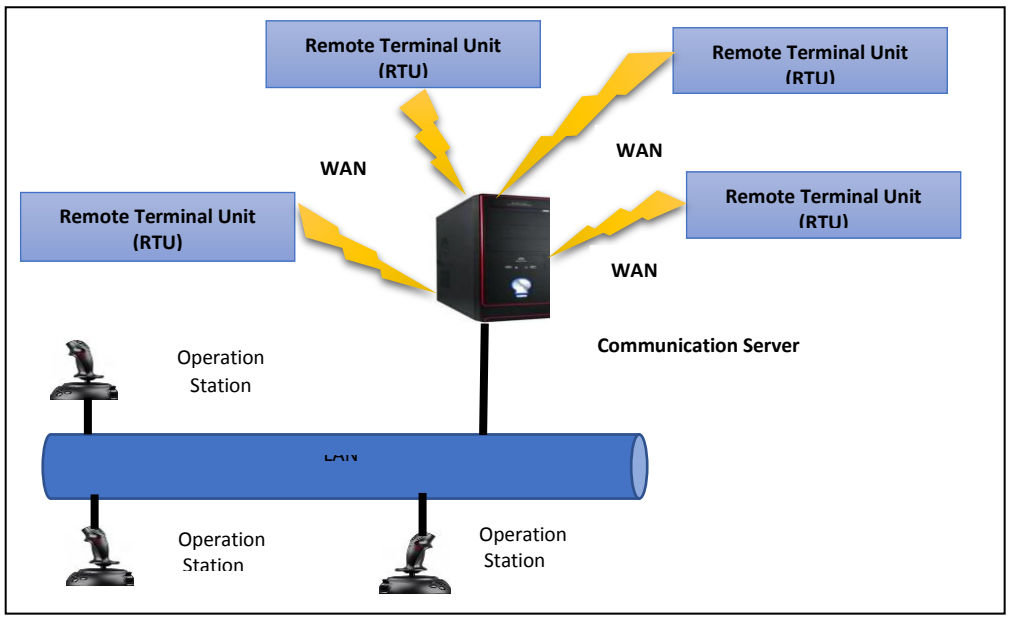

Fig.2 Second generation distributed SCADA systems

2-3 Third generation of SCADA systems

- In these systems the door become open for open source software instead of monopolistic software with restrictions.
- Protocols over internet protocol (IP) become available for communication.
- We can also make our custom protocol over (IP) to increase our systems performance and security.

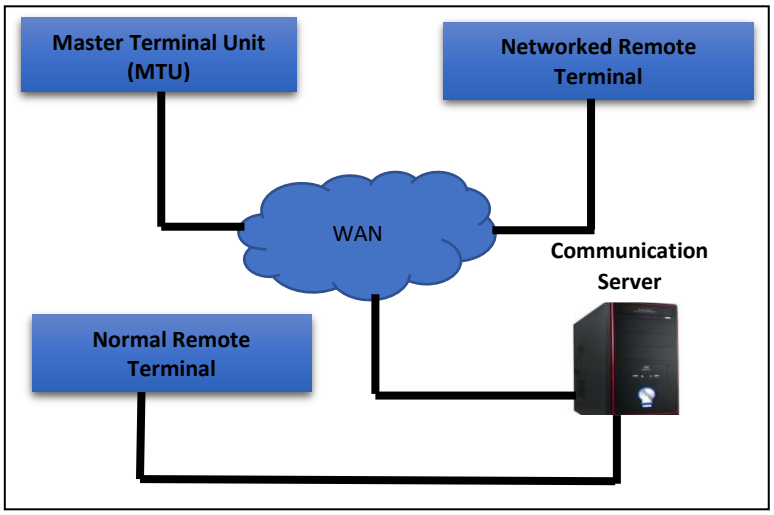

Fig. 3 Third generation networked SCADA

2-4 Fourth generation of SCADA systems (IOT)

- These systems nowadays became the best solution for large scale and wide business as it is easy to maintain and integrate.
- Increased data access ability, security, cost, efficiency, flexibility, availability, and scalability.

