Available *online* at: http://ajeeet.ft.unand.ac.id/

Andalas Journal of Electrical and Electronic Engineering Technology

ISSN 2777-0079

Review Article

Use of IoT Technology in Home Security Monitoring Systems: A Review

Rahmawati Fitriyan, Muhammad Imran Hamid, Abdul Rajab

Department of Electrical Engineering, Faculty of Engineering, Universitas Andalas, Padang, 25163, Indonesia

ARTICLE INFORMATION

Received: May 23, 2024
Revised: June 13, 2024
Accepted: July 21, 2024
Available online: July 23, 2024

KEYWORDS

Internet Of Things, Monitoring System, Smart Home, Security Features, Communication

CORRESPONDENCE

E-mail: rahma.fitriyan28@gmail.com

A B S T R A C T

Utilizing IoT technology in home security monitoring systems offers an effective solution to improve energy efficiency and security by allowing users to monitor and control electronic devices remotely via the Internet. The basic principles of a smart home include reliable connectivity, device interoperability, stringent security and privacy, and energy efficiency. IoT communications are supported by technologies such as RFID and Wi-Fi to ensure effective wireless data transmission. IoT facilitates connecting new devices without additional installation, using technologies such as Wi-Fi, Barcodes (QR codes), and Bluetooth for various applications. The application of IoT in home security monitoring involves platforms such as Blynk and web servers for remote control, with a focus on data protection and system security. This paper compiles various research and conference-related aspects of IoT, including privacy, educational guidelines, system characterization, innovative grid communications, bridge monitoring, RFID authentication, Wi-Fi technology, Bluetooth communications, smart home applications, and security systems. Topics covered include energy monitoring systems, smart home security, earthquake detection, IoT privacy and security, automation, edge intelligence, and Internet of Things architecture.

INTRODUCTION

The Internet of Things (IoT) is becoming an increasingly interesting topic of conversation in the era of Industrial Revolution 4.0 because its concept has the potential to influence our lifestyle and the way we work [1]. The IoT can be implemented in many aspects of human life, such as home automation systems [2]. The home automation system works with electronic devices connected to the Internet to be monitored or controlled remotely [3], [4].

The energy usage monitoring and control system is part of a home automation system that allows energy usage reports anywhere via the Internet [5], [6]. In an era of increasing awareness of the importance of energy efficiency and home security, developing electrical energy monitoring systems and home security is becoming increasingly crucial [7], [8]. On the other hand, houses that are left empty or when the occupants are careless are vulnerable to fire and other security risks [9]. Therefore, sophisticated communication and information technology can be a solution to monitor, save, and control household equipment and activities effectively [10].

A smart home is a system that has been programmed and can work automatically by utilizing IoT technology. This system can control various electronic devices at home, such as lights, AC, TV, and so on [11], [12]. One of the essential features of a smart home is the security feature. This feature can monitor the house's condition remotely and provide warnings if something undesirable occurs, such as theft or fire [13]. This technology was created to increase energy efficiency, security, comfort, and other benefits [14]. With the increasing availability of smart devices and widespread internet connectivity, the need for intelligent monitoring systems in the home is becoming increasingly urgent [15], [16].

Developing IoT smart home monitoring systems with security features has become an international concern. Several papers addressing this issue proposed IoT-based intelligent security alert systems for homes, including intruder detection, fire, smoke detection, and continuous monitoring [17]. Along with technological developments, one of the security features in fire alarm systems has also experienced a significant increase in capabilities in recent years [18], [19]. Fire accidents are rare, but the impact will be huge if they happen. Therefore, this system is expected to be able to save from fire hazards and other features [20].

Reading IoT smart home monitoring systems with additional security features is essential in Indonesia. These systems utilize technology to increase security and prevent theft and delivery [21], [22]. Smart home systems using IoT platforms have been designed to improve security safety, automate the home, and provide remote monitoring and control [23], [24]. Using cloud-based IoT to monitor and control electrical resources at home can result in energy savings and cost reductions [25]. In addition,

https://doi.org/10.25077/ajeeet.v4i1.111

home monitoring systems based on object sensors and cloud computing can help maintain residential security, reducing the risk of theft and trespass [26]. IoT technology allows the implementation of advanced security systems that can be applied to homes, buildings, and environments [27].

Technological developments have gradually experienced significant changes in utilizing various aspects of information, mainly thanks to advances in hardware and software [28], [29]. One example of the application of this technology is the ability to detect earthquakes at home. This connected security system can quickly detect earthquakes and take preventive measures using IoT integration in the smart home concept [30]. Network-connected sensors allow homes to send alerts and automatically take safety measures such as closing doors and windows, providing additional protection to residents against potential earthquake risks [31]. With increasing awareness of the importance of earthquake preparedness, IoT-based security innovations in smart homes provide proactive measures to protect occupants and their assets [32].

