INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
Special Issue, March-April 2023, Vol 3 (02), 16-19.
International conference on Innovation towards Sustainable Development Goals-ICISDG'23 ISSN No: 2583-0368

Achieving efficient and secure data acquisition in grid-connected solar, wind, and battery systems for cloud-supported internet of things

M.Poornima[1], G.Boopathiraja[2], S. Sugunadevi[3], R.Nandhini[4], N.Barathkumar[5]
[1,2,3,4,5] *Electrical & Electronics, Christ the King Engineering College/ Anna University ,India.*

Article Type: Research

OPENACCESS
Article Citation:
Naveen.SB[1], Santhosh raj.S[2], Visveswaran.A[3], Suresh Kumar.K[4], Ashok Raj.M[5], "Power handling using buck boost converter", International Journal of Recent Trends In Multidisciplinary Research, March-April 2023, Vol 3(02), 16-19.

https://www.doi.org/10.59256/ijrtmr.20230402c05

Abstract: The current world's scarcity of resources is driving everyone towards energy-efficient technologies. Among all of these resources, power is one that must be monitored and controlled as needed, as electricity usage increases. It described an excellent implementation of an intelligent remote monitoring system for solar Photovoltaic (PV), Wind Energy Conversion System (WECS), and battery systems used in a greenhouse setting in this research. The proposed system design can be placed in solar PV, WECS, and batteries to solve management issues, shorten mean time to repair, and reduce maintenance costs. It created a smart remote monitoring system based on the internet of things to monitor Solar PV, WECS, and batteries. This system included internet-based remote monitoring of solar PV, WECS, and batteries via host, network GPRS (Global Positioning Radio Service), embedded system gateway, and Arduino. Our demonstration results show that the system can monitor, store, and alter data from solar PV, WECS, and batteries. Remote monitoring functions are thus performed in real time.

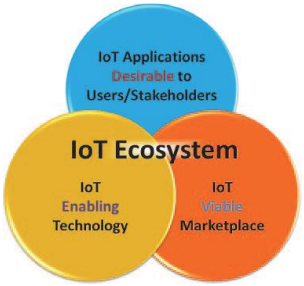
Key Word: PV, WECS, IOT, GPRS

1. Introduction

We are all aware that the planet is facing a severe challenge from the rapid depletion of fossil fuel supplies. The majority of today's energy demand is fulfilled by fossil and nuclear power facilities. Renewable energy methods such as wind, solar, biomass, geothermal, and others provide a minor portion. We are rapidly approaching a period of acute gasoline scarcity. "Energy cannot be generated or destroyed; it can only be changed from one form to another," according to the rule of conservation of energy. The majority of current research is focused on energy conservation and better energy utilization. There has also been research towards the development of dependable and durable systems for harvesting energy from nonconventional energy sources. Wind and solar power sources, in particular, have grown at an astonishing rate in the last decade. Both are pollution-free, plentiful electricity sources. India is a big consumer of energy resources, with high economic growth rates and more than 17 percent of the world's population. India's energy demand is increasing despite the global financial crisis. In compared to China, Japan, and Russia, India utilizes the most energy for residential, business, and agricultural purposes. Solar energy is energy that comes from the Sun. It is renewable, limitless, and does not pollute the environment. Solar-charged battery systems provide continuous power supply 24 hours a day, regardless of weather conditions. We can collect a big amount of power from solar radiations by using the suitable technology for the geographical area. Furthermore, solar energy is predicted to be the most promising alternative energy source. The global hunt for and growth in the cost of conventional fossil fuels is making supply-demand of electricity products nearly impossible, particularly in remote places. Generators, which are frequently utilised as an alternative to traditional power supply systems, are known to run only during specific hours of the day, and the expense of fueling them is becoming increasingly problematic if they are to be used commercially. Wind energy is the kinetic energy associated with atmospheric air movement. For hundreds of years, it has been used for sailing, grain grinding, and irrigation. Wind turbines transform kinetic energy into more useable kinds of power. Wind energy systems have been utilised for irrigation and milling since ancient times, and it is now being employed to create electricity at the turn of the twentieth century. Many countries have constructed windmills for water pumping, particularly in rural areas. Wind turbines convert wind energy into mechanical power, which can either be utilised directly for grinding or converted to electric power to create electricity. Wind turbines can be utilised individually or in groups known as wind farms.