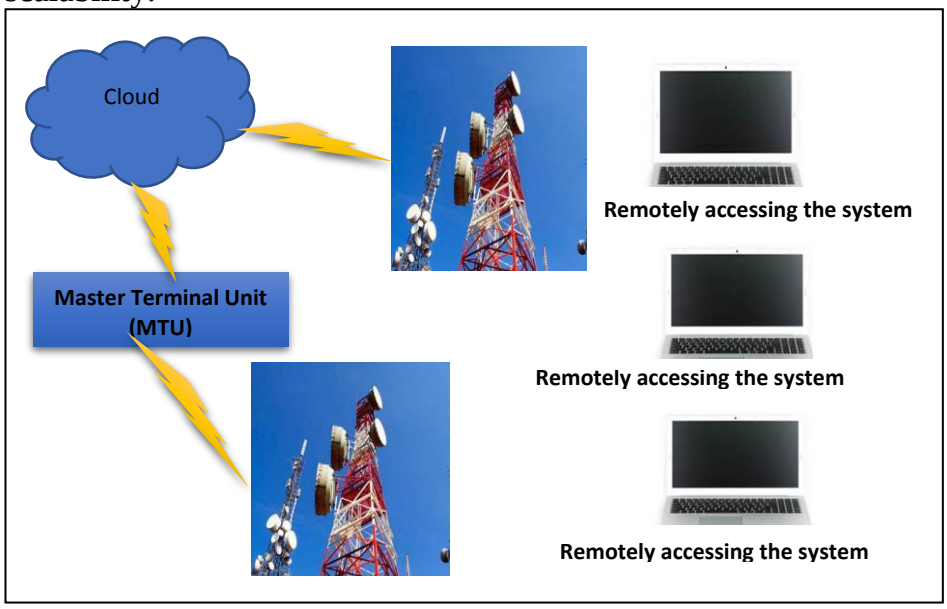

Fig. 4 Fourth generation IOT cloud-based SCADA system

3 **Recommendations for Securing Cloud Based SCADA Systems**

SCADA systems in cloud environment are not like regular IT systems; it can't be assumed that by simply using some strong password policies, antivirus protection, firewalls, or frequent patching will solve the security problems. Some basic principles can be considered for protecting Industrial cloud based SCADA systems. These principles have the objective of protecting vulnerable infrastructure by surrounding these systems with a combination of security tools [12-18]. Along with speed, Security is one of the key requirements for business success. Virtual private network (VPN) technologies provide a means of secure and private transmission of data over unsecure and shared network infrastructure. With the permanent need to raise the business efficiencies in conjunction with greatly reduced IT operational expenditures, organizational leaders look into enabling more mobile working patterns for their workforce and thus increasing the scope of efficiency and flexible communication channels. They must continue to maximize the economies of scope in their existing data infrastructure investments [19]. This paper aims to analyze how VPN enable enterprise workforces to share data seamlessly and securely over common yet separately maintained network infrastructures, such as through an Internet service provider (ISP) between enterprise networks or with corporate extranet partners. A Virtual Private Network is Virtual, meaning that the overall bandwidth and capacity of the physical infrastructure is transparent to the VPN connection and it can be owned by the Public Internet Service Provider. The virtual nature is achieved through the tunneling techniques operated on the upper layers. Computer networks in general and VPN networks in particular use encryption protocols to secure their exchange of data and information. Depending on the type of dedication, function, its size, services it provides, it can choose from a wide range of standards.

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that audits network traffic flows to detect and prevent vulnerability exploits. There are two types of prevention system they are Network (NIPS) and Host (HIPS). These systems watch the network traffic and automatically take actions to protect networks and systems [20, 21]. IPS issue is false positives and negatives. False positive is defined to be an event which produces an alarm in IDS where there is no attack. False negative is defined to be an event which does not produces an alarm when there is an attacks takes place. Inline operation can create bottlenecks such as single point of failure, signature updates and encrypted traffic. The actions occurring in a system or network is measured by IDS.

3 **Proposed System**

The proposed system as show in Fig. 5, our SCADA System based on secured nodes was implemented, which connects each other through VPN channel "encrypted'' to ensure the isolation of our system form external attacks. The remote terminal unit (RTU) also connected to master terminal unit (MTU) through unit encrypted VPN channel, so in our diagram when the end user need to connect to MTU master terminal unit the firewall of our system protect on MTU from un-

recognized end point users, so it verifies the user name and its privileges to our system, then if it is ok the user can connect to the MTU smoothly. If the privileged user is infected or trying to send more requests more than normal the system, consider it as an attack and block source user IP. Otherwise when the user is connected to the MTU and wants to reach one of our system RTU, The system MTU itself can do it and redirect the request to the requested RTU, so we reached to our RTUs securely. On the other hands we protect our system form reverse connection coming from our RTUs as the flow of our connection. Coming from firewall and MTU reaching to the RTUs besides our firewall have form rules to secure our system form IPS. Fraud attacks.

