Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
May 2024 5(5), 304–311

EXAMINING THE INFLUENCE OF IOT ON WIRELESS SENSOR NETWORKS

Anand Kumar Dwivedi[1], Virendra Tiwari[2], Akhilesh A. Waoo[3] ✉, Shankar Bera[4]

[1,2,3,4] Department of Computer Science & Engineering, AKS University, SATNA, MP, India

ABSTRACT

We are in the world of the Internet and the Internet makes tasks easier. It is observed that IoT exerts a major effect on wireless systems. Multiple sectors are using the IoT based on wireless systems. IoT and WSNs are working jointly and making the way easier than easy. Now we are not only communicating person to person via a device all over the world but drastic technology which comes and it has simply made life easier, which is IoT (Internet of Things). As the name suggests communication among the things we see via the Internet. Now things will be also connected to the internet and they will behave. In this paper, we will discuss the different areas of uses of IoT along with the internal component of IoT via its architecture and advantages and disadvantages.

Keywords: Cloud, Confidentiality WSN, IoT, Security, IoT Components, Sensors

Corresponding Author

Akhilesh A. Waoo,
akhileshwaoo@gmail.com

DOI
10.29121/shodhkosh.v5.i5.2024.1883

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The way the World Wide Web was influenced started by connecting different computers via connecting media such as wired media, but later on, a wireless mechanism was also introduced, which enhanced the technology and forms of accessing internet data by mobile. Similar mechanisms for the connection of devices moved towards the IoT [1]. So IoT is a trending technology for the connection of different objects to the internet and can transfer data easily. IoT not only connects the devices but also works with several sensors. IoT comprises a broad range of those types of devices that have connected to the WWW [2]. These types of devices collect data by using sensors and actuators and transfer this gathered data through the Internet for further processing. All devices like phones, homes, TVs, etc. must be "smart" such as smart TVs, smartphones, and smart home [3]. The IoT term is Kevin Ashton introduced this, the executive director of the Auto-ID center. In the year of 2003, it became very popular through this.

2. IOT ARCHITECTURE

The architecture of the IoT differs from its functional and its solutions. However, it consists of four main components (Fig 1). They are:

1. Devices/Sensors.

2. Networks and Gateways.
3. A layer of Management service /Cloud.
4. Application layer.

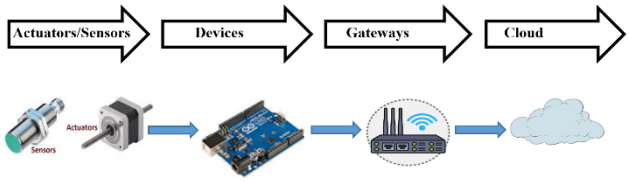

Fig. 1: Components of the IoT

The architecture of IoT is a way to design various components nexus of all things so that they can deliver services in the presence of networks and fulfill the needs of the future.

Here is the list of layers (stages) of IoT that provide solutions for the architecture of IoT (Fig 2).

Actuators and Sensors

Actuators or sensors are the key components of the IoT; they can sense the data and process the data over any network. These types of tools are connected through communication media, such as wired or wireless. Many of the sensors needed connectivity through the sensor gateways. Networking over a personal or localized network is used for the connection of the sensors and actuators [4].

Network and Gateways

When the sensors and actuators are working, they produce a huge amount of data, so to handle this data; high-speed gateways are needed along with the networks for transporting the data. They can use a network like a LAN or WAN.

Edge IT

Before transporting the data into the cloud, this component analyses and preprocesses the data. These are the gateways and both equipment and software. If the data provided by the gateways and sensors is not updated from its earlier values, it is not able to transfer the data over to the cloud, but it also saves the data.

Cloud

This stage processes the collected information through analytics; it comes under management services, and it also does security control as well as management of different devices [5]. Besides this, the cloud also transfers the stored data that is needed by end users in areas such as healthcare, the environment, retail, etc.

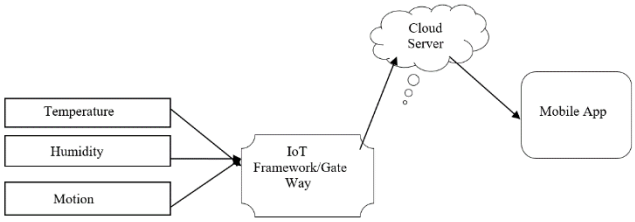

Fig. 2: List of Layers (Stages) of IoT

3. IOT APPLICATIONS IN THE REAL WORLD

The ubiquitousness of the Internet of Things has become a reality; a variety of industries have adopted it [6]. The versatility of IoT makes it an attractive option for so many businesses, organizations, and government agencies that it just doesn't make sense to ignore it [7]. Know more about IoT applications (Fig 3) in various industries below:

IoT in Agriculture

For planting indoors, IoT always monitors and makes proper management of the climate condition concerning the plant in turn to increase the production, but the plant which is outside, the devices that use the IoT technology, can sense the soil, climate as well as nutrients and makes the better decision for fertilizers and so on [8].