IOT PRINCIPLES AND COMMUNICATION

IoT Principle

The Internet of Things (IoT) principles revolve around the interconnection of various physical devices or objects with sensing, communication, and information-processing capabilities, enabling them to interact and share data over a network without human intervention [33]. IoT systems usually consist of three layers: data acquisition through sensors and actuators, data transfer using different devices, and data analysis through various analytical techniques [34]. Communication capabilities are critical in turning smart devices into connected networks, facilitating enhanced interactions between devices and humans [35]. The IoT paradigm covers sensors, information technology, data analysis, machine learning, and security mechanisms, presenting technical challenges requiring innovative solutions for successful real-life implementation [36].

Internet of Things (IoT) in smart homes is a concept where various physical devices are connected to the Internet, allowing them to communicate and share data automatically [37]. Devices such as bright lights, thermostats, security cameras, smart locks, and sensors (motion, temperature, humidity) are connected via a hub or gateway [38]. This device can be controlled and monitored via a mobile application or dashboard and utilizes cloud services for data storage and analysis. The basic principles of IoT in a smart home include reliable connectivity, interoperability between devices from various manufacturers, and strict security and privacy to protect user data [39]. Ease of use and energy efficiency are essential, ensuring devices are easy to install and operate and consume as little power as possible [40]. This system must be scalable to accommodate additional devices without reducing performance and reliable and flexible to adapt to technological developments and changing user needs. [41].

The advantages of smart home IoT include enhanced comfort by automating everyday tasks, improved security through real-time monitoring, and increased energy efficiency through intelligent control [42]. Additionally, it can lead to cost savings by optimizing energy use and simplifying maintenance. However, implementing smart home IoT presents challenges, such as cybersecurity risks, device interoperability issues, high initial costs, and reliance on stable internet connectivity [43]. Real-life examples demonstrate the practical use of IoT in residential settings, such as using smart thermostats to adjust the temperature based on occupant behaviors and using innovative security solutions utilizing cameras and sensors to safeguard homes against intrusion [44]. The future of smart home IoT appears promising with the integration of artificial intelligence to enhance system intelligence and the development of more sophisticated and user-friendly devices. Efforts to standardize IoT systems are expected to enhance interoperability among devices and platforms, making smart homes more accessible to a broader audience [45]. By acknowledging and addressing these challenges, we can better leverage IoT technology to create a safer, more comfortable, and efficient home environment [46].

IoT Communication

Communication is a medium used to send and receive data from one point to another using different methods and protocols. Communication can be via cable or wireless. The Internet initially became widespread via cable communication, and it can be implemented that IoT can be implemented in wired communication. However, if considered reality, wired communication can only be achieved in some places [47]. Cable networks have disadvantages related to mobility issues and installation costs. Effective, low-cost, simple wireless media will be applied to IoT [48]. In the world of technology, several transmission modules and protocols are known, including RFID, Wi-Fi, Barcode, ZigBee, and Bluetooth.

Radio Frequency Identification Technology (RFID)

RFID uses radio waves to transmit data, utilizing RFID tags placed on various objects. These RFID tags are of two types: active tags, equipped with their power source, and passive tags, which do not require an external power source [49]. RFID operates in various frequency bands, namely 135 KHz and 5.875 GHz, which include low frequency (LF), high frequency (HF), ultra-high frequency (UHF), and very high frequency (SHF). RFID transponders can respond in less than 100 milliseconds, making this technology suitable for IoT environments [50].

Wi-Fi

Wi-Fi is a wireless networking technology that uses the globally recognized IEEE 802.11 standard to send and receive data, signals, and other commands. This technology works in a frequency range between 2.4 and 60 GHz, with average data speeds ranging from 1 Mbps to 54 Mbps. The effective range of Wi-Fi usually reaches around 100 meters, using a point-to-hub network topology **[**51**]**. Wi-Fi has more advantages in adding new devices than cable media or RFID technology. On a wired network, each addition of a new device requires additional physical installation, such as pulling new cables, which can be a complicated and time-consuming process [52]. In contrast, in a Wi-Fi network, adding new devices can be done quickly without additional installation, making it a more practical and efficient solution. This feature makes Wi-Fi especially suitable for use in IoT, where the ability to add and connect new devices quickly and efficiently is often required. [53].