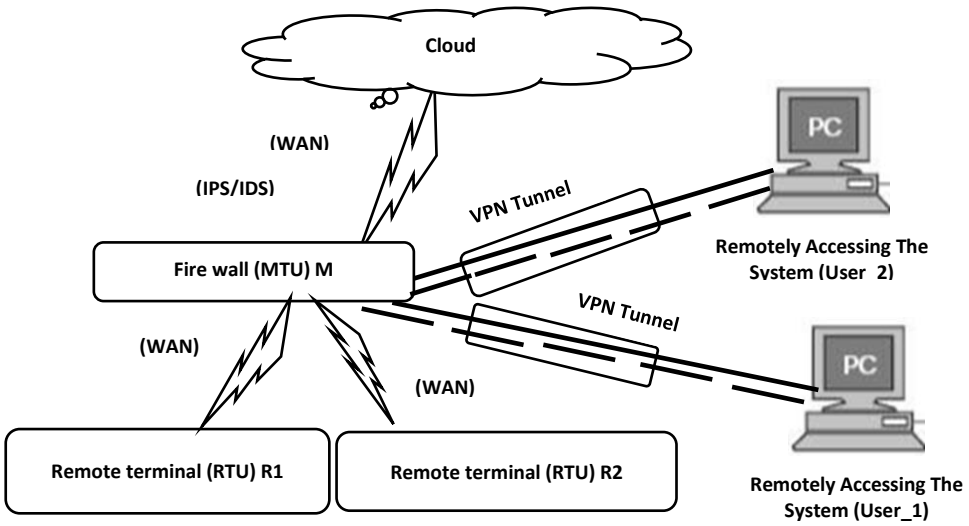

Fig. 5 Proposed Cloud SCADA System

The flowchart for the proposed system is given bellow:

Which can be describe as follows;

- At the begging the system search for a User IP request and then check if it is a valid IP address or not and which is repeated sequentially or a valid user.
- The second step check that the request of the valid user is connected over VPN channel or not, if is connected over VPN channel then move to the next step; if not, drop the user connection.
- Next, check the user validation using the firewall system (IPS/IDS), if it is a valid user then moved to the next step, [if] not, drop the user connection.
- Then, check the IP No. of the requested RTU; if the requested IP address of the RTU is Exist, move to the next step or if it is not Exist, drop the user connection.
- Finally, the Firewall system redirect the user to the requested RTU for monitoring and controlling it through the Cloud SCADA system.

