IJoCED

Indonesian Journal of Computing, Engineering, and Design

Journal homepage: http://ojs.sampoernauniversity.ac.id/index.php/IJOCED

Bridging Internet of Things and Wireless Sensor Networks: Applications and Challenges

S. Shahriar[1], I. Rahaman[2], A. Bin Karim[1], M. M. Hasan[3], F. Chowdhury[3], M. Sarker[2]*

[1] Dept. of Mechatronics Engineering, RUET, Rajshahi-6204, Bangladesh
[2] Dept. of Electrical & Electronic Engineering, RUET, Rajshahi-6204, Bangladesh
[3] Dept. of Mechanical Engineering, RUET, Rajshahi-6204, Bangladesh

Correspondence: E-mail: asif.mte.148004@gmail.com

ABSTRACT

With the increasing demand of Wireless Sensor Networks (WSNs) innovations, it cuts numerous zones mobile communication, cloud computing and embedded system in modern living. Internet of Things (IoT) is widely used in environmental condition monitoring, logistic support and interfacing sensors and actuators wirelessly, which can be controlled from very long distance. This offers the capacity to control the world from a corner of a room. Wherein sensors and actuators operate reliably with the help of IoT. Wireless data transmission that uses Radio Frequency (RF) has major technical burdens and security vulnerability. The IoT replaced RF as it provides secure transmission capabilities. In this paper, we exhibit a technical overview of WSNs and IoT especially their drawbacks and challenges. Additionally, this paper discusses the progress of the WSNs and IoT innovation.

ARTICLE INFO

Article History:
Received 13 Sept 2019
Revised 05 Mar 2020
Accepted 23 Mar 2020
Available online 03 April 2020

Keywords:
Internet of Things,
Wireless Sensor Networking,
Wireless Communication,
Secure Wireless Transmission,
RF.

1. INTRODUCTION

Internet of Things (IoT) represents a worldwide network of uniquely addressable interconnected objects. According to Gubbi *et al.* (2013), IoT is an "interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation with cloud computing as the unifying framework". Therefore, the IoT aims to improve one's comfort and efficiency by enabling cooperation among smart objects. The standard IoT usually consists of many Wireless Sensor Networks (WSNs) and Radio Frequency Identification Devices (RFID). WSNs is a paradigm that was tremendously explored by the research community in the last two decades (Oppermann *et al.*, 2014). A WSN consists of smart sensing devices that can communicate through

direct radio communication while RFID devices are not as sophisticated. They mainly consist of two parts: an integrated circuit with some computational capabilities and an antenna for communication. The term "Internet-of-Things" was first introduced by Kevin Ashton to describe how IoT can be created by "adding radio-frequency identification and other sensors to everyday objects" (Altolini *et al.*, 2013). Over time, the term has gained more meanings. In this paper, the IoT is defined as a system of uniquely identifiable objects (things) and virtual addressability that would create an Internet-like structure for remote locating, sensing, operating, and/or actuating of entities, which we would term internet connected-constituents (ICCs). Sections 2 to 5 review useful but overlapping conceptualizations of IoT from various literature across the disciplines of strategy, operations management/manufacturing, systems theory, and information systems.

The IoT is a novel paradigm shift in IT arena. The "Internet" in IoT is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies (Mallik, 2019). Today, more than 100 countries are linked into exchanges of data, news and opinions through internet. According to Internet World Statistics, as of 31 December 2011, there was an estimated of 2,267,233,742 internet users worldwide. This signifies 32.7% of the world's total population is using Internet. Even internet is going into space through Cisco's Internet Routing in Space (IRIS) program in the coming fourth years. Meanwhile, the "Things" in IoT can be any object or person that is distinguishable. Everyday objects include not only electronic devices we encounter and use daily and technologically advanced products such as equipment and gadgets, but "Things" that we do not do normally think of as electronic at all—such as food, clothing and furniture, materials, parts and equipment, merchandise and specialized items, landmarks, monuments and works of art and all the miscellany of commerce, culture and sophistication (Mallik *et al.*, 2019). In other words, "Things" can be both living things like person, animals—cow, calf, dog, pigeons, rabbit etc., plants—mango tree, jasmine, banyan and so on and non-living things like chair, fridge, tube light, curtain, plate etc. any home appliances or industry apparatus.