QR Code

A barcode is a machine-readable representation of information formed from a combination of areas of high and low reflectance on the surface of an object. This pattern is then converted into a binary code combining 1 and 0. Barcodes have unique characteristics in lines (bars) and spaces (spaces), differentiating them from other identification technologies such as RFID. This barcode system is often used on goods labels to facilitate identification and tracking [54]. QR Code is the latest version of barcode technology that can be identified using a cellphone camera. The shape resembles a sticker attached to an item, which differs from RFID, which uses a chip [55]. Additionally, barcodes have the advantage of lower cost and installation than RFID, making them a more economical and practical choice for IoT applications. These factors make barcoding a viable solution for various purposes in IoT applications [56].

Bluetooth

Bluetooth is a wireless technology that is very popular among cell phone users. This technology operates at the 2.4 GHz frequency in the ISM (Industrial, Scientific, and Medical) frequency band [57]. Bluetooth has experienced significant development with the emergence of more efficient versions, such as Bluetooth Low Energy (BLE) and Bluetooth Smart [58]. This technology connects various electronic devices, such as smart watches, cell phones, earphones, keyboards, mice, printers, cars, and many other devices. [59]. Bluetooth in various electronic devices allows connection and interaction between these devices, providing a crucial role in developing and applying IoT technology. With Bluetooth, devices can communicate with each other efficiently and wirelessly, supporting broader integration and more innovative functionality across a wide range of IoT applications [60].

IMPLEMENTATION OF IOT IN RESIDENTIAL SECURITY MONITORING SYSTEMS

The development of IoT technology has been widely applied in everyday life, including home security systems. IoT allows real-time monitoring of home conditions through various platforms such as Blynk applications, websites, etc., thereby significantly increasing home monitoring capabilities and security.

Blynk

After conducting an in-depth literature review regarding using Blynk in residential security systems, it can be concluded that Blynk allows users to control and monitor home security systems remotely via iOS and Android apps. With a customizable interface, users can manage electronic devices, store sensor data for real-time monitoring, and use multiple hardware platforms such as Arduino and Raspberry Pi for broad compatibility. This enables efficient monitoring and flexible control of home security wherever the user is located [61].

Additionally, the Blynk platform enables seamless integration between various sensors such as PZEM-004 T, DHT, Magnetic Door, RFID, Infrared Motion, Flame, and MQ-135 Gas with hardware such as Arduino Mega and Raspberry Pi 3 in a smart home security system. These sensors are connected directly to the microcontroller, relaying their data to the Blynk application for monitoring and control. Users can easily monitor home conditions and immediately act via smartphone or PC. When a sensor like the MQ-135 detects gas or smoke, the system will automatically respond, increasing security inside the home [62].

Blynk implements robust security protocols in home security systems by providing secure data transmission over the Internet to micro-controllers, keeping user information confidential through encrypted cloud server communications. Blynk's notification system also includes security features to alert about energy usage and power loss, with customized threshold settings to minimize unnecessary alerts, increasing security awareness and promoting energy conservation [63].

Blynk was evaluated in the study for its ability to integrate with extensive IoT networks, improving home security with automatic water level detection. Through the Blynk application and internet connection, sensor data can be captured and monitored efficiently via smartphone without distance constraints. The implementation of the automatic water tank filling system successfully measured the water level with high accuracy, with an error rate of around 3%, demonstrating the effectiveness and reliability of this technology in practical applications [64].

The main challenges in using Blynk in smart home systems include limited wireless transmission range and high cost. To address this, research focuses on implementing WiFi-based systems that are affordable and energy efficient, increasing accessibility for homeowners. Additionally, the limitation of an unfriendly user interface is overcome by adopting the well-known Blynk app with an easy-to-use interface, allowing users to easily monitor and control devices in a smart home system [65].

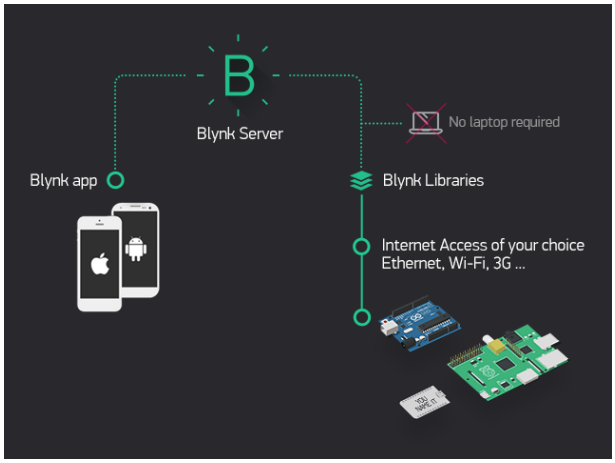

Figure 1. How Blynk Works

These findings highlight several key benefits of using Blynk in IoT-enabled home security systems, including the ability to control and monitor the system remotely via iOS and Android apps with customized interfaces. Seamless integration with various sensors and hardware, such as Arduino and Raspberry Pi, is also essential, allowing users to monitor home conditions efficiently and respond to events such as gas or smoke detection automatically. The study also assessed Blynk's ability to integrate with broader IoT networks, improving home security through practical applications such as automatic water level detection. It