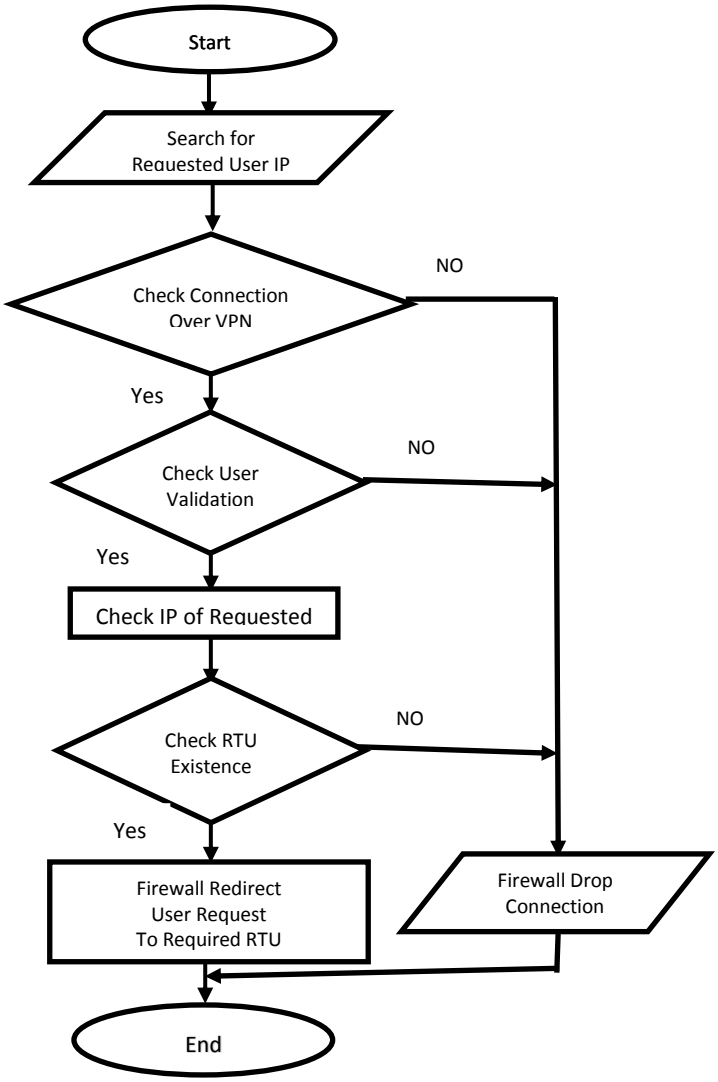

Fig. 6 Flowchart of the proposed system

5 Remote Terminal Units (RTU)

There are three main platforms can be used, namely as ESP8266-EXUnits,also named ESP-12E DEVKIT V2, Arduino with Wi-Fi shield based unit and Raspberry pi based unit (RPI).In this case Arduino UNO is used along with an Arduino Wi-Fi shield, the system reliability would be lower because it is a composite system. Major drawback comparing to others is the cost of the system where the Arduino UNO kit with the Wi-Fi shield will cost about five times than ESP12E approximately. Raspberry pi 3 is a very good option which is more reliable and is a real time unit with many features but has a limited number of GPIO and its ADC/DAC must be interfaced through SPI communication, also its cost is about 13

times more than ESP system.ESP-12E is an UART-Wi-Fi module, with a lower price in the trade and ultra-low power consumption technology, designed especially for mobile devices and IOT applications [22, 23] and it can be programmed with Arduino IDE software. Also, it can directly work as a Server itself or connect to Wi-Fi and send data to remotely located server with extremely low cost and high processing speed about 80 MHz (160MHz maximum). Also, ESP8266-12E is among the most integrated Wi-Fi chip in the industry; it integrates the antenna switches, power amplifier, low noise receive amplifier, filters, power management modules, it requires minimal external circuitry, and the entire solution, including front-end module, is designed to occupy minimal PCB area. ESP8266-12E also integrates an enhanced version of Tensilica's L106 Diamond series 32-bit processor, with on-chip SRAM, besides the Wi-Fi functionalities. ESP8266EX is often integrated with external sensors and other application specific devices through its GPIOs; codes for such applications are provided in examples in the SDK. But there are few drawbacks such as it has only one Analog and the major drawback is its low Wi-Fi range. The following table, Table 1, gives a comparison between all of three platforms units in accordance to its cost and drawbacks;

Table 1 comparison of RTU Units;

Method	Cost (LE)	Drawbacks
ESP12E	≈100 LE	Limited No. of ADC, Week WI-FI signal
Arduino + WI-FI	≈450LE	High cost, lower reliability and need more power
Raspberry-PI	≈1350LE	High cost, depends on the SD card, limited No. of GPIO, analog I/O through SPI

Each unit of the Remote Terminal Unit, RTU, was implemented using an ESP 8266-EXUnits. The above drawbacks of the ESP12E are overcomes as follows;

- Limitation of ADC channels: this drawback is solved by using an Analog Multiplexer, CD4067B or CD4097B, CMOS family which draw a little power, this analog multiplexer has 16 input or 8 differential input with a fast switching rate which equals 10 to 30 nSec. So, we can expand the ADC of the ESP12E up to 16 ADC channels with a little power consumption.
- Week Wi-Fi signal: this drawback is solved using an external Antenna with the ESP12E module which Boost the Wi-Fi signals to be a suitable for our application.

The interfacing to the ESP unit is carried through some of its GPIO's for monitoring and controlling the low level devices. Also, an analog input can be connected through the ADC channel of the ESP12E or through the multiplexer input channels to the ADC input of the ESP module. Also, analog output can be output through its PWM channels, which can be used as analog output by filtering it or used as a PWM signal to control the speed of a DC motor or varying the DC output to a different DC loads. Multi-Points of the RTU (ESP's) can be added to the cloud

SCADA system, and the MTU of the system can handle all of them for monitoring and controlling.
Also, a PCB card was designed for interfacing the GPIO of the ESP8266-12E module and its analog input/output. The schematic circuit for the designed interface card and its PCB are shown in Fig. 7 and Fig. 8 respectively.