With the expected growth in world population, the demand for energy will continuously increase. Current power grids were built decades ago, and even though they are regularly upgraded, their capability to fulfil future demands is uncertain. Existing reserves of fossil fuels are limited and impose harmful emissions, making social and environmental implications and impact inevitable. The result of this current state is the transition of the traditional centralized grid towards a distributed hybrid energy generation system that heavily relies on renewable energy sources, such as wind and solar systems (Lund *et al.*, 2015), biomass, fuel cells, and tidal power. Smart grid is a concept that integrates information and communication technologies (ICT) with grid power systems, to achieve efficient and intelligent energy generation and consumption (Stojkoska & Trivodaliev, 2017). It is characterized by a two-way flow of both electricity and information. Approaches in smart grid include novel solutions that would effectively exploit the existing power grid to reduce or eliminate blackouts, voltage sags and overloads. Utilities

could benefit, as the load demand in critical situations would decrease. If demand is greater than the total generation, these systems could prevent the grid failure or major blackouts, and increase the reliability, quality, security and safety of the power grid.

The concept of IoT, combined with smart metering, has the potential to transform residential houses, homes and offices into energy-aware environments. There is an increasing interest in the research community to incorporate the IoT paradigm in the smart grid concept, particularly in smart home solutions. The trends of web search popularity for the terms: Internet of Things, Smart Grid and Smart Home since 2004 are shown in **Figure 1**. From **Figure 1**, it can be projected that the interest for the terms Internet of Things and Smart Home are continuously increasing.

2. TOOLS OF IOT TECHNOLOGY

2.1. Wireless Sensor Networks (WSNs)

WSNs refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, SenSys, and EWSN (J. Yick *et al.*, 2008; A. Kumar, 2017; F. K. Shaikh and S. Zeadally, 2017). Typically, each sensor network node has several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source which is usually a battery or an embedded form of energy harvesting. **Figure 2** illustrates the schematic of wireless sensor networking. It can be seen there are communications between cluster heads. Meanwhile, each member node in one cluster sends out information to their cluster head. Some of the cluster head sends information to the BS, which then relay the information to the Satelite-Internet-Mobile communication, then to the control center.

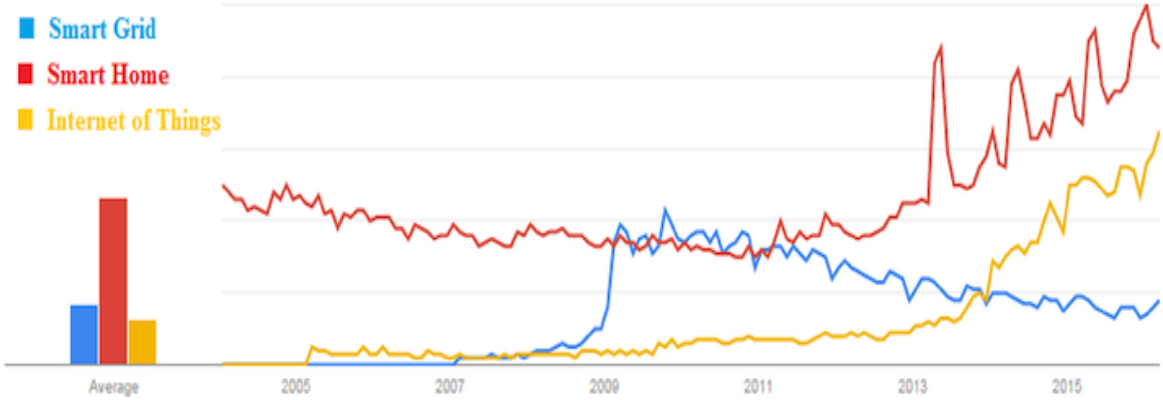

Figure 1. Interest over time according to Google trends since 2004 for terms Internet of Things, Smart Grid and Smart Home (Stojkoska & Trivodaliev, 2017).

