Study on Smart Home Integrated with IoT

Seyed Ahmad Edalatpanah[1,*] ID **, Nadia Ghasemabadi[2]**

[1] Department of Industrial Engineering, Ayandegan Institute of Higher Education, Tonekabon, Iran; saedalatpanah@gmail.com

[2] Department of Computer Engineering, Institute of Higher Education, Tenekabon, Iran; ghasemabadinadia@gmail.com.

Abstract

The term "smart house" is no longer limited to the centralized, partially automated regulation of environmental systems, whereas the Internet of Things (IoT) is the growth of internet-based services. IoT has more and more applications. The IoT environment is using new technologies more and more frequently. The industrial Wireless Sensor Network (WSN). has already made it one of the uses for IoT is the smart house. Fast advancements in technology and architecture have created a number of difficulties, including how to manage and regulate the entire system and secure servers and smart homes, among others. In this work, the IoT architecture is presented. Homes that can be monitored and controlled remotely by household appliances and devices are known as smart homes. The entire system can be referred to as a "smart home in an IoT environment" or "IoT-based smart houses" when various household devices in smart homes link with the internet using appropriate network architecture and standard protocols. Home automation tasks are made easier by smart homes. In addition to discussing the issues and difficulties faced by the IoT and IoT-enabled smart home systems, this article also offers a few solutions.

1|Introduction

Thanks to the internet, the ability to interact with anybody, anywhere, at any time has revolutionized human life. Technological advancements have dramatically decreased the price of sensors, processors, transmitters, and receivers. So, these items can all be employed in our daily lives [1]. If someone wants to increase the number of internet services available, the internet of Things (IoT) might be considered an increase in internet services [2]. The IoT is a current trend in today's internet.

IOT: the network of computers that will connect to physical objects or things in the actual world using the existing internet infrastructure. Things can be any kind of thing, such as furniture, equipment, automobiles,

etc. The entire system is called the IoT when these devices connect to the internet using a specific infrastructure and accepted protocols [3]–[5].

Things: whether physical or digital, moving or still, objects will play an active role in the overall system. Things will talk to other things; this is known as things-to-things communication. When objects can engage or communicate with humans, this is called things-to-human communication [6]. But the IoT is more than just a futuristic fantasy. It already exists and affects more than just technological advancement. These devices and items communicating via the internet can set up their configurations and run autonomously [7]. The IoT architecture is depicted in *Fig. 1* [8].
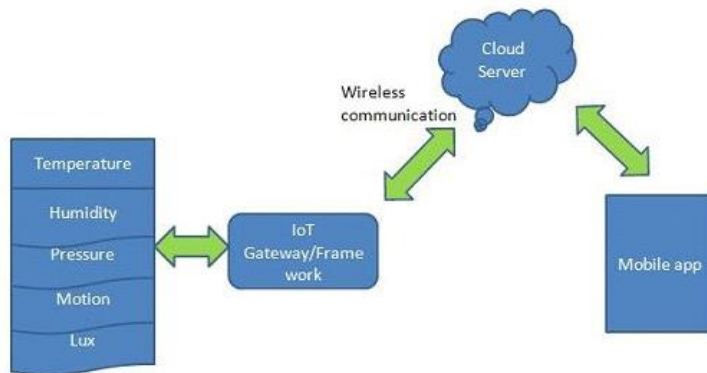

Fig. 1. Architecture of IoT.