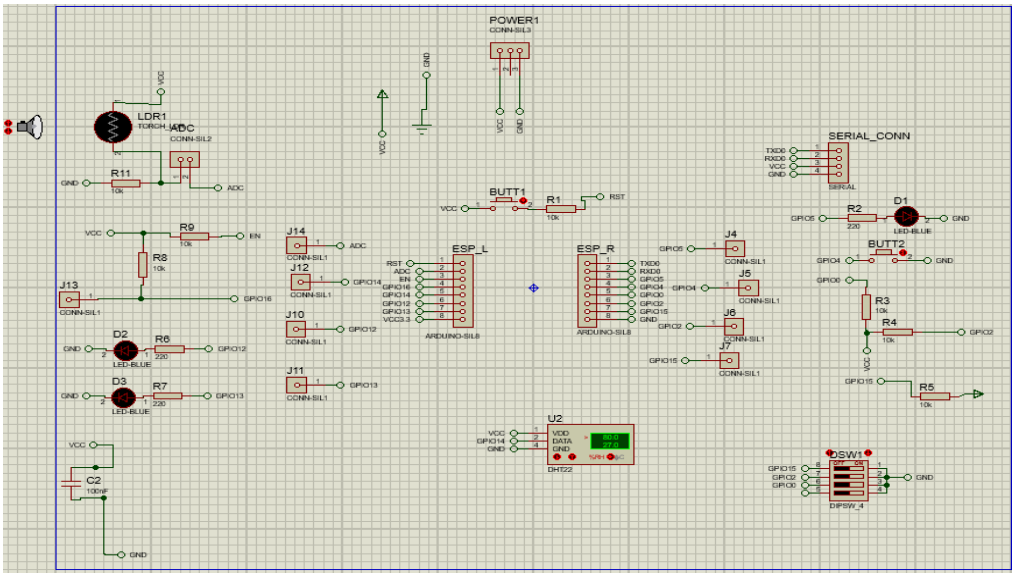

Fig. 7 Schematic circuit for interfacing ESP8266-12E.

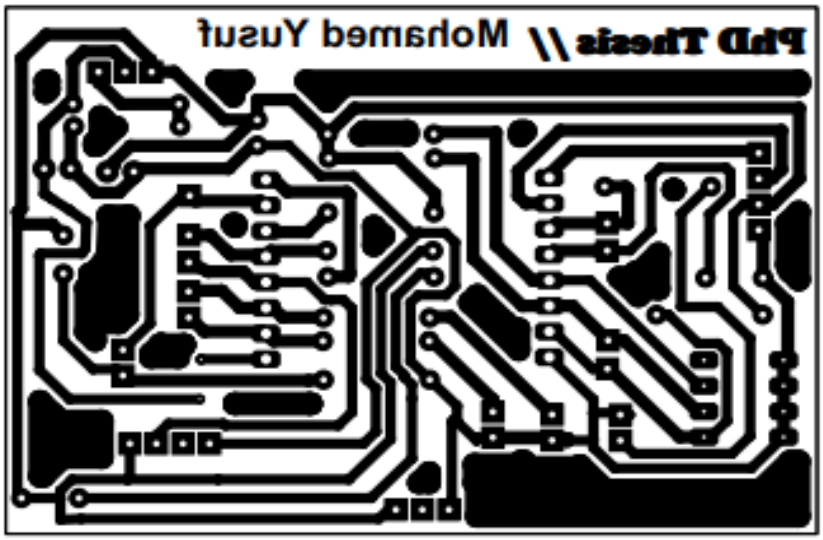

Fig. 8 PCB layout for interfacing ESP8266-12E.

The final interfacing card after soldering the components is shown in Fig. 9 and the ESP8266-12E is attached to it as a shield. Pin assignment for the ESP8266-12E module is shown in Fig. 10

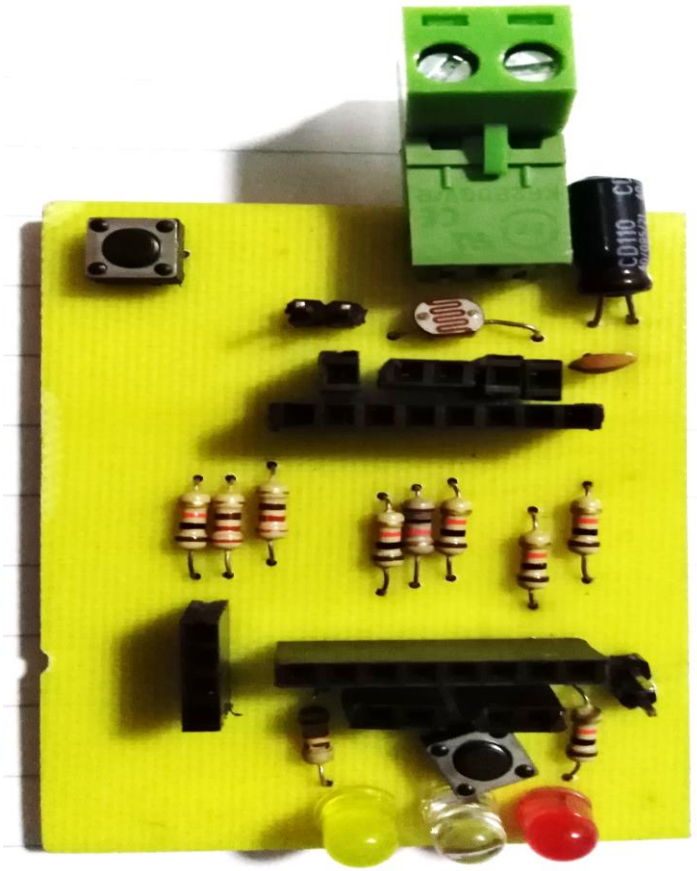

Fig. 9 Final ESP8266-12E interfacing Card.