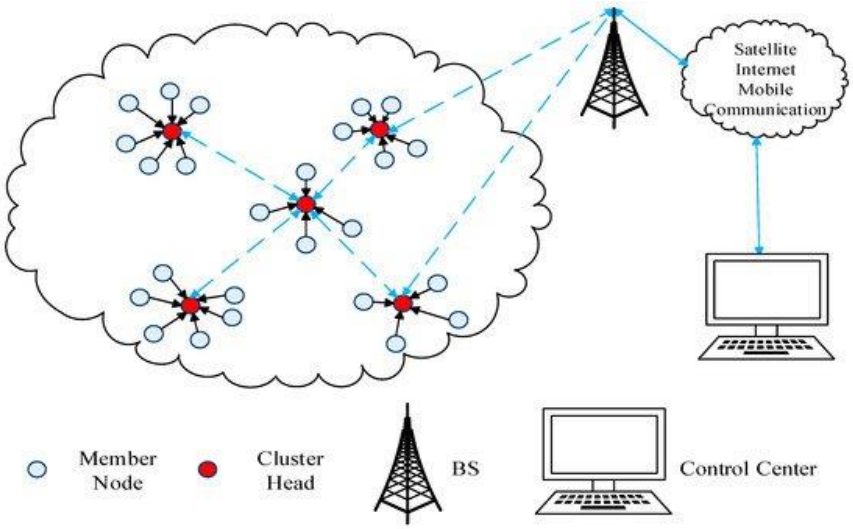

Figure 2. Wireless sensor networking terminology (Radhappa *et al.*, 2018; Zhao *et al.*, 2018).

2.2. Middleware

Middleware refers to a software layer interfered between computer applications to make it simpler for the software developers to achieve real time communication between input and output. The middleware was used to hide the details of different technologies to free IoT developers from software services that are not directly related to the specific IoT application. Middleware expanded its popularity in the year of 1980's because of its vital role in shortening the addition of different legacy technologies into new ones. It also added the development of new services with the DCS (distributed computing system).

2.3. Cloud Computing

Both IoT and the Cloud computing have a great relationship. The IoT provides enormous amounts of a data whereas cloud computing is required to offer a pathway to store and prevent the data loss. Thus, cloud computing helps to increase the efficiency and control movement of IoT (Stergiou *et al.*, 2018; Varghese & Buyya, 2018; Amoore, 2018; Karim *et al.*, 2018). One can save the valuable time and the cost during operating data and can use the data without any redundancy by using Cloud Computing. The cloud computing architecture can be seen in **Figure 3**.

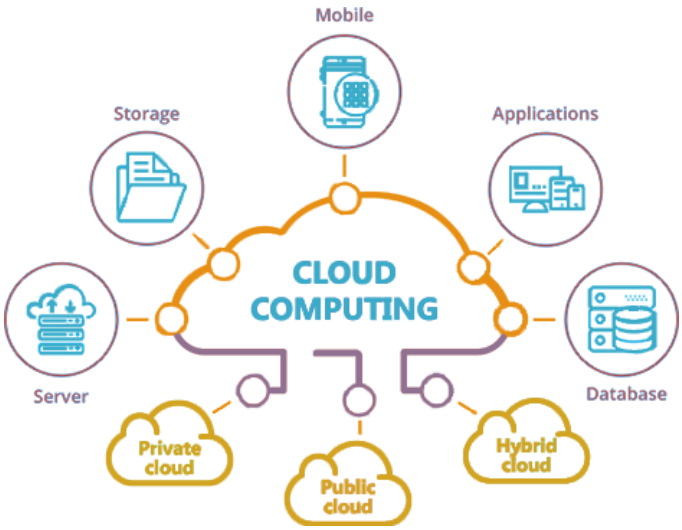

Figure 3. Cloud Computing Architecture.

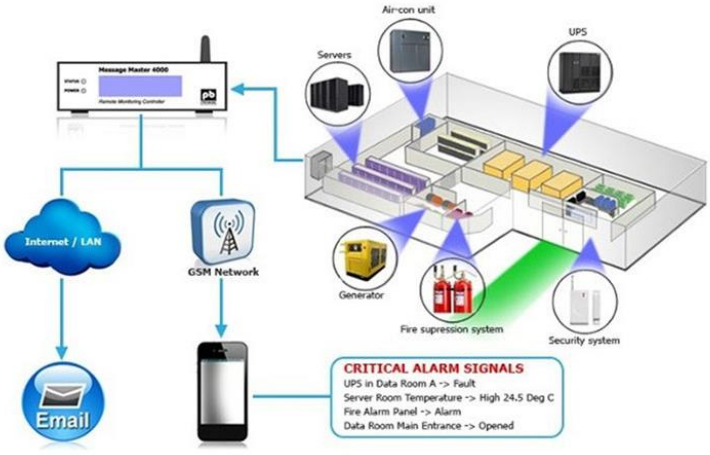

Figure 4. Environmental Condition Monitoring using WSN.