IoT in Consumer Use

Citizens, wear IoT devices that provide them the entertainment, health updates, and network connections (Bluetooth and Internet). IoT devices monitor health regularly e. g. Smartwatch, and Smartphone [9].

IoT devices for home make a smart home that monitors the environment and controls the things that comfort you when you enter the home [10].

Along with that, the smart lock also uses the IoT devices which enable the enter the appropriate person in the house even, when they do not have a key [11][39].

IoT in Insurance

Like other industries, the insurance industry also uses IoT. They can offer discounts for IoT devices like Fitbit [12]. Fitness tracking enables the insurance to provide individualized coverage and promote better lifestyle choices, which ultimately benefits both the insurer and the consumer [13].

IoT in Manufacturing

IoT is another important factor for manufacturing industries. GPS and RFID technology can help to track any product from its starting in the factory to its original destination store. These IoT sensors can collect information about the tracking as well as the environmental condition concerning the product [14].

IoT in Transportation

As the new mechanism was invented for transportation, everyone has listened to the driverless car (Tesla) or self-driving car. They gather the data from their sensors and execute the process according to the data. GPS also plays a big impact in transportation for navigating the current status of the vehicle [15].

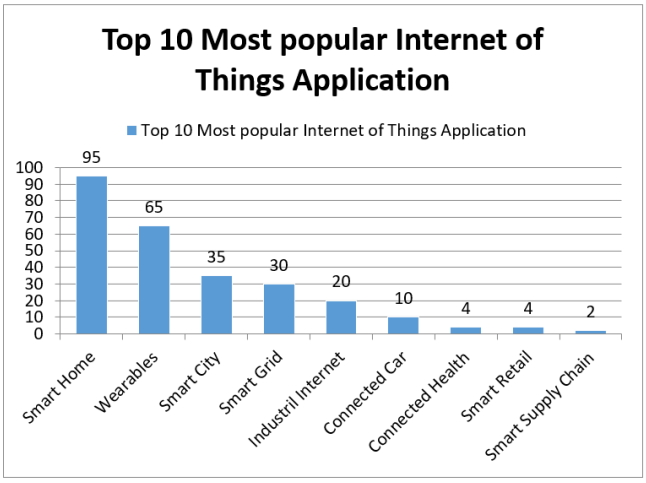

Fig. 3: Top 10 Most Popular IoT Applications

4. WIRELESS SENSOR NETWORK IN IOT

The WSN using IoT is a wireless network with fewer infrastructures used for deploying the number of sensors for monitoring the environmental condition and physical condition, Wireless Sensor Networks (WSNs) have begun to get the focus of academia due to the rapid growth of the wireless medium and embedded electronics. A typical WSN consists

of microscopic pieces called nodes. These nodes have an embedded CPU, a small amount of calculation capability, and some savvy sensors. Nodes use these sensors to keep an eye on outside conditions like humidity, pressure, heat, and vibration. A typical WSN node includes four parts: an antenna, a transceiver, a unit that handles data, and a power unit. By letting nodes connect with others and communicate data collected by their sensors, these appliances accomplish forth crucial tasks. A centralized system requires nodes to interact with others. The idea of the internet emerged as an outgrowth of this system's necessity. [16][38].

5. WSN-RELATED IOT CONSTRAINTS

The complexity of IoT is achieved by various heterogeneous objects being shown and communicating in various contexts and it also complicates the deployment of security measures [17]. Existing WSN security research largely handles only personal problems without considering the implications of the IoT's tenets and distinctive features laid out in this document [18] (Fig 4).

Real-time scheduling

It is a demanding topic for sensor networks with limits on resources. In that instance, the IoT system has an effective service gateway design to minimize the amount of data that must be supplied. Using sophisticated data-driven middleware designed to provide real-time information only when scans reach a threshold and constantly examining user data [19].