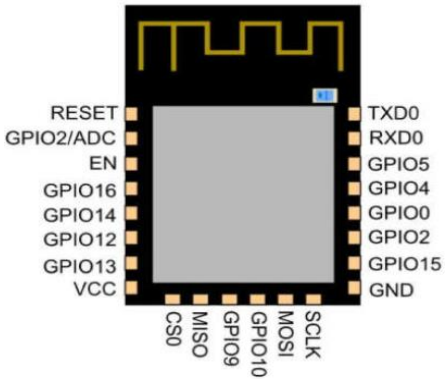

Fig. 10 Pin assignment for the ESP8266-12E module.

One of the GPIO's of the ESP8266EX module was used as PWM output for controlling the speed of a permanent magnet DC motor. For driving the armature circuit of the DC motor a drive circuit L6203, H-Bridge MOSFET driver, were used, which has a Max. Current of 5A and Max. Voltage of 48 Volt DC. The block diagram for the driver circuit is shown Fig. 11. Also the schimatic for the driner circuit and PCB layout are given in Fig. 12 and Fig. 13 respectively.

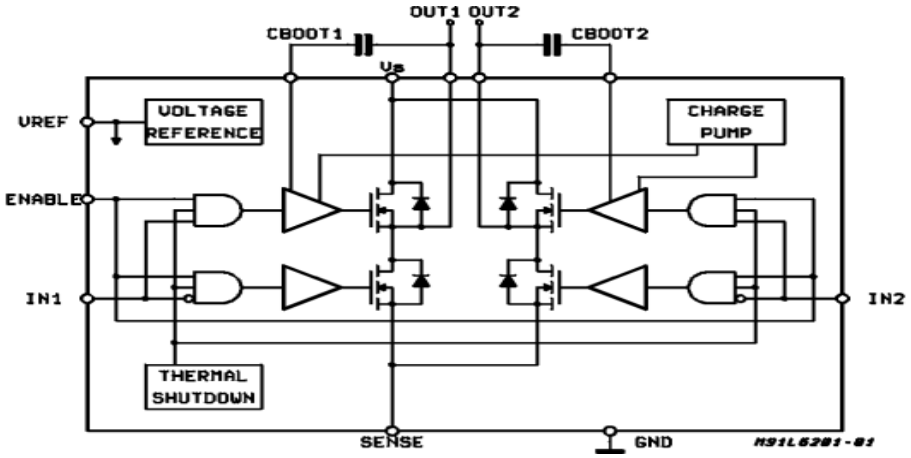

Fig. 11 Block diagram for L6203 Driver circuit.

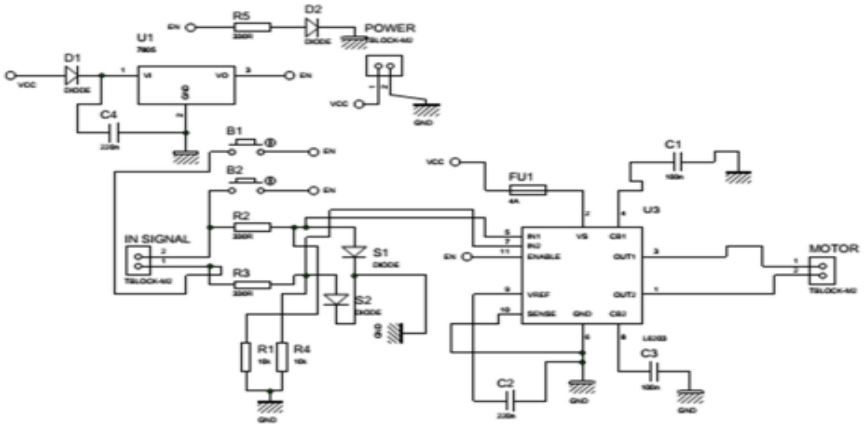

Fig. 12 Drive schematic Circuit.