2. The Internet Of Things

One year after the past edition of the Cluster book 2012 it can be clearly stated that the Internet of Things (IoT) has reached many different players and gained further recognition. Out of the potential Internet of Things application areas, Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem (figure 3.1) have acquired high attention. In line with this development, the majority of the governments in Europe, in Asia, and in the Americas consider now the Internet of Things as an area of innovation and growth. Although larger players in some application areas still do not recognise the potential, many of them pay high attention or even accelerate the pace by coining new terms for the IoT and adding additional components to it. Moreover, end-users in the private and business domain have nowadays acquired a significant competence in dealing with smart devices and networked applications.



As the Internet of Things continues to develop, further potential is estimated by a combination with related technology approaches and concepts such as Cloud computing, Future Internet, Big Data, robotics and Semantic technologies. The idea is of course not new as such but becomes now evident as those related concepts have started to reveal synergies by combining them. However, the Internet of Things is still maturing, in particular due to a number of factors, which limit the full exploitation of the IoT. Among those factors the following appear to be most relevant:

- No clear approach for the utilisation of unique identifiers and numbering spaces for various kinds of persistent and volatile objects at a global scale.
- No accelerated use and further development of IoT reference architectures like for example the Architecture Reference Model (ARM) of the project IoT-A.
- Less rapid advance in semantic interoperability for exchanging sensor information in heterogeneous environments.
- Difficulties in developing a clear approach for enabling innovation, trust and ownership of data in the IoT while at the same time respecting security and privacy in a complex environment.
- Difficulties in developing business which embraces the full potential of the Internet of Things.
- Missing large-scale testing and learning environments, which both facilitate the experimentation with complex sensor networks and stimulate innovation through reflection and experience.
- Only partly deployed rich interfaces in light of a growing amount of data and the need for context-integrated presentation.
- Practical aspects like substantial roaming-charges for geographically large-range sensor applications and missing technical availability of instant and reliable network connectivity.

Overcoming those hurdles would result in a better exploitation of the Internet of Things potential by a stronger cross-domain interactivity, increased real-world awareness and utilization of an infinite problem-solving space. Here the subsequent chapters of this book will present further approaches and solutions to those questions. In addition eight new projects from the recent call on SMARTCITIES in the scope of the European Research Program FP7, including a support and coordination action on technology road-mapping, will reinforce this year the research and innovation on a safe/reliable and smart Internet of Things, and complete the direct IoT related funding of 70M in FP7. Furthermore, a project resulting from a joint call with Japan will explore the potential of combining IoT and Cloud technologies.

3. Proposed System

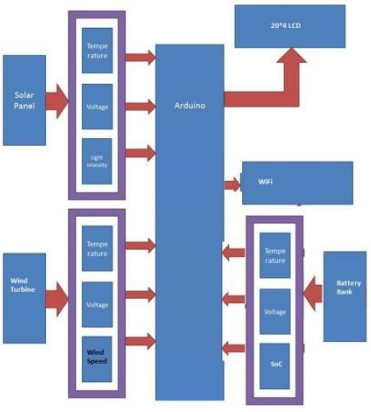


Figure 2 Block diagram of the proposed system

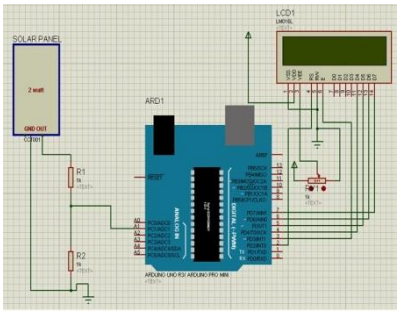
Figure 2 shows the block diagram of Achieving Efficient and Secure Data Acquisition for Cloud-supported Internet of Things in Grid connected Solar, Wind and Battery Systems.

4. Monitoring Solar System

Most photovoltaic systems contain parts such as the solar modules (panels) to provide the electrical power, a battery charger for converting the panel output to the battery voltage, a battery pack to store energy during the day and provide it during the night time, an inverter to transform the battery voltage to the proper line voltage for operating home appliances and an line source selector to switch between the solar and grid power. When the sun is shining during the daytime, the solar photovoltaic cells convert the sunlight falling on them into electricity. Although the efficiency of the conversion may be only about 17%, solar power can easily reach 1KW/m2 and suitable panels can produce 5000 Watts in these conditions. Solar panels typically produce a high voltage, 120V DC being a common figure. The battery charger has to convert this to match the battery voltage, generally 48V DC. Solar light power charges the batteries continuously during the daytime; therefore, the charger has to keep tracking the maximum power point to optimize the yield of the system. As the charger has to charge the battery also, this device forms the most elaborate part of the system. With the above arrangement, the solar panels charge the battery during the daytime and the battery discharges during the night. The size of the battery depends on one day of consumption plus some extra to tide over an overcast day. That also decides the size of the solar panel. Batteries are essentially heavy and the lead-acid types generally have a lifespan of about 7 years. The batteries feed the inverter, which converts the 48V DC into the line voltage – usually 230V AC or 110V AC. With a 5KW continuous rating, inverters can essentially run almost all household appliances such as the clothes dryer, the washing machine, the dishwasher and the electric kitchen oven. When the inverter is supplying a large load, the battery current may climb up to 200A. Multiple sensors measure the solar field power from and temperature of the solar modules divided into arrays. The information comes to a PV panel via a CAN bus, which unites all the sensors. The PV panel also acts like a gateway between the CAN bus and a single board computer.