Security and confidentiality

In real-world applications, privacy, safety, and trust are also important worries. Different levels of safety may have to be gained in a challenging way. These safeguards work for M2M deployments where there is already a trust connection between the server and the device [20]. With this "IP to the field" concept, sensor nodes have additional roles in addition to the regular capacities. Therefore, with this included responsibility, the sensor nodes will face new tasks or issues. We will deal with the following potential tasks: security, service quality (QoS), and network configuration. The following themes are examined [21].

The configuration

Sensor nodes must manage a range of duties aside from taking care of QoS and security, including networking for new nodes joining the network [22], ensuring self-healing by detecting and eliminating faulty nodes, and addressing management for the development of scalable connections, among others. The newest Internet node's power to manage her is not a regular feature, though [23]. Therefore, for this network setup to work correctly, the user has to set up the required applications and take proper precautions to prevent device failures.

Reliability of data

When a malicious node joins the network and injects data that is wrong or when a volatile wireless channel plays with the original data, the data integrity of the WSN can be threatened [24]. Data integrity will be changed, for instance, if a mobile node sends untrue data to packets received by the BS. Still, an unreliable network may be blamed for data loss or alteration. As a result, it is essential to maintain data integrity throughout data packet transmission [25].

The concept of confidentiality

Reliability is one of the numerous challenges linked to security in the Web of Things. All data is kept private by choosing encryption features like Triple DES, AES block ciphers, and Blowfish, which all use common and shared secret keys [26]. However, as a security measure, the encryption process is insufficient to guarantee the private nature of the data and information. To successfully spread highly sensitive information, the attacker can perform traffic analysis on the data that is encrypted. Also, the malicious node can use a common group keypad to successfully undermine the functionality of other sensor nodes' capabilities. before waking up and understanding personal information.

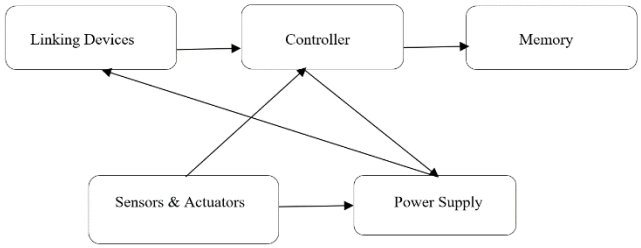

Fig.4: IoT Network

The availability

By exploiting compromised nodes, WSNs can be exploited [27]. An additional fee should be levied to incorporate the WSN safeguarding algorithms for encryption. Researchers have, however, created essential methods where some up-to-date the code and reused it whereas other investigators use additional communications to achieve those goals. In addition, methods for accessing the data have been developed. Therefore, availability is essential for maintaining the operational services of WSNs. Furthermore, it promotes maintaining the entire network up until its conclusion.

Aggregation of data

As was earlier said, WSNs serve as vital IoT constituents that have grown in many kinds of real-time applications. WSN nodes are typically small, devices that are powered by batteries. So, for WSN data aggregation, the network's durability is of the greatest significance [28]. Numerous issues, involving higher usage of energy, or raised endurance and energy ineptitude, were discovered during the data collection procedures [37].

6. ADVANTAGES OF IOT APPLICATION

IoT application (Fig 5) has several benefits while in use. Some of them are listed below:

Provide Security

User can monitor their home by using their smartphone and ability to control them. It provides the personal safety of the home [29].

Connected

You and your whole family can be connected from the network.

Healthcare

Users can get real-time health updates without the doctor's visit and also decide on treatment when an emergency there.

Cost-effective operations of a business

All operations related to the business can be tracked and operated efficiently by using the IoT; it manages the product, inventory, tracking orders, customer satisfaction, etc. [30].

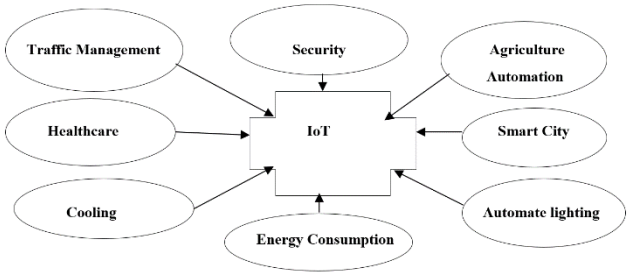

Fig.5: Applications of IoT

7. DISADVANTAGES OF IOT APPLICATIONS

Apart from the advantages, there are some disadvantages too:

Issue of Privacy

Hackers can steal your confidential information as they hack the network by which you are connected [31].

Increases Unemployment

The unskilled laborers may have lost their jobs.

