Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp. 4326-4332
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.446

A Study: An Analysis Of Smart Home

Harendra Singh Negi Computer Science and Engineering Graphic Era Deemed to be University Dehradun, India mail.harendrasinghnegi@gmail.com

Suraj Dwivedi Department of Computer Application Graphic Era Deemed to be University Dehradun, India dwivediformat@gmail.com

Dr. Manish Kumar Lila Associate Professor, Department of Mechnaical Enginnering, Graphic Era Hill University, Dehradun

Bhawnesh Kumar Computer Science and Engineering Graphic Era Deemed to be University Dehradun, India bhawneshmca@gmail.com

Kamlesh Purohit Computer Science and Engineering Graphic Era Deemed to be University Dehradun, India kamleshpurohit80@gmail.com

Abstract— The technology is evolving quickly these days, which improves home security systems. Automation in the security field increases authenticity. Homeowners have access to a variety of electrical appliances that must constantly be monitored from a distance. In this paper, a face detection method and a home security system are both suggested. The system will notify the owner of any illegal access or whenever the actions needed to make progress by sending a notification to the user. The user can take the required actions after he receives the message. An independent system is implemented using the Internet of Things as a communication network. Python-coded Raspberry Pi is employed as the controlling unit.

Keywords—home security, automation, temperature, humidity

I. INTRODUCTION

One of the biggest investments in life is a person's home, which contains all of their private and secret information. People's lives depend on it, so any improvement will indeed increase everyone's level of comfort. Citizens are always trying new things to make themselves more comfortable. This is for simplifying daily tasks or possibly doing away with some of them. People can now control some household duties by installing smart equipment in their houses [1]. There is no need to be close to the gadget when using this type of intelligent equipment because remote control is an option. In addition to routine house chores like adjusting the lighting or temperature, home security is another consideration. It makes sense that individuals would wish to preserve it given that it can be used to deposit precious and private items and papers. The usage of traditional mechanical door locks dates back to Ancient Egypt. The typical mechanism has been updated for the present. But these new strategies for regulating domestic activities must be simple to use and comprehend. People need solutions to make their acts simpler rather than just refining them. The home environment must be simple to integrate the smart gadgets into. The

Internet of Things is not well defined. Despite this, it is one of the most well-liked themes, and many businesses engage in its research and development [2]. Additionally, it is expected to release an increasing number of connected gadgets. IoT growth was influenced by this. Understanding its significance and difficulties is necessary because it is rapidly evolving and used in many goods. The phrase describes linking machines to the Internet that are not directly under human control [2]. These kinds of gadgets are "things." Such gadgets can be linked together to form an intelligent, invisible network [3], which can be attainable via the cloud. In contrast to the functionalities that each device can provide, the framework must provide a control system. Through that link, the smart devices are remotely programmed and operated. Since embedded technology enables Internet-based communication between IoT items or with users, all IoT products have this capability [4]. Numerous industries have built intelligent appliances. Nearly every day, a business declares the arrival of a new IoT-enabled product [5]. Wearable technology, connected vehicles, smart healthcare, and smart agriculture are some of the most well-liked applications. As a result, everyone can use wearable and smart medical gadgets to monitor their own activities or connected car solutions to operate their vehicles thanks to the Internet of Things. Smart homes are yet another Home automation solution that distinguishes as the most active segment. According to a 2015 data report, more than 50000 people look for "smart homes" regularly, and around 240 businesses and startups make investments in this sector [5]. The Nest Thermostat [6] and Philips Hue Light Bulb [7] are only two examples of the home appliances that can be integrated into a single, remote-accessible system using the method presented in this review. The fact that all setups are completed on a single device is the gateway's key benefit. In addition, procedures for maintaining security are thus essential just on that device. The method offered in this article offers a new open source smart home application that is implemented procedurally. Even though there are other projects that deal with this topic, it is simple to incorporate the system described in this paper within a real house. Users of the suggested design have the option of quickly adding new capabilities.