5. Voltage Measurement in PV

Voltage Measurement of the Solar Panel is very easy which is up to 5 volts. But if we want to measure more than 5 volts then we have to use some additional circuitry like Voltage Divider. This circuitry changes according to Voltage, which means How Much Voltage we have to Measure. It is shown in figure



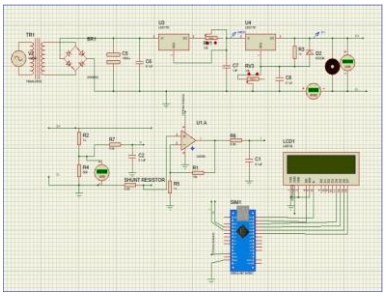
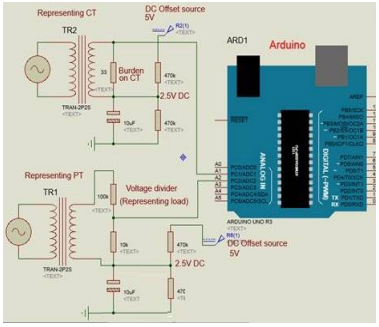


Figure 3 Monitoring PV system with Arduino Figure 4 Battery Charger Circuit



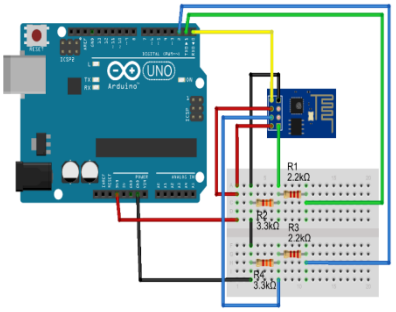


Figure 5 Voltage and Current MeasurementFigure 6 WiFi Connected Cloud

Figure 7 Data Storing in Cloud

6. Conclusion

It has been demonstrated through experimentation that the solar PV, WECS, and battery monitoring utilising the Internet of Things with Arduino works well. This was accomplished by monitoring the parameters successfully through the internet. The system that was built not only monitors the parameters of the solar PV, WECS, and battery, but it also manipulates the data and produces the report according to the requirement. For instance, it may compute the unit plot and produce the total units that were generated in a given month. Additionally, it syncs all of the parameters to the cloud at the appropriate times. The user will be able to analyse the state of the many parameters in the solar PV, Wind Energy Conversion System, and battery with the help of this.