Dependency

Once the user gets the decision from the system, they may always be dependent.

The exploitation of technological advances and the global web

In IoT, we are dependent on the internet and it makes people unintelligent as they remain on devices in place of doing work physically and people become lazy.

8. CHALLENGES IN WSNS

While the networks of sensors and other autonomous systems possess a lot in common, they must contend with plenty of unique issues and obstacles. Those constraints reflect an impact on how a WSN is designed, which led to algorithmic processes and protocols that are unusual and not found in other distributed systems. There are a few steps described below.

Flexibility

The scale of social security numbers varies, possibly ranging from a handful of sites to several dozen. Additionally, the deployment density can be altered appropriately. The node's density could become so high all over the high-resolution data-gathering process that each node has an abundance of neighbors within its transmission range. The protocols used in SNs should be adaptable to various levels and capable of successfully keeping up with performance [32].

Topology of the Sensors Network

Despite WSNs making progress in several fields, the networks continue to have limited Assets in the Energies domain, Processing capacity, memory storage, and communication abilities [33]. Energy resources are the most important of all the aforementioned obstacles, as indicated by the vast array of algorithms, techniques, and protocols that have been developed to conserve energy. and, thus, incorporate the generation of the network. A variety of states that among several vital features that could reduce the rates of energy consumption in WSNs is topology maintenance [34].

The Use of Power

As was previously stated, most WNS problems were brought on by a lack of power supplies. The links' dimensions affect how big a power source is as a power source. As a result, whenever expanding hardware and software, careful thought must be paid concerning how efficient energy is economically. Knowledge enlargement, for instance, uses less energy during radio transmission, but it spends greater amounts of power during manipulation, calculation, as well as filtration [35]. A subdivision of nodes may be turned off in some applications to save energy, while some applications require all nodes to operate concurrently. The energy tactics moreover entail surroundings [36].

9. CONCLUSION

Through a variety of technologies, IoT has been gradually bringing a sea of technological changes into our daily lives, which in turn helps to make our lives easier and more comfortable though few are drawbacks too. IoT has many applications across all industries, including healthcare, manufacturing, transportation, education, government, mining, and habitat, amongst others. Issues with WSNs, from applications to difficulties from the technological viewpoint. In essence, it is required to go over the most appropriate technology to be used for creating a WSN as well as the

communication processes (such as signal processing, topology, methods, etc.). The application constraints play a major role in these decisions, amid other factors.

CONFLICT OF INTERESTS

None

ACKNOWLEDGMENTS

None

REFERENCES

Perera C.; Harold C.; Liu H.; Jayawardena S. (2015). The Emerging Internet of Things marketplace From an Industrial Perspective: A Survey, *IEEE Transactions on emerging topics in computing*||.

Al-Fuqaha; Guizani M.; Mohammadi M.; Aledhari M.; Ayyash M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376.*

Luigi; I. Antonio; M. Giacomo. The Internet of Things: A survey. *Science Direct Journal of Computer Networks, 2010 Volume 54, Pages: 2787–2805.*

W. Miao; L. Ting; L. Fei, ling S., Hui D. (2010). Research on the architecture of the Internet of Things.

Sichuan Province; China*. IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE) Pages: 484-487.*

Ms.Neha K.; Vinita S., Sudhanshu N. (2016). A Survey paper on RFID Technology, its applications, and Classification of Security/Privacy Attacks and Solutions*, IRACST -International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol.6, No4.*

Edge computing - http://searchdatacenter.techtarget.com/definition/edge-computing.

IoT - The Architecture of IoT Gateways - Internet of Things Protocols and Standards -

R. Abdmeziem; D.Tandjaoui; "Internet of Things: Concept, Building blocks, Applications and Challenges, Computer and Society, *Cornell University.*

M. S. Islam; G. K. Dey (2019). Precision Agriculture: Renewable Energy Based Smart Crop Field Monitoring and Management System Using WSN via IoT. *International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, pp. 1-6, doi: 10.1109/STI47673.2019.9068017.*

K. Begum; S. Dixit (2016). Industrial WSN using IoT: A survey. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 499-504, doi: 10.1109/ICEEOT.2016.7755660.*

Sarkar S.; Rao K. U.; Bhargav J.; Sheshaprasad S. and Sharma A. C.A. (2019). IoT-Based Wireless Sensor Network (WSN) for Condition Monitoring of Low Power Rooftop PV Panels. *IEEE 4th International Conference on Condition Assessment Techniques in Electrical Systems (CATCON), Chennai, India. pp. 1-5, doi: 10.1109/CATCON47128.2019.CN004.*