3. NETWORKING APPLICATIONS

IoT and WSNs were originally motivated by military applications, which ranged from large scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection.

3.1. Environment Monitoring

In environmental monitoring, sensors are used to monitor a variety of environmental parameters or conditions. Environmental monitoring is one of the earliest applications of sensor networks. Sensors can be deployed on the ground or under water to monitor air or water quality. For example, water quality monitoring can be used in the hydrochemistry field.

Sensors can be used to monitor biological or chemical hazards in locations, for example, a chemical plant or a battlefield. Sensors can be densely deployed in an intended region to detect natural or non – natural disasters (Barzegaran *et al.*, 2019; Kelly *et al.*, 2013; Garcia *et al.*, 2018; Saravanan *et al.*, 2018). The schematic of environmental monitoring using WSNs are illustrated in **Figure 4**.

3.2. Military Application

Due to ease of deployment, self-configurability, untended operation, and fault tolerance, sensor networks will play more important roles in future military C3I (Command, Control, Communications and Intelligence) systems and make future wars more intelligent with less human involvement. Sensors can be mounted on unmanned vehicles, tanks, fighter planes, submarines, missiles, or torpedoes to guide them around obstacles to their targets and lead them to coordinate with one another to accomplish more effective attacks or defences (Balaji *et al.*, 2018; Shrestha & Hale, 2019).

Sensor nodes can be deployed around sensitive objects, for example, atomic plants, strategic bridges, oil and gas pipelines, communication centers, and military headquarters, for protection purpose. Sensors can be deployed for remote sensing of nuclear, biological, and chemical weapons, detection of potential terrorist attacks, and reconnaissance. Sensors can be deployed in a battlefield to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

3.3. Health Care Application

WSNs can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care ex-

penditures in the current health care systems (Amin *et al.*, 2018; Almarashdeh *et al.*, 2019; Ayyildiz *et al.*, 2019). Wearable sensors can be integrated into a Wireless Body Area Network (WBAN) to monitor vital signs, environmental parameters, and geographical locations, and thus allow long term, non-invasive, and ambulatory monitoring of patients or elderly people with instantaneous alerts to health care personal in case of emergency. It allows for immediate reports to users about their current health statuses, and real-time updates of users' medical records (Hrytskiv *et al.*, 1998; Griggs *et al.*, 2018; Manogaran *et al.*, 2018). The healthcare monitoring by using IoT and WSN are illustrated in **Figure 5**.

3.4. Industrial Process Control

Tiny sensors can be embedded into the regions of a machine that are inaccessible by humans to monitor the condition of the machine and alert for any failure (Scott, 2018; Peres & Fogliatto, 2018). For example, wireless sensors can be installed at production and assembly lines to monitor and control production processes. Chemical plants or oil refineries can use sensors to monitor the condition of their miles of pipelines (Deshmukh *et al.*, 2018). In industry, WSNs can be used to monitor manufacturing processes or the condition of manufacturing equipment.

3.5. Security and Surveillance

Acoustic, video, and other kinds of sensors can be deployed in buildings, airports, subways, and other critical infrastructure, for example, nuclear power plants or communication centers to identify and track intruders and provide timely alarms and protection from potential attacks.

3.6. Home Intelligence

WSNs can be used to provide more convenient and intelligent living environments for human beings. Wireless sensors can be embedded into a home and connected to form an autonomous home network. Wireless sensors can be used to remotely read utility meters in a home, for example, water, gas, or electricity, and then send the readings to a remote center through wireless communication. In addition to the above applications, self-configurable WSNs can be used in many other areas, for example, disaster relief, traffic control, warehouse management, and civil engineering.