Smart home: a smart home is a dwelling or a living space equipped with technology that enables automatic and remote control of all appliances and household gadgets [9]. Users of smart homes may easily monitor and manage all home electronics and appliances online. Home appliances connect utilizing established protocols and a correct network architecture. *Fig. 2* illustrates a fundamental IoT-based concept for smart homes. The entire system may be broken down into two sections: one section includes all of the household appliances, switch modules, and R.F. transmitters and receivers; the second section has all of the interface devices, processors, data collectors, and GPRS modules that will connect to the internet [10].
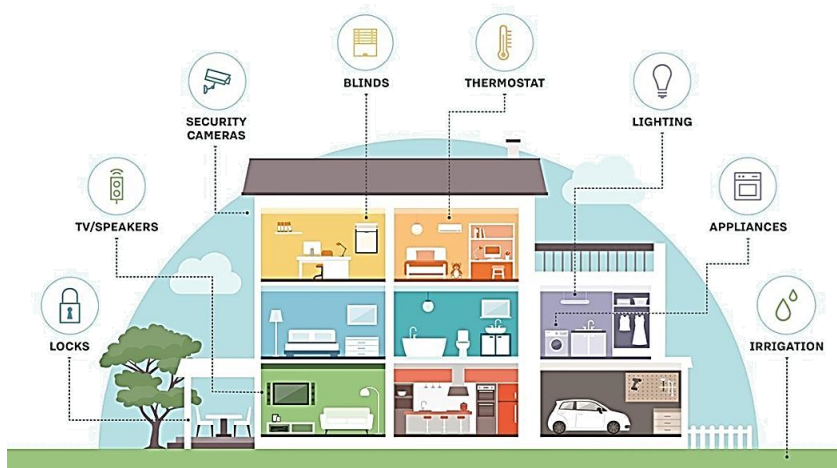

Fig. 2. Basic idea for smart home system using IoT.

Only four domestic appliances are shown in this document for consideration: a light, a fan, a television, and a gas outlet. Yet, the user can connect various gadgets [11]. All of these home appliances will be connected to the switch modules. Any form of a module that modifies its state in response to a signal may be found in a switch module [12]. When a switch module is linked to a device, the related home devices' states also change when the switch module changes its state [2], [4], [8], [13]. It is possible to employ relays as switch modules. It is a commonly known electromagnetic device or relay switch [14]. It magnetically joins two circuits while electrically isolating them. Switch modules will link to the smart central controller via an R.F. transceiver. One transceiver will be included in each switch module, or one transceiver may connect to all switch modules.

Each switch module and device will be identified with a distinct identity [13]. At the intelligent central controller, one R.F. transceiver will connect. R.F. modules speak to one another at a frequency of 433MHz [15]. The 433 MHz spectrum was created specifically for R.F. communication [2], [4]. The smart central controller will be the intermediary between home appliances and the internet server [16].

2 | Related Work

Authors' descriptions of the layered architecture of the IoT-based smart home system can be found in [8]. The application layer, network layer, and sensor layer are the three layers that make up the smart home system. Beginning at the bottom, the sensing layer gathers data from all household appliances and sends it to the network layer in the centre [17]. The network layer uses the internet to transfer data to the topmost application layer, which has a variety of apps at various levels for various uses. The SAMSUNG S3C2440A microprocessor, an ARM-based microcontroller, was employed for data collecting and processing at the sensing layer [8]. Authors of [5] have already designed a reconfigurable smart sensor interface device for industrial Wireless Sensor Network (WSN) in IoT environment using CPLD. This device integrates data collecting, processing, and wired and wireless transmission [18]. The data gathering of several sensor nodes is difficult for industrial WSN in IoT environments. Although microcontrollers have the advantages of low cost and power consumption, when employed as interface devices, they conduct a task via an interrupt, making these multisensory acquisition interfaces not parallel in gathering multisensory data. A complex programmable logic device is a CPLD. Both the microcontroller and the CPLD are very similar. But each has benefits and drawbacks. In an industrial WSN, CPLD/FPGA is used.

The radio frequency 433MHz Wireless Sensor and Actuator Network (WSAN) is set up by the smart home control system using a smart central controller. Radio frequency modules, switch modules, control modules, etc., have all been developed by Wang et al. [18] and Agrawal et al [19]. to control all types of appliances directly. The smart system has features for managing, controlling, and monitoring appliances, home security, and energy usage. [2], [4]. It is beneficial for security purposes that Authors used R.F. identification in [1], [2], [4]. Each household device receives a distinct identity thanks to this technology. So that each device may be explicitly identified, the R.F.'s range can be adjusted in both directions. For smart homes, managing efficient and secure human-machine connections is quite challenging. Secure Access Gateway (SAG), which acts as the interface between distant users and managed devices, was designed and developed for home area networks by Tongtong et al. [21].