 https://doi.org/10.25077/ajeeet.v4i1.111

shows that Blynk facilitates effective control of home security systems and is reliable in integrating various technologies to improve the overall security and functionality of a smart home. How Blynk works via the Internet can be seen in Figure 1.

As observed in Figure 1, Blynk operates through the Internet. This requires the selected hardware to possess Internet connectivity. Some microcontrollers, such as the Arduino Uno, require Ethernet or Wi-Fi Shield to communicate, while other microcontrollers have Internet-enabled, such as ESP8266, Raspberry Pi with Wi-Fi dongle, Particle Photon or SparkFun Blynk Board. Even without a shield, connection via USB to a laptop or desktop *is possible* [66].

WEB Server

Web servers are crucial infrastructure in IoT systems that enable efficient data exchange and centralized device management when implementing home security systems. It can be concluded after conducting an in-depth literature review regarding using the web in residential security systems. First, Web applications in smart home security systems allow owners to access activities and images from the database remotely and receive live notifications of intruder alerts via smartphone. In power failure situations, the system uses the cellular network for communication, allowing updating and managing the facial database via a web application on the smartphone. Android app automatically refreshes data every 15 minutes for effective monitoring and control [67].

Additionally, the web server platform facilitates the integration of sensors and hardware in a home security system with Raspberry Pi 2 using Python scripts and the Requests library to monitor updates in text files. The system also sends a POST request to an HTTP web server powered by NodeJS and MongoDB to record door-open events based on date and time. Data can be accessed via GET requests from the Android app. At the same time, the Ethernet shield on the Arduino MCU allows communication with web-based Android apps for remote device management and scheduling [68].

Protective measures are required to protect user data in a home security system. The use of robust encryption methods such as WPA2 (Wi-Fi Protected Access 2) or advanced encryption techniques is essential to prevent unauthorized access or interception of data. WPA2 protects unauthorized access by encrypting data sent over a Wi-Fi network so that only devices with the correct encryption key can access and read that data. Additionally, dedicated security engines that connect directly to gateways and routers can manage connections based on IP addresses and MAC (Media Access Control) addresses for additional security. Routine security checks by the application engine can detect unauthorized activity in real-time data transmission, while placing a firewall between the Internet and the smart home layer can prevent Internet threats and secure the system as a whole [69].

This assessment evaluates the capabilities of web servers in integration with IoT networks to improve home security with a focus on a Raspberry Pi-based automated service request system. This system allows sensors processed by the Raspberry Pi to automatically send service requests to the homeowner or related parties via a web server or cloud via the Internet when abnormalities are detected in the smart home. This approach enhances overall security measures with rapid response to situations that require immediate action [70].

Using a web server, a PHP-based web application connected to a MySQL database via scripts, allows efficient storage of sensor data and data retrieval. A design that focuses on user-friendliness and simplicity helps overcome the complexity of users interacting with web applications. Responsive web pages using the Bootstrap framework overcome compatibility issues with a seamless display on mobile and desktop devices. Selecting free administration templates also speeds up application development, reducing the time and resources required. Enhanced graphical data visualization in web applications provides users with deeper insights and enhanced decision-making capabilities compared to mobile applications [71].

These findings assess the ability of web servers to integrate with IoT networks to improve home security by summarizing some of the main benefits of their use in IoT-based home security systems. This includes the ability to access and manage data remotely via web and smartphone applications, using technologies such as Raspberry Pi, Python, NodeJS, and MongoDB to integrate sensors and hardware, as well as implementing security measures such as WPA2 encryption, IP-based connection management, and MAC, regular security checks, and use of firewalls. This approach also highlights the web server's ability to support an automated service request system responsive to emergencies or events that require immediate action and efficiently manage sensor data and information visualization for better decision-making. These findings assess the ability of web servers to integrate with IoT networks to improve home security by summarizing some of the main benefits of their use in IoT-based home security systems. This includes the ability to access and manage data remotely via web and smartphone applications, using technologies such as Raspberry Pi, Python, NodeJS, and MongoDB to integrate sensors and hardware, as well as implementing security measures such as WPA2 encryption, IP-based connection management, and MAC, regular security checks, and use of firewalls. This approach also highlights the web server's ability to support an automated service request system responsive to emergencies or events that require immediate action and efficiently manage sensor data and information visualization for better decision-making.