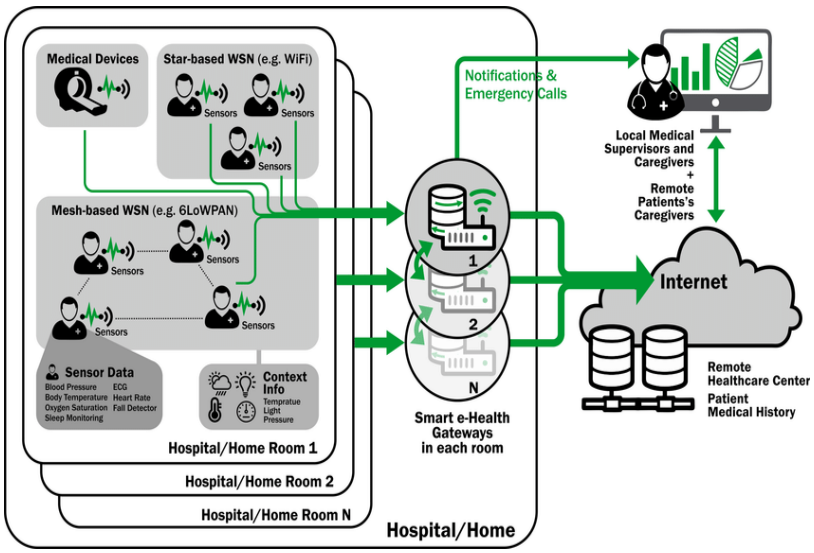

Figure 5. Healthcare Monitoring using IoT and WSN.

4. NETWORK DESIGN OBJECTIVES

4.1. Small Node Size

Reducing node size is one of the primary design objectives of sensor networks. Sensor nodes are usually deployed in a harsh or hostile environment in large numbers. Reducing node size can facilitate node deployment, and reduce the cost and power consumption of sensor nodes.

4.2. Low Node Cost

Reducing node cost is another primary design objective of sensor network. Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, it is important to reduce the cost of sensor nodes so that the cost of the whole network is reduced.

4.3. Low Power Consumption

Reducing power consumption is the most important objective in the design of a sensor network. Since sensor nodes are powered by battery and it is often very difficult or even impossible to change or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged (George *et al.*, 2018).

4.4. Self – Configurability

In sensor networks, sensor nodes are usually deployed in a region of interest without careful planning and engineering. Once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

4.5. Scalability

In sensor networks, the number of sensor nodes may be on the order of tens, hundreds, or thousands. Network protocols designed for sensor networks should be scalable to different network sizes.

4.6. Adaptability

In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

4.7. Reliability

For many sensor network applications, it is required that data be reliably delivered over noisy, error-prone, and time-varying wireless channels. To meet this requirement, network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery.

4.8. Fault Tolerance

Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing, and self-recovering.

4.9. Security

In many military applications, sensor nodes are deployed in a hostile environment and thus are vulnerable to adversaries. In such situations, a sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks (Khan & Salah, 2018; Tonyali *et al.*, 2018).

4.10. Channel Utilization

Sensor networks have limited bandwidth resources. Thus, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

4.11. Quality of Service Support

In sensor networks, different applications may have different Quality of Service (QoS) requirements in terms of delivery latency and packet loss. Some applications, for example, fire monitoring, are delay sensitive and thus require timely data delivery. Other applications, for example, data collection for scientific exploration, are delay tolerant but cannot stand packet loss (Viriyasitavat *et al.*, 2019; Tello-Oquendo *et al.*, 2019; Shahadat *et al.*, 2019). Thus, network protocol design should consider the QoS requirements of specific applications.

5. NETWORK DESIGN CHALLENGES

5.1. Limited Hardware Resources

Sensor nodes have limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

5.2. Massive and Random Deployment

Most sensor networks consist of large number of sensor nodes, from hundreds to thousands or even more. Node deployment is usually application dependent, which can be either manual or random. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. The sensor nodes must autonomously organize themselves into a communication network before they start to perform a sensing task.

5.3. Dynamic Environment

A sensor network usually operates in a dynamic and unreliable environment. On one hand, the topology of a sensor network may change frequently due to node failures, damages, additions, or energy depletion. On the other hand, sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. The connectivity of the network may be frequently disrupted because of channel fault or signal attenuation.

5.4. Diverse Application

Sensor networks have wide range of applications. The requirements for each application may vary significantly. No network protocol can meet the requirements of all applications. The design of sensor networks is application specific.

5.5. Limited Energy Capacity

Sensor nodes are battery powered and thus have very limited energy capacity. This constraint presents many new challenges in the development of hardware and software, and the design of network architectures and protocols for sensor networks. To prolong the operational lifetime of a sensor network, energy efficiency should be considered in every aspect of sensor network design, not only hardware and software, but also network architectures and protocols.