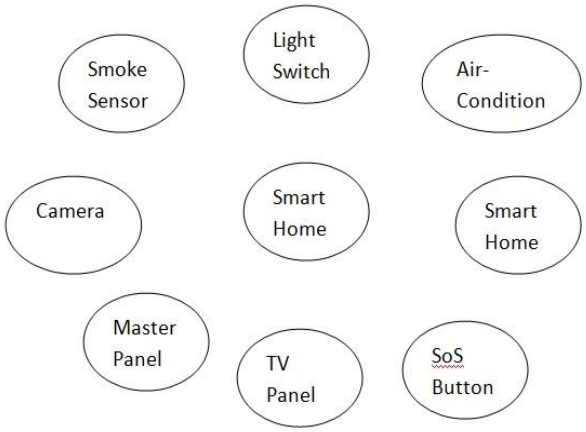

Fig. 1. States of Smart Home

II. LEADER OF FIELD

IoT activity was an attempt to develop an open source, global project. Using plugins, this project can easily incorporate more technologies. As a result, IoT activity allows a wide variety of devices with various communication protocols to engage with one another. The plan's goal is to develop a protocol for Internet communication that can be used by both wired and wireless devices. Projects for smart homes may be developed more easily as a result. As a result, this API allows for the integration of numerous information-transportation systems. They could be based on cloud communications, Bluetooth, or Wi-Fi.

Additionally, there are protocols that enable online and intranet communication between smart devicesTwo instances of this are Z-Wave and ZigBee [9]. For remote control, certain wireless methods were developed. Despite having identical concepts, the frequencies, transmission distances, and data rates between them vary. Sparrow sensor nodes were introduced by Tudose et al. [10] to build a smart home monitoring system. The gateway device receives data from the sensor nodes on a regular basis via Ip packets connections. Apple Home Kit [11] is an illustration of a smart home setup. This allows an iOS-powered Smartphone to operate home appliances. Data transport is encrypted and doesn't require the use of a separate gateway device. More than 50 brands of goods with built-in software are available through Home Kit [11]. Blinds, latches, valves, climate control, and illumination are a few features. The user can control and automate their activities after installing items on the phone with the relevant app from the Platform. Using Siri, they may create scenes and even give specific voice instructions. A substantial portion of these smart home products fall under the category of security equipment. Secure Dana An easy-to-install door locking device that fits into the deadbolt hole is the Bluetooth Z-Wave Smart Lock [12]. This allows you to unlock the door from a Smartphone and works with both Android and iOS-enabled Smartphone s. It may also allow other people to open the door with their consent. Oplink Integrated Alarm Protector [13] provides a different locking option. Samsung offers a system that combines additional controls and monitoring features for the house. The Smart Things Home Monitoring Kit [14] is a collection of gadgets that range from standard home monitors to mobile-controlled appliances. As a result, it is equipped with cameras, smoke detectors, and even lighting control systems. There are numerous different security devices that have been created, and the most of them employ cameras to monitor homes, such as the Drop cam Pro Mobile internet Wireless Video Monitoring Camera, Belkin Net Cam HD Wireless IP Camera, or D-Link - cloud Camera 5000 [15].

III. RELATED WORK

Two methods for implementing house security employing IoT are presented in Govinda et al(2014) .'s investigation into Design and Implementation of Security for Smart Homes based on GSM technology [16]. Using webcams that sound an alert and email the owner whenever the camera detects motion is one technique. Due to the price of the cameras employed, this method of detecting infiltration is incredibly successful but also relatively expensive. The cameras must be of high quality, which calls for a wide field of view and an image resolution strong enough to spot movement. Additionally, portable cameras like dome cameras will be far more expensive than fixed cameras. Instead of using regular SMS to send messages or alarms to the home owner, Karri and Daniel (2005) devised an SMS-based system using GSM. [17] Jayashri and Arvind (2013) created a fingerprint-based identification system for doors [18]. By only allowing users whose fingerprints have been registered by the home's owner, this technology helps users. By using the sensor, this technology can also be employed to control who enters the house. The system also comes with extra home safety capabilities like controlled burns and carbon monoxide leak detection. Fingerprint scanners are an excellent system, but they are pricey and difficult to integrate into an Interconnected setup. Some experts also believe that depending only on a fingerprint sensor is risky because it is relatively easy to lift and copy someone's fingerprints. In two-factor authentication systems that additionally incorporate an additional layer of protection, such as a PIN, Access codes, or virtual assistants, fingerprint scanners should always be used. [19] This inexpensive solution can manage both home automation and security with just a few requirements. This home security system does not employ a Smartphone app or other user interface, but simply the numbers from the device's dial. The system is platform independent, allowing it to be employed on a wide range of phones with different operating systems. The system operates when the launch pad is connected to wifi at home. The most