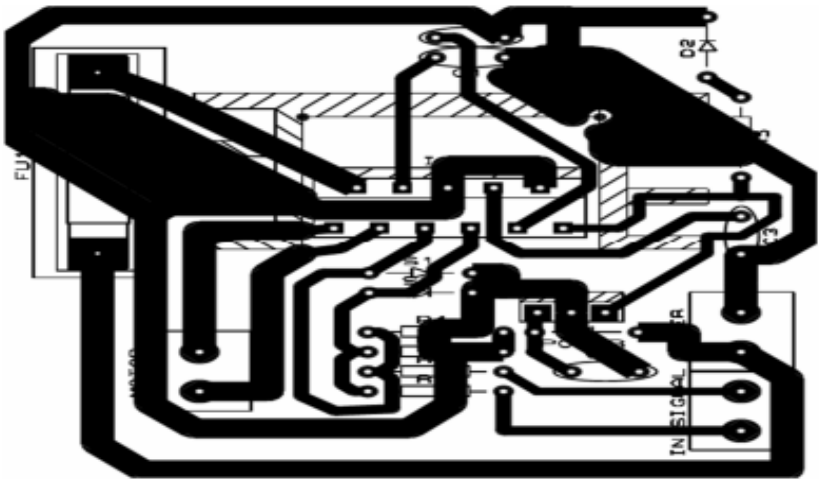

Fig. 13 Drive Circuit PCB layout.

6 SCADA Server Options

There are four major server options. Remote desktop connection with local data storage, Open Source SCADA software, IOT service provider and Private IOT server are considered.

A. RPI server with local data storage
In this method remote desktop software like Team Viewer, and Chrome Remote desktop has been used to access the client side computer which is the easiest one but the security is worth.

B. Open Source SCADA software
Here, an existing open source SCADA has been used to develop a suitable SCADA using it. The limitations for this approach is that it takes only two points per second when showing the data. Security of this system can be easily improved by closing all ports and use inside the intranet. So it comes to security concerns as highly secured.

C. IOT service provider
In IoT based SCADA systems with sensors and actuators, communication is based on a separate IP address each connected to a cloud. Most importantly this decentralized approach allows sensors and actuators to communicate with each other and take their own decisions.

D. D. Private IOT server
Though it is easy to implement above methods it will be unsecured to use someone else's IoT cloud or a server.

Therefore, an open source private IoT server is used.
In our system, a private server will be used which gives most of the features on the local server as well. Most importantly in this method data will be securely handled for instantaneously monitoring and control.
All server options discussed above are compared to each other and tabulated, as shown in Table 2, with respect to security, ease of installation, ease of using and ease of adding new components. Security, is the main feature we are concerned to because of sensitive data monitoring and controlling is our interest.
As shown the proposed our private server is easy for using, available for adding new components and also has high security.

Table 2: Comparison of server options

SCADA server	Security	Installation	Ease of using	Adding new components
Remote desktop Connection with Local data storage	Lower security	Easy to install	Easy to use	Need a special method
Open SCADA software	High security	Medium	Support some protocols	Easy to add new components
IOT service provider	For most of these server user has to pay after certain data limit			

Private IOT server	Secured because of the private server is an issue	Difficult to install	Easy to use most of variable limitations and date point limitations are avoided	Easy to add new components. (There is no need to have internet. Internet would be enough)
Our Private IOT server	High Security	No need for installation	Easy to use most of variable/ instantaneously	Scalable/Easy to add new components.

7 Conclusions

The purpose of this paper was to propose a cost effective, simple, reliable and secured Cloud SCADA system. The proposed Cloud SCADA System based on secured nodes was implemented, which connects each other through VPN channel "encrypted'' to ensure the isolation of our system form external attacks. The remote terminal unit (RTU) also connected to master terminal unit (MTU) through unit encrypted VPN channel, so in our system, when the end user need to connect to MTU the firewall of our system protect on MTU from un-recognized end point users. Each unit of the Remote Terminal Unit, RTU, was implemented using an ESP 8266-EXUnits. The interfacing to the ESP unit is carried through some of its GPIO's for monitoring and controlling the low level devices. Also, an analog input can be connected through the ADC channel of the ESP and analog output can be output through its PWM channels. Multi-Points of the RTU (ESP's) can be added to the cloud SCADA system, and the MTU of the system can handle all of them for monitoring and controlling. Comparing the cost of our system with pervious work, its lower than Arduino + WI-FI method by five times and 13 times lower than Raspberry-PI method. Also comparing with other server options the proposed server is easy for using, available for adding new components and also has high security.