CONCLUSIONS

From this research, IoT technology in residential home security monitoring systems provides an effective solution for increasing energy efficiency and home security. The basic principles of IoT in a smart home include reliable connectivity, device interoperability, strict security and privacy, and energy efficiency. Various technologies, such as RFID, Wi-Fi, and Bluetooth, are used in IoT applications to enable effective wireless data transmission. Implementing IoT in home security involves using platforms such as Blynk and web servers to monitor and control home security remotely, focusing on data protection and system security. The journal also discusses various research on smart home systems, IoT technology, security, monitoring and control, and other topics such as earthquake detection, automation, and Internet of Things architecture.

Overall, IoT in smart home security systems offers the potential to create a safer, more comfortable, and efficient home environment.

REFERENCES

[1] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018, doi: 10.1016/j.jksuci.2016.10.003.

[2] Y. A. Rozzi and A. Luthfi, "Dual Server Implementation for Improving Reliability of Online Energy Monitoring System," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 5, pp. 8835–8839, 2020, doi: 10.30534/ijatcse/2020/277952020.

[3] A. Luthfi and Y. A. Rozzi, "Design of Raspberry Pi Web-based Energy Monitoring System for Residential Electricity Consumption," pp. 4–8, 2020.

[4] R. Sarmah, "SURE-H : A Secure IoT Enabled Smart Home System," *2019 IEEE 5th World Forum Internet Things*, pp. 59–63, 2019.

[5] F. Li, J. Clemente, M. Valero, Z. Tse, S. Li, and W. Z. Song, "Smart Home Monitoring System via Footstep-Induced Vibrations," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3383–3389, 2020, doi: 10.1109/JSYST.2019.2937960.

[6] G. Liu, H. Meng, G. Qu, L. Wang, L. Ren, and L. Fang, "Distributed optical fiber sensor temperature dynamic correction method based on building fire temperature-time curve," *J. Build. Eng.*, vol. 68, no. February, p. 106050, 2023, doi: 10.1016/j.jobe.2023.106050.

[7] S. Tanwar *et al.*, "An Advanced Internet of Thing-based Security Alert System for Smart Home," 2017.

[8] N. A. Prasetyo, A. G. Prabawati, U. Atma, and J. Yogyakarta, "Smart Home : Power Electric Monitoring and Control in Indonesia," vol. 13, no. 3, pp. 143–151, 2019.

[9] P. Kumar and U. C. Pati, "IOT-based monitoring and control of appliances for smart home," *2016 IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. RTEICT 2016 - Proc.*, vol. 769008, pp. 1145–1150, 2017, doi: 10.1109/RTEICT.2016.7808011.

[10] S. J. Philip, T. Jack, and T. Carte, "Computers in Human Behavior There 's No place like home : Understanding users ' intentions toward securing internet-of-things (IoT) smart home networks," vol. 139, no. August 2022, 2023.

[11] S. Bagde, P. Ambade, M. Batho, P. Duragkar, P. Dahikar, and A. Ikhar, "Internet of Things (IoT) Based Smart Switch," *J. ISMAC*, vol. 3, no. 2, pp. 149–162, 2021, doi: 10.36548/jismac.2021.2.007.

[12] I. Daniela *et al.*, "ScienceDirect Using IoT for Automated Heating of Means of Using of a Means of OpenHAB Using IoT IoT for for Automated of Means of Using IoT for Automated Heating of a Platform Smart Home by Means of OpenHAB Using IoT for Automated Heating of a Platfor," *IFAC Pap.*, vol. 55, no. 11, pp. 90–95, 2022, doi: 10.1016/j.ifacol.2022.08.054.

[13] D. Pal, X. Zhang, and S. Siyal, "Technology in Society Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society : A smart-home context using a resistive modelling approach," *Technol. Soc.*, vol. 66, no. July, p. 101683, 2021, doi: 10.1016/j.techsoc.2021.101683.

[14] T. Malche, "Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021," *Proc. 5th Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2021*, pp. 65–70, 2021.

[15] K. Erkert, A. Lamontagne, J. Chen, J. Cummings, and M. Hoikka, "An End-to-End System for Monitoring IoT Devices in Smart Homes," pp. 929–930, 2022.

[16] B. A. Pramajuri, T. Hadyanto, M. Ade, and C. Rahmani, "LITERATURE REVIEW : SMART HOME BASED ON IOT FOR SECURITY SYSTEM," pp. 3–7.