There is a security issue because many nodes in a WSN are connected to the internet. Establishing the initial session key between the wireless sensor nodes and controlling the centre are the two primary issues in this network. Regarding security and issues, the smart home energy management system is proposed with a simple key establishment mechanism [14]. IP addresses are required for all internet-connected devices [3]. The IPv4 protocol has a very limited address space and is still used. People must switch to IPv6, which offers a vast address space, as the number of users grows. The lack of interoperability in smart home systems is caused by the fact that current market practice effectively binds consumers to proprietary technologies, forcing them to purchase only devices conforming to a specific manufacturer's system to enjoy full interoperability. Vittorio Miori et al. have proposed the intriguing approach of DomoNet, an "ecosystem" software created to overcome compatibility issues with pre-existing smart home systems.

3 | Study Summarize

The Smart Home system is susceptible to a wide range of concerns, issues, and challenges. Managing all applications in an IoT environment is challenging since they rapidly grow in number. The question of how to govern and oversee these numerous, expanding uses arises. If these ever-increasing applications were not properly and readily handled, the system could not be more secure and comfortable [2]. On the server side, security is lower because no unique authentication technique is employed. This can result in a system that

isn't secure. An attacker might gain entry to the victim's home and destroy the entire smart home system. Another issue that could arise is connectivity [4].

- *Standards: standardization is crucial because the IoT is becoming increasingly widespread. Difficulties include deciding which standard to employ, which will provide a secure medium, and how to increase system reliability.*
- *Identification: each device needs identification to be recognized individually. User information should be kept private. Privacy should be provided while maintaining connection.*
- *Authentication is necessary to protect a Smart Home system from an intruder. Only authorized users may receive access from the server.*
- *Security: the system must be capable of responding appropriately to security risks. Moreover, the system must be capable of reconfiguring itself after attacks.*
- *Application integration in an IoT environment is the major hurdle to overcome.*
- *Coordination: between the globally connected items, people, programmes, processes, etc., coordination is necessary.*
- *Data storage: as IoT applications grow, a tremendous amount of data is being gathered. Where to store the vast amounts of data is the problem. Large databases can resolve this issue. It requires using artificial intelligence algorithms to separate meaning from redundant information.*
- *Network self-organization: the topology of a network should be designed so that each linked device can self-organize. Actually, the ability for a network to self-organize should exist.*

4 | Conclusion

The IoT has numerous uses in various industries. IoT is already set up to work with industrial WSNs. It was created for the smart home system. The architecture of IoT and smart houses using IoT are presented in this paper. The IoT and smart homes have some issues. Some of them might be reduced with the use of new technologies. This essay discusses potential problems and difficulties. This paper has covered new technologies and approaches to enhance IoT applications. IoT currently uses CPLD controllers, Zigbee modules, and R.F. modules.

Author Contributions

If your research article has several authors (i.e., those who have contributed substantially to the work), you are recommended, but not required, to list the contributions of each author in the following statement: "conceptualization, X.X. and Y.Y.; methodology, X.X.; software, X.X.; validation, X.X., Y.Y. and Z.Z.; formal analysis, X.X.; investigation, X.X.; resources, X.X.; data curation, X.X.; writing-original draft preparation, X.X.; writing-review and editing, X.X.; visualization, X.X.; supervision, X.X.; project administration, X.X.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript." The relevant terms are explained in the CRediT taxonomy.