References

1. C. Mylonas, I. Abdallah, E. N. chatzi, "Deep Unsupervised Learning For Condition Monitoring and Prediction of High Dimensional Data with Application on Wind farm SCADA Data", Model Validation and Uncertainty Quantification, Volume 3, pp 189-196, 2019.
2. S. Jayasinghe, T. Iqbal, G. Mann, "Low-Cost and Open Source SCADA Options for Remote Control and Monitoring of Inverters", IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-4, 16 April 2018.

3. Md. Jamelunissa, S.R. Murthy, A. Poojitha, "Industrial Process Control Using SCADA and Open Source Tools", International Journal of Advanced Research in Electronics and Communication Engineering, February 2017.
4. T. Lojka, I. Zolotova, "Improvement of Human-Plant Interactivity via Industrial Cloud-Based Supervisory Control and Data Acquisition System", IFIP International Federation for Information Processing, pp 83-90, 2014.
5. V. Bhanumathi K. Kalaivanan, "Application Specific Sensor-Cloud: Architectural Model", Springer Computational Intelligence in Sensor Networks, Studies in Computational Intelligence776, pp. 277-305, 2019.
6. V.Ramaraju, V.Katneni, M.Phil,V. K.Manda, "Super SCADA Systems: A Prototype for Next Gen SCADA System", IAETSD Journal for advanced research in applied sciences, volume 5, issue 3, pp. 107-115, 2018.
7. Burg, A. Chattopadhyay A. , K. Lam, "Wireless Communication and Security Issues for Cyber Physical Systems and the Internet-of-Things", Proceedings of the IEEE Volume 106, No. 1, pp. 38-60, 2018.
8. C. Wang, J. Shen, Q. Liu, Y. Ren, T. Li "A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things", Security and Communication Networks, pp. 1-8, 2018.
9. Hoda S., Yearwood J., Almogren A., "Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks", Applied Soft Computing Journal, 71, pp. 66-77, 2018.
10. P. Massonet, L. Deru, "End-to-end Security Architecture for Federated Cloud and IoT Networks", IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1-6, 2017.
11. R. Mahmoud, T. Yousuf, F. Aloul, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), pp. 336-341, 2015.
12. T. A. Tareke, S. Datta,**"** Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions /Organizations", Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE, pp. 533- 538, 2018.
13. Z. Firdaus, N. Jamil, Q. S. Qassim, M. E. Rusli, N. Ja'affar, M. Daud, H. C. Hasan, " A Study on Security Vulnerabilities Assessment and Quantification in SCADA Systems" Journal of Engineering and Applied Sciences, Vol. 13. Iss. 6, pp. 1338-1346, May 2018.
14. R. Chatterjee, S. Roy," Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud", International Journal of Engineering Science and Computing, Vol. 7, Iss. 5, pp. 11818-11821, May 2017.
15. Y. Cherdantseva, P. Burnap, A. Blyth, "A review of cyber security risk assessment methods for SCADA systems", Journal of computers and security, Vol. 56, pp. 1-27, Feb. 216.
16. V. Chang, M. Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Service Computing, pp. 1-15, 2015.
17. A. Shahzad, S. Musa, A. Aborujilah and M. Irfan, "A New Cloud Based Supervisory Control And Data Acquisition Implementation to Enhance the Level of

Security Using Test bed" Journal of Computer Science Vol. 10, Iss. 4, pp. 652-659, 2014.
18. J. Gao, W. Liang, C. L. Philip Chen, "SCADA communication and security issues", Journal: Security and Communication Networks, Vol. 7, Iss. 1, pp. 175-194, 2014.
19. M. Elezia, B. Raufia, "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption", World Conference on Technology, Innovation and Entrepreneurship, Procedia - Social and Behavioral Sciences 195, 1938 – 1948, Published by Elsevier Ltd, 2015.
20. M. Keshk, N. Moustafa, E. Sitnikova, G. Creech, "Privacy Preservation Intrusion Detection Technique for SCADA Systems", Military Communications and Information Systems Conference (MilCIS), pp. 1-6, 2017.
21. M. Korcák, J. Lámer and F. Jakab, "Intrusion Prevention/Intrusion Detection System (IPS/IDS) for WIFI Networks", International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.4, pp. 83-95, July 2014.
22. D. Dobrilovic, Z. Stojanov, "Building ESP8266 Wi-Fi module network based on open-source hardware and single-board computers", International Conference and Workshop Mechatronics in Practice and Education – MECHEDU 2017, 2017.
23. P. Zhang, T. Liu, Z. X. Yang, Y. Mou, Y. H. Wei and D. Chen, "Design of remote control plug." IEEE International Conference on Applied Superconductivity and Electromagnetic Devices (ASEMD), pp. 29-30, 2015.