[17] M. M. Thakur, S. Shete, P. Avhad, and S. Deore, "Smart Home Security Application," vol. 5, no. 2, pp. 3–6, 2023.

[18] J. Pantelic, Y. Joo, B. Staven, and Q. Liu, "Energy & Buildings Cooking emission control with IoT sensors and connected air quality interventions for smart and healthy homes : Evaluation of effectiveness and energy consumption," *Energy Build.*, vol. 286, p. 112932, 2023, doi: 10.1016/j.enbuild.2023.112932.

[19] S. Somani, "IoT Based Smart Security and Home Automation," *2018 Fourth Int. Conf. Comput. Commun. Control Autom.*, pp. 1–4, 2018.

[20] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered," pp. 1–19, doi: 10.3390/s20133625.

[21] L. Mehdi, Y. Ouallou, O. Mohamed, and A. Hayar, "New smart home's energy management system design and implementation for frugal smart cities," *2018 Int. Conf. Sel. Top. Mob. Wirel. Networking, MoWNeT 2018*, pp. 149–153, 2018, doi: 10.1109/MoWNet.2018.8428865.

[22] D. Y. Setyawan and H. Setiwan, "Monitor and Control-Based Raspberry Pi for Designing Smart Home through Internet of Things," no. December, pp. 95–101, 2020.

[23] M. Umer *et al.*, "IoT based smart home automation using blockchain and deep learning models," 2023, doi: 10.7717/peerj-cs.1332.

[24] A. Biswas, D. Biswas, S. S. Chauhan, and A. Borwankar, "Smart home equipment control system with raspberry Pi and Yocto," *Proc. World Conf. Smart Trends Syst. Secur. Sustain. WS4 2020*, pp. 553–558, 2020, doi: 10.1109/WorldS450073.2020.9210376.

[25] E. A. Kadir, A. Siswanto, and A. Yulian, *Home Monitoring System Based on Cloud Computing Technology and Object Sensor*, vol. 2. Springer Singapore. doi: 10.1007/978-981-10-8471-3.

[26] Kabita Agarwal and Arun Agarwal*, "Sci-Hub | Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT. 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) | 10.1109/I-SMAC47947.2019.9032629," *Coll. Eng. Technol.*, pp. 629–633, 2019, [Online]. Available: https://sci-hub.se/10.1109/I-SMAC47947.2019.9032629

[27] A. Xin, L. Yiheng, T. Yawen, and B. Zhengde, "The typical application of internet of things in China in the future: The smart home," *2018 Int. Conf. Electron. Technol. ICET 2018*, pp. 361–364, 2018, doi: 10.1109/ELTECH.2018.8401403.

[28] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "applied sciences IoT Privacy and Security : Challenges and Solutions," pp. 1–17, 2020.

[29] V. D. Vaidya, "A Comparative Analysis on Smart Home System to Control , Monitor and Secure Home , based on technologies like GSM , IOT , Bluetooth and PIC Microcontroller with ZigBee Modulation," *2018 Int. Conf. Smart City Emerg. Technol.*, pp. 1–4.

[30] W. Fan, W. Wang, C. Liang, M. Yang, W. Hsu, and Y. Shiau, "Smart Earthquake Disaster Prevention System," no. May, 2021, doi: 10.18494/SAM.2021.3160.

[31] J. Lee, I. Khan, S. Choi, and Y. Kwon, "A Smart IoT Device for Detecting and Responding to Earthquakes," pp. 1–19, 2019, doi: 10.3390/electronics8121546.

[32] R. K. Badhon, A. R. Barai, and F. Zhora, "Remote Real Time Monitoring and Safety System for Earthquake and Fire Detection Based on Internet of Things," pp. 2019–2022, 2019.

[33] P. Raja, D. S. Kumar, D. S. Yadav, and D. T. Singh, "The Internet of Things (IOT): A Review of Concepts, Technologies, and Applications," *Int. J. Inf. Technol. Comput. Eng.*, no. 32, pp. 21–32, 2023, doi: 10.55529/ijitc.32.21.32.

[34] Z. Fang *et al.*, "IOTA: A Framework for Analyzing System-Level Security of IoTs," *Proc. - 7th ACM/IEEE Conf. Internet Things Des. Implementation, IoTDI 2022*, pp. 143–155, 2022, doi: 10.1109/IoTDI54339.2022.00017.

[35] Z. Shouran, A. Ashari, and T. Kuntoro, "Internet of Things (IoT) of Smart Home: Privacy and Security," *Int. J. Comput. Appl.*, vol. 182, no. 39, pp. 3–8, 2019, doi: 10.5120/ijca2019918450.