6. CONCLUSION

The progress of WSNs and IoT innovation have been presented in this paper. Some important measures along with security protocols which can be very useful for further studies are also reviewed. From the discussion on network design objectives and network design challenges, a new research area on network design can be created by combining some of the objectives and the challenges. It is expected that the review done in this paper would be helpful for the network designer and researcher.

ACKNOWLEDGEMENTS

The authors are thankful to Avijit Mallik (Dept. of Mechanical Engineering, RUET) and his supervisor Dr. M. M. Z. Shahadat (Professor, Dept. of Mechanical Engineering, RUET) for their undeniable help and supports to conduct this research.

REFERENCES

Almarashdeh, I., Alsmadi, M. K., Farag, T., Albahussain, A. S., Badawi, U. A., Altuwaijri, N., Almaimoni, H., Asiry, F., Alowaid, S., Alshabanah, M., Alrajhi, D., Fraihet, A. Al, & Jaradat, G. (2019). *Real-time elderly healthcare monitoring expert system using wireless sensor network*. http://arxiv.org/abs/1908.03518.

Altolini, D., Lakkundi, V., Bui, N., Tapparello, C., & Rossi, M. (2013). Low power link layer security for IoT: Implementation and performance analysis. *2013 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013*, 919–925. https://doi.org/10.1109/IWCMC.2013.6583680.

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Kumar, N. (2018). A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Generation Computer Systems*, *80*, 483–495. https://doi.org/10.1016/j.future.2016.05.032.

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography*, *42*(1), 4–24. https://doi.org/10.1177/0309132516662147.

Ayyildiz, C., Erdem, H. E., Dirikgil, T., Dugenci, O., Kocak, T., Altun, F., & Gungor, V. C. (2019). Structure health monitoring using wireless sensor networks on structural elements. *Ad Hoc Networks*, *82*, 68–76. https://doi.org/10.1016/j.adhoc.2018.06.011.

Balaji, G. N., Nandhini, V., Mithra, S., Priya, N., & Naveena, R. (2018). IOT based smart crop monitoring in farm land. *Imperial Journal of Interdisciplinary Research (IJIR) Peer Reviewed-International Journal*, *4*.

Barzegaran, M., Cervin, A., & Pop, P. (2019). Towards quality-of-control-aware scheduling of industrial applications on fog computing platforms. *IoT-Fog 2019 - Proceedings of the 2019 Workshop on Fog Computing and the IoT*, 1–5. https://doi.org/10.1145/3313150.3313217.

Deshmukh, P. V. M., Adat, D. M., Ladgaonakar, B. P., & Tilekar, S. K. (2018). Designing of an embedded system for wireless sensor network for hazardous gas leakage control for industrial application. *I-Manager's Journal on Embedded Systems*, *6*(2), 1–9.

Garcia, G. T., Sanchez, V. M., Lopez Marin, C. N., Cortez, J. I., Rios Acevedo, C. A., Gonzalez, G. S., Hernandez Ameca, J. L., & Molina Garcia, M. D. C. (2018). Wireless sensor network for monitoring physical variables applied to green technology (IoT green technology). *European Journal of Electrical Engineering and Computer Science*, *2*(2). https://doi.org/10.24018/ejece.2018.2.2.15.

George, A. M., Kulkarni, D. S. Y., & George, D. V. I. (2018). A Survey on ultra low power design techniques for IOT application. *Current Trends in Information Technology*, *7*(3), 9–16. http://computerjournals.stmjournals.in/index.php/CTIT/article/view/8.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T.

(2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, *42*(7), 1–7. https://doi.org/10.1007/s10916-018-0982-x.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010.

Hrytskiv, Z., Hrytskiv, Z., Voloshynovskiy, S., & Rytsar, Y. (1998). Cryptography and steganography of video information in modern communications. *Proceedings of the 3rd International Conference on Telecommunications in Modern Satelite, Cable and Broadcasting Services TELSIKS'97*, *1*, 164-167. http://130.203.136.95/viewdoc/summary;jsessionid=505370095487EF560A78C7B04A430D8D?doi=10.1.1.36.9860.

Karim, A. Bin, Hassan, M. Z., Akanda, M. M., & Mallik, A. (2018). Monitoring food storage humidity and temperature data using IoT. *MOJ Food Processing & Technology*, *6*(4), 400–404. https://doi.org/10.15406/mojfpt.2018.06.00194.