References

1. *National Institute of Standards and Technology (NIST). Guide to Industrial Control Systems, 2011*
2. *Centre for the Protection of National Infrastructure (CPNI). Good Practice Guide, Process Control and SCADA Security, 2008*
3. *J. D. M Edgar. Immunology. Elsevier Churchill Livingstone. Edinburgh, 2006*
4. *E. Knapp. Industrial network security: securing critical infrastructure networks for smart grid, scada, and other industrial control systems. Waltham, MA 02451: Elsevier, 2011. [E-book] Available:Books24x7*
5. *P. Giura and W. Wang. "A Context-Based Detection Framework for Advanced Persistent Threats," in 2012 International Conference on Cyber Security, pp.69-74 .*
6. *Fortinet. "Threats on the Horizon- Rise of Advanced Persistent Threats,"2013. [Online]. Available:http://www.fortinet.com/sites/default/files/solutionbrief/threats-on-thehorizon-rise-of-advanced-persistent-threats.pdf. [July 15, 2014]*
7. *N. Virvilis, D. Gritzalis, and T. Apostolopoulos. "Trusted Computing vs.Advanced Persistent Threats: Can a Defender Win This Game?," in 2013 IEEE 10th International Conference on Autonomic and Trusted Computing (UIC/ATC), pp. 396-403.*
8. *Kaspersky." Kaspersky Lab Identifies 'MiniDuke', a New Malicious Program Designed for Spying on Multiple Government Entities and Institutions Across the World," 2013. [Online]. [November 3, 2014].*
9. *R. Radvanovsky and J Brodsky. Editor, Handbook of Scada/Control Systems Security. London: CRC Press, 2013. [E-book] Available: Books24x7.*
10. *PonemonInstitute. "2014 State of EndpointRisk,"2014.[Online]. Available: https://www.lumension.com/Lumension/media/graphics/Resources/2014 -state-of-the-endpoint/2014-State-of-the-Endpoint-WhitepaperLumension.pdf. [October 7, 2014].*
11. *M. Krotofil and D. Gollmann. "Industrial Control Systems Security: What is happening?," in Industrial Informatics (INDIN), 2013, 11th IEEE International Conference, pp. 664-669.*
12. *R. S. H. Piggin. "Emerging Good Practice for Cyber Security of ICS and SCADA," in System Safety, incorporating the Cyber Security Conference 2012, 7th IET International Conference,pp. 1-6.*
13. *M. Bere. "A Preliminary Review of ICS Security Frameworks and Standards Vs. Advanced Persistent Threats," in press.*
14. *F, Skopik, I Friedberg and R Fiedler. " Dealing with advanced persistent threats in smart grid ICT networks," in .Innovative Smart Grid Technologies Conference, ISGT, 2014 pp. 1-5.*
15. *A. Averbuch and G. Siboni., G. "The Classic Cyber Defense Methods Have Failed - What Comes Next,". Military and Strategic Affairs, Vol 5, no 1, pp 45-58, May 2013. [Online]. Available: http://doaj.org/. [Accessed: July. 4, 2014].*
16. *J. deVries, H.Hoogstraaten, J. van den Berg and S. Daskapan. "Systems for Detecting Advanced Persistent Threats: A Development Roadmap Using IntelligentData Analysis," in Cyber Security International Conference, 2012, pp. 54-61.*
17. *P. Bhatt, T, E Yano and P,M Gustavsson. "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks," in IEEE 8th International Symposium Service Oriented System Engineering SOSE, 2014, pp.390 -395.*
18. *M. Chapple, and D. Seidl. Cyberwarfare: information operations in a connected world. Burlington, Jones and Bartlett Learning, 2015. [Ebook]. Available: Books24x7.*
19. *E. G. Amoroso. Cyber Attacks: Protecting National Infrastructure. Burlington, Elsevier , 2011. [E-book]. Available:Books24x7.*
20. *N. Virvilis and D. Gritzalis. "The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?," in Eighth International Conference Availability, Reliability and Security ARES, 2013, pp. 248 –254.*
21. *P. Parham. The Immune System (Third Edition). Garland Science. New York, 2009.*
22. *A. K. Abbas, A, H Lichtman, and S Pillai. Basic Immunology (forth edition). Elsevier Saunders. Philadelphia, 2014.*
23. *Cohen, and L. A. Segel. Design Principles for the Immune System and Other Distributed Autonomous Systems. Cary, NC, USA: Oxford University Press, 2001. [E-book]. Available: http://www.ebrary.com.*
24. *S. A. Mohamed, R A Ammar and S Rajasekaran. "Artificial Immune Systems: Models, Applications, and challenges," in 27th Annual ACM Symposium on Applied Computing, 2012, pp. 256-258.*
25. *E. Hart and J. Timmis (2008). "Application areas of AIS: The past, the present and the future". Applied Soft Computing, Vol 8, no1, pp 191-201, January 2008. [Online]. Available: (http://www.sciencedirect.com/science/article/pii/S1568494607000087) [Accessed, January 28, 2015].*
26. *V. D. Kotov and V. I. Vailyev. "Artificial immune system based intrusion detection system," in Artificial immune system based intrusion detection system, SIN , 2009, pp. 207-12.*
27. *Z. Sadeghi and A. S. Bahrami. "Improving the Speed of Network Inrusion Detection." Aerospace and Electronic Systems, IEEE Transactions, Vol 31, no 3, pp. 1193 – 1198, July 1995. [Online]. Available: http://ieeexplore.ieee.org/. [Accessed January 28, 2015].*
28. *A.Somayaji, M. Locasto and J. Feyereisl. "Panel: The future of biologically-inspired Security: Is there anything left to learn," in Workshop on New Security Paradigms, NSPW, 2007, pp. 49-54.*