[36] M. Nasir, K. Muhammad, A. Ullah, J. Ahmad, S. Wook Baik, and M. Sajjad, "Enabling automation and edge intelligence over resource constraint IoT devices for smart home," *Neurocomputing*, vol. 491, pp. 494–506, 2022, doi: 10.1016/j.neucom.2021.04.138.

[37] C. Brooks *et al.*, "A Component Architecture for the Internet of Things," *Proc. IEEE*, vol. 106, no. 9, pp. 1527–1542, 2018, doi: 10.1109/JPROC.2018.2812598.

[38] F. Masmoudi, Z. Maamar, M. Sellami, A. I. Awad, and V. Burégio, "A Guiding Framework for Vetting the Internet of Things," *J. Inf. Secur. Appl.*, vol. 55, no. August, 2020, doi: 10.1016/j.jisa.2020.102644.

[39] J. Lukkien, "A systems of systems perspective on the internet of things," *ACM SIGBED Rev.*, vol. 13, no. 3, pp. 56–62, 2016, doi: 10.1145/2983185.2983195.

[40] R. H. Weber, "Accountability in the Internet of Things," *Comput. Law Secur. Rev.*, vol. 27, no. 2, pp. 133–138, 2011, doi: 10.1016/j.clsr.2011.01.005.

[41] J. Kwan, Y. Gangat, D. Payet, and R. Courdier, "An Agentified Use of the Internet of Things," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp. 311–316, 2017, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.76.

[42] F. Lacerda, M. Lima-Marques, and A. Resmini, "An Information Architecture Framework for the Internet of Things," *Philos. Technol.*, vol. 32, no. 4, pp. 727–744, 2019, doi: 10.1007/s13347-018-0332-4.

[43] I. Grønbæk, "Architecture for the Internet of Things (IoT): API and interconnect," *Proc. - 2nd Int. Conf. Sens. Technol. Appl., SENSORCOMM 2008, Incl. MESH 2008 Conf. Mesh Networks; ENOPT 2008 Energy Optim. Wirel. Sensors Networks, UNWAT 2008 Under Water Sensors Syst.*, pp. 802–807, 2008, doi: 10.1109/SENSORCOMM.2008.20.

[44] C. Li and B. Palanisamy, "Privacy in Internet of Things: From Principles to Technologies," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 488–505, 2019, doi: 10.1109/JIOT.2018.2864168.

[45] M. Khanafer and M. El-Abd, "Guidelines for teaching an introductory course on the Internet of things," *IEEE Glob. Eng. Educ. Conf. EDUCON*, vol. April-2019, pp. 1488–1492, 2019, doi: 10.1109/EDUCON.2019.8725186.

[46] F. Alkhabbas, R. Spalazzese, and P. Davidsson, "Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study," *Internet of Things (Netherlands)*, vol. 7, p. 100084, 2019, doi: 10.1016/j.iot.2019.100084.

[47] M. Zeinali and J. Thompson, "Comprehensive practical evaluation of wired and wireless internet base smart grid communication," *IET Smart Grid*, vol. 4, no. 5, pp. 522–535, 2021, doi: 10.1049/stg2.12023.

[48] S. Hou and G. Wu, "A low-cost IoT-based wireless sensor system for bridge displacement monitoring," *Smart Mater. Struct.*, vol. 28, no. 8, 2019, doi: 10.1088/1361-665X/ab2a31.

[49] D. P. F. Moller and H. Vakilzadian, "Wireless communication in aviation through the Internet of Things and RFID," *IEEE Int. Conf. Electro Inf. Technol.*, pp. 602–607, 2014, doi: 10.1109/EIT.2014.6871833.

[50] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, 2015, doi: 10.1109/JIOT.2014.2360121.

[51] L. Tian, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11ah research," *J. Netw. Comput. Appl.*, vol. 182, no. February, 2021, doi: 10.1016/j.jnca.2021.103036.

[52] M. Ushakova, Y. Ushakov, P. Polezhaev, and A. Shukhman, "Wireless self-organizing Wi-Fi and bluetooth based network for internet of things," *2019 Int. Conf. Eng. Telecommun. EnT 2019*, pp. 1–5, 2019, doi: 10.1109/EnT47717.2019.9030584.

[53] S. Saloni, "WiFi-Aware as a Connectivity Solution for IoT," pp. 137–142, 2016.

[54] R. S. Verma, B. R. Chandavarkar, and P. Nazareth, "Mitigation of hard-coded credentials related attacks using QR code and secured web service for IoT," *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, pp. 1–5, 2019, doi: 10.1109/ICCCNT45670.2019.8944592.