G. Thangarasu; P. D. D. Dominic; M. bin Othman; R. Sokkalingam and K. Subramanian, (2019). An Efficient Energy Consumption Technique in Integrated WSN-IoT Environment Operations. *IEEE Student Conference on Research and Development (SCOReD), Bandar Seri Iskandar, Malaysia. pp. 45-48, doi: 10.1109/SCORED.2019.8896238.*

Mahakalkar N.; Pethe R. (2018). Review of Routing Protocol in a Wireless Sensor Network for an IOT Application*. 3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India. pp. 21-25, doi: 10.1109/CESYS.2018.8723935.*

Priyanka M.; S. Leones Sherwin V.; J. Lydia. (2018). Energy Aware Multiuser & Multi-hop Hierarchical –Based Routing Protocol for Energy Management in WSN-Assisted IoT. *3rd International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India. pp. 701-705, doi 10.1109/CESYS.2018.8724073.*

Rakesh K.L.; Amiya K. R.; Suraj Sharma (2019). Building Reliable Routing Infrastructure for Green IoT Network, *IEEE Access 7 129892– 129909, https://doi.org/10.1109/Access.628763910.1109/ ACCESS.2939883.*

Arat F.; Demirci S. (2019). Energy and QoS Aware Analysis and Classification of Routing Protocols for IoT and WSN.*7th International Conference on Electrical and Electronics Engineering (ICEEE), Antalya, Turkey, pp. 221- 225, doi: 10.1109/ICEEE49618.2020.9102614.*

Prakash R.; Kansal P.; Kakar V. K. (2019). Optimized Hybrid Clustered Protocol for IoT Heterogeneous Wireless Sensor Networks," *IEEE Conference on Information and Communication Technology, Allahabad, India, pp. 1-6, doi: 10.1109/CICT48419.2019.9066258.*

https://dx.doi.org/10.29121/shodhkosh.v5.i5.2024.1883 M. Hanady Abdulsalam; Bader A. Ali; EmanAl R.; EmanAl R. (2018). Usage of mobile elements in Internet of Things environment for data aggregation in wireless sensor networks. Comput. Electr. Eng. 72 789–807.

M. Amarlingam; Pradeep K. M.; P. Rajalakshmi; Sumohana S. C.; C.S. Sastry. (2018). Novel Light Weight Compressed Data Aggregation using sparse measurements for IoT networks, J. Network Comput. Appl., Vol. 121, Pages 119-134.

Mr. Muruganandam K.; Dr. Balamurugan B.; Dr. Sibaram K. (2018). Design of Wireless Sensor Networks for IoT Application: A Challenges and survey, ijecs, Page No.: 23790-23795.

J. Claessens. (2008). Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer.

Kang; S.H. (2019). Energy Optimization in Cluster-Based Routing Protocols for Large-Area Wireless Sensor Networks. Symmetry, 11, 37.

Fault management frameworks in wireless sensor networks: A survey Comput. Commun. (2020).

Yao L.; Du. X. (2020). Sensor Coverage Strategy in Underwater Wireless Sensor Networks. Int. J. Comput. Commun. Control.

Chawra V. K. and Gupta G. P. (2022). Memetic algorithm-based energy efficient wake-up scheduling scheme for maximizing the network lifetime, coverage, and connectivity in three-dimensional wireless sensor networks, Wireless Personal Communications, vol. 123, pp. 1507–1522.

Yilmaz E. (2021). A half-duplex two-way relay station assisted cellular uplink and downlink communications," in European Wireless; 26th European Wireless Conference, pp. 1–7.

Alkhamisi N.; M.S.H.; Buhari S.M. (2016). A cross-layer framework for sensor data aggregation for IoT applications in smart cities, IEEE International Smart Cities Conference (ISC2), Trento (2016) 1–6, https://doi.org/ 10.1109/ISC2.2016.7580853.

B. Bamleshwar Rao, Akhilesh A. Waoo. (2021) Advanced System to Identify Users and Devices in IoT using Token-Based Authentication, International Journal of Innovative Science and Research Technology, Volume 6, Issue 10, ISSN: 2456-2165.

Tiwari, Anurag and Waoo, Akhilesh A., IoT based Smart Home Cyber-Attack Detection and Defense (2023). TIJER - International Research Journal | August 2023, Volume 10, Issue 8, Available at SSRN: https://ssrn.com/abstract=4537209.