Kelly, S. D. T., Suryadevara, N. K., & Mukhopadhyay, S. C. (2013). Towards the Implementation of IoT for Environmental Condition Monitoring in Homes. *IEEE Sensors Journal*, *13*(10), 3846–3853. https://doi.org/10.1109/JSEN.2013.2263379.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022.

Lund, P. D., Mikkola, J., & Ypyä, J. (2015). Smart energy system design for large clean power schemes in urban areas. *Journal of Cleaner Production*, *103*, 437–445. https://doi.org/10.1016/j.jclepro.2014.06.005.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 77–92. https://doi.org/10.22373/cj.v2i2.3453.

Mallik, A., Hossain, S. A., Karim, A. Bin, & Hasan, S. M. (2019). Development of LOCAL-IP based environmental condition monitoring using wireless sensor network. *International Journal of Sensors, Wireless Communications and Control*, *9*(4), 454–461. https://doi.org/10.2174/2210327909666190208161832.

Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P. M., Sundarasekar, R., & Thota, C. (2018). A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems*, *82*, 375–387. https://doi.org/10.1016/j.future.2017.10.045.

Oppermann, F. J., Boano, C. A., & Römer, K. (2014). *A decade of wireless sensing applications: Survey and taxonomy* (pp. 11–50). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40009-4_2.

Peres, F. A. P., & Fogliatto, F. S. (2018). Variable Selection Methods in Multivariate Statistical Process Control: A Systematic Literature Review. *Computers and Industrial Engineering*, *115*, 603–619. https://doi.org/10.1016/j.cie.2017.12.006.

Radhappa, H., Pan, L., Xi Zheng, J., & Wen, S. (2018). Practical overview of security issues in

wireless sensor network applications. *International Journal of Computers and Applications*, *40*(4), 202–213. https://doi.org/10.1080/1206212X.2017.1398214.

Saravanan, K., Anusuya, E., Kumar, R., & Son, L. H. (2018). Real-time water quality monitoring using Internet of Things in SCADA. *Environmental Monitoring and Assessment*, *190*(9), 1–16. https://doi.org/10.1007/s10661-018-6914-x.

Scott, D. M. (2018). Industrial Process Sensors. CRC Press. https://doi.org/10.1201/9781315219950.

Shahadat, M., Mallik, A., & Islam, M. (2019). Development of an automated gas-leakage monitoring system with feedback and feedforward control by utilizing IoT. *Facta Universitatis - Series: Electronics and Energetics*, *32*(4), 615–631. https://doi.org/10.2298/fuee1904615s.

Shrestha, I., & Hale, M. L. (2019). Detecting dynamic security threats in multi-component IoT systems. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 7146–7155. https://hdl.handle.net/10125/60151.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems*, *78*, 964–975. https://doi.org/10.1016/j.future.2016.11.031.

Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. In *Journal of Cleaner Production* (Vol. 140, pp. 1454–1464). Elsevier Ltd. https://doi.org/10.1016/j.jclepro.2016.10.006.

Tello-Oquendo, L., Lin, S. C., Akyildiz, I. F., & Pla, V. (2019). Software-defined architecture for QoS-aware IoT deployments in 5G systems. *Ad Hoc Networks*, *93*, 101911. https://doi.org/10.1016/j.adhoc.2019.101911.

Tonyali, S., Akkaya, K., Saputro, N., Uluagac, A. S., & Nojoumian, M. (2018). Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems. *Future Generation Computer Systems*, *78*, 547–557. https://doi.org/10.1016/j.future.2017.04.031.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849–861. https://doi.org/10.1016/j.future.2017.09.020.

Viriyasitavat, W., Xu, L. Da, Bi, Z., Hoonsopon, D., & Charoenruk, N. (2019). Managing QoS of Internet-of-Things services using blockchain. *IEEE Transactions on Computational Social Systems*, *6*(6), 1357–1368. https://doi.org/10.1109/TCSS.2019.2919667.

Zhao, Z., Xu, K., Hui, G., & Hu, L. (2018). An energy-efficient clustering routing protocol for wireless sensor networks based on AGNES with balanced energy consumption optimization. *Sensors*, *18*(11), 3938. https://doi.org/10.3390/s18113938.