[55] S. Babu and S. Markose, "IoT enabled Robots with QR Code based localization," *2018 Int. Conf. Emerg. Trends Innov. Eng. Technol. Res. ICETIETR 2018*, pp. 7–11, 2018, doi: 10.1109/ICETIETR.2018.8529028.

[56] K. Di Chang, J. L. Chen, H. C. Chao, and C. W. Liu, "The potential cloud application model for internet of things - Case study of shopping malls," *Proc. - 2014 10th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2014*, pp. 954–957, 2014, doi: 10.1109/IIH-MSP.2014.239.

[57] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with bluetooth smart," *Ad Hoc Networks*, vol. 57, pp. 19–31, 2017, doi: 10.1016/j.adhoc.2016.08.012.

[58] R. N. Gore, H. Kour, M. Gandhi, D. Tandur, and A. Varghese, "Bluetooth based Sensor Monitoring in Industrial IoT Plants," *2019 Int. Conf. Data Sci. Commun. IconDSC 2019*, pp. 1–6, 2019, doi: 10.1109/IconDSC.2019.8816906.

[59] T. M. T. Pham and J. Yang, "Exploring Bluetooth Communication Protocols in Internet-of-Things Software Development," *Proc. - 2020 IEEE Int. Conf. Softw. Maint. Evol. ICSME 2020*, pp. 792–793, 2020, doi: 10.1109/ICSME46990.2020.00093.

[60] M. Collotta and G. Pau, "Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes," *Comput. Electr. Eng.*, vol. 44, pp. 137–152, 2015, doi: 10.1016/j.compeleceng.2015.01.005.

[61] M. A. Omran, B. J. Hamza, and W. K. Saad, "The design and fulfillment of a Smart Home (SH) material powered by the IoT using the Blynk app," *Mater. Today Proc.*, vol. 60, no. xxxx, pp. 1199–1212, 2022, doi: 10.1016/j.matpr.2021.08.038.

[62] M. Sheth and P. Rupani, "Smart Gardening Automation using IoT with BLYNK App," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, vol. 2019-April, no. Icoei, pp. 266–270, 2019, doi: 10.1109/icoei.2019.8862591.

[63] A. Othman and N. H. Zakaria, "Energy Meter based Wireless Monitoring System using Blynk Application via smartphone," *IEEE Int. Conf. Artif. Intell. Eng. Technol. IICAIET 2020*, 2020, doi: 10.1109/IICAIET49801.2020.9257827.

[64] C. A. Siregar, D. Mulyadi, A. W. Biantoro, H. Sismoro, and Y. Irawati, "Automation and control system on water level of reservoir based on microcontroller and blynk," *Proceeding 14th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2020*, pp. 4–7, 2020, doi: 10.1109/TSSA51342.2020.9310836.

[65] B. Bohara, S. Maharjan, and B. R. Shrestha, "IoT Based Smart Home using Blynk Framework," 2020, [Online]. Available: http://arxiv.org/abs/2007.13714

[66] H. Durani, M. Sheth, M. Vaghasia, and S. Kotech, "Smart Automated Home Application using IoT with Blynk App," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2018*, no. Icicct, pp. 393–397, 2018, doi: 10.1109/ICICCT.2018.8473224.

[67] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, "Smart Home Security Using IoT and Face Recognition," *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, pp. 1–6, 2018, doi: 10.1109/ICCUBEA.2018.8697695.

[68] M. A. Hoque and C. Davidson, "Design and implementation of an IoT-based smart home security system," *Int. J. Networked Distrib. Comput.*, vol. 7, no. 2, pp. 85–92, 2019, doi: 10.2991/ijndc.k.190326.004.

[69] A. Kumar Ray, A. Bagwari, and I. -Mohan Nagar Ghaziabad, "9 th IEEE International Conference on Communication Systems and Network Technologies IoT based Smart home : Security Aspects and security architecture," *2020 IEEE 9th Int. Conf. Commun. Syst. Netw. Technol.*, vol. 1, 2020, doi: 10.1109/CSNT.2020.41.

[70] P. K. Madupu and B. Karthikeyan, "Automatic Service Request System for Security in Smart Home Using IoT," *Proc. 2nd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2018*, no. Iceca, pp. 1413–1418, 2018, doi: 10.1109/ICECA.2018.8474684.

[71] D. *Vasicek*, J. Jalowiczor, L. Sevcik, and M. Voznak, "IoT Smart Home Concept," *2018 26th Telecommun. Forum, TELFOR 2018 - Proc.*, pp. 1–4, 2018, doi: 10.1109/TELFOR.2018.8612078.