Informed Consent Statement

Not applicable

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Mohapatra, H., & Rath, A. K. (2020). Fault-tolerant mechanism for wireless sensor network. *IET wireless sensor systems*, *10*(1), 23–30. DOI:10.1049/iet-wss.2019.0106

[2] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance in WSN through PE-LEACH protocol. *IET wireless sensor systems*, *9*(6), 358–365. DOI:10.1049/iet-wss.2018.5229

[3] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, *9*(6), 447–457. DOI:10.1049/iet-wss.2019.0081

[4] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, *9*(4), 145–155. DOI:10.1049/iet-net.2019.0155

[5] Mohapatra, H., & Rath, A. K. (2020). Fault tolerance in WSN through uniform load distribution function. *International journal of sensors, wireless communications and control*, *11*(4), 385–394. DOI:10.2174/2210327910999200525164954

[6] Mohapatra, H., & Rath, A. K. (2020). Nub less sensor based smart water tap for preventing water loss at public stand posts. *Proceedings of 2020 ieee workshop on microwave theory and techniques in wireless communications, mttw 2020* (pp. 145–150). IEEE. DOI: 10.1109/MTTW51045.2020.9244926

[7] Mohapatra, H., & Rath, A. K. (2022). IoE based framework for smart agriculture: Networking among all agricultural attributes. *Journal of ambient intelligence and humanized computing*, *13*(1), 407–424. DOI:10.1007/s12652-021-02908-4

[8] Mohapatra, H., & Rath, A. K. (2021). A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid. *Cluster computing*, *24*(3), 2193–2211. DOI:10.1007/s10586-021-03255-x

[9] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. *International journal of sensor networks*, *37*(4), 219–232. DOI:10.1504/IJSNET.2021.119483

[10] Mohapatra, H., & Rath, A. K. (2019). Fault tolerance through energy balanced cluster formation (ebcf) in wsn. *Advances in intelligent systems and computing* (pp. 313–321). Springer. DOI: 10.1007/978-981-13-2414-7_29

[11] Panda, H., Mohapatra, H., & Rath, A. K. (2020). WSN-based water channelization: an approach of smart water. *Lecture notes in civil engineering* (pp. 157–166). Springer. DOI: 10.1007/978-981-15-2545-2_15

[12] Mohapatra, H., & Rath, A. K. (2020). IoT-based smart water. *IOT technologies in smart-cities: from sensors to big data, security and trust*, *63*. http://dx.doi.org/10.1049/PBCE128E_ch3

[13] Mohapatra, H. (2020). Offline drone instrumentalized ambulance for emergency situations. *IAES international journal of robotics and automation (IJRA)*, *9*(4), 251–255. DOI:10.11591/ijra.v9i4.pp251-255

[14] Mohapatra, H. (2021). Socio-technical challenges in the implementation of smart city. *2021 international conference on innovation and intelligence for informatics, computing, and technologies, 3ict 2021* (pp. 57–62). IEEE. DOI: 10.1109/3ICT53449.2021.9581905

[15] Mohapatra, H., & Rath, A. K. (2020). *Fundamentals of software engineering: designed to provide an insight into the software engineering concepts*. BPB publications.

[16] Mohapatra, H. (2021). Designing of fault tolerant models for wireless sensor network. *University*. http://hdl.handle.net/10603/333160%0Ahttps://shodhganga.inflibnet.ac.in:8443/jspui/handle/10603/333160

[17] Mohapatra, H., & Rath, A. K. (2020). Social distancing alarming through proximity sensors for COVID-19. *Easy chair*, *18, 1-6*. https://easychair.org/publications/preprint/dMGk

[18] Mohapatra, H. (2021). *Smart city with wireless sensor network.* Networking Of Smart City Applications. https://www.amazon.com.tr/Smart-City-Wireless-Sensor-Network/dp/B09P47J4XB

[19] Wang, M., Zhang, G., Zhang, C., Zhang, J., & Li, C. (2013). An iot-based appliance control system for smart homes. *Proceedings of the 2013 international conference on intelligent control and information processing, icicip 2013* (pp. 744–747). IEEE. DOI: 10.1109/ICICIP.2013.6568171

[20] Gabhane, J. P., Thakare, M. S., & Craig, M. M. (2017). Smart homes system using internet-of-things : issues , solutions and recent research directions. *International research journal of engineering and technology (IRJET)*, *4*(5), 1965-1969.

[21] Li, T., Ren, J., & Tang, X. (2012). Secure wireless monitoring and control systems for smart grid and smart home. *IEEE wireless communications*, *19*(3), 66–73. DOI:10.1109/MWC.2012.6231161