significant studies on the topic are discussed in this section. The authors provided a description of smart homes and their key components in [20]. Then they discussed a number of security issues relating to smart home devices. They also gave a description of the security studies that have been performed to address security challenges in smart homes, as well as some prospective solutions. The authors claim that this is the first of its kind "optical Morse code-based electronic locking system" and that it is an original idea that has never been studied. It was created using IoT technologies and Morse code, which is a novel method for building an electronic lock [21]. This device uses LEDs (Light emitting diodes) as an encryption medium to transmit signals. Smart phones' LEDs were used to increase accessibility for the general public. The optical signal can be decoded on the receiver's side after it has been picked up from the LED by a microcontroller, such as an Arduino processor, and a photosensitive resistor. After decoding the signal, it might upload the lock's present condition to the cloud so the owner can keep track of the lock. The system passed the authors' real-time testing, and they discovered that it operates as intended across a range of illumination conditions. Additionally, the designers assert that their user-friendly layout is straightforward. The IoT system here works really well and is accessible to everyone because cell phones are used as LEDs. It is also a less expensive option. [22] Anitha et al. (2016) suggested a model for artificial intelligence-based home automation systems and cyber security systems [23, 24]. There are numerous studies being done on this home automation system. J. Saha and his collaborators presented the Innovative Home automation Based Combined Virtual Monitoring System, Security Systems, and Security System [25]. The system combines security alarm, remote monitoring, and mobile healthcare monitoring. K. GB, D. Kumar, K. Pai, and Mannikandan J. proposed the design of a phoneme-based speech automation system for homes. Before suggesting an automated home that would use those audio signals, the authors studied a variety of speech signals [26]. An article on a smart home automation system using IP, Bluetooth, GSM, and Android is presented by A. Shinde and a coauthor [27]. Edge computing was introduced in the home automation system by T. Chakraborty and S. K. Datta in their paper, "Home automation integrating edge computing and the internet of things" (28). An IoT-based home automation system with a personal assistant was presented in a paper by Drs. V. Chayapathy, Anitha G. S., and Sharath B [29]. Using an IoT-based Sensing and Monitoring Platform, M. Al-Kuwari and his coauthor developed a system for smart house automation [30]. The authors provided a very simple explanation of how home automation might be accomplished using IoT. Additionally, numerous other researchers have conducted numerous studies on this home automation system. Besides, a huge number of scholars are still engaged in this large subject.

IV. IMPLEMENTATION

Hardware is used to display the Smart Home system's implementation. In order to operate home appliances and provide house safety and security against unintentional fires, short circuits, etc., the implementation configuration of a smart home system comprises of many hardware modules that are connected via a Wi-Fi module and an Arduino microcontroller. Three cases make up the entire hardware configuration. Wi-Fi enabled home automation in the first scenario. The second scenario configures IOT for temperature and humidity reading. In the third scenario, fire, short circuit, and overvoltage alerts are sent with GPS position information. This system's output is received through the use of a mobile app for smart home automation. Up until the system is connected to wifi via the internet, switching can be done using a mobile app from anywhere, both inside and outside the home. The humidity and temperature sensors are used with this Wi-Fi connection to make it simple to monitor the state of the house. Additionally, it helps with energy management systems. The temperature and moisture of the air are

measured, sensed, and reported by a humidity sensor. In building a database for a future analysis of the home's condition, this is very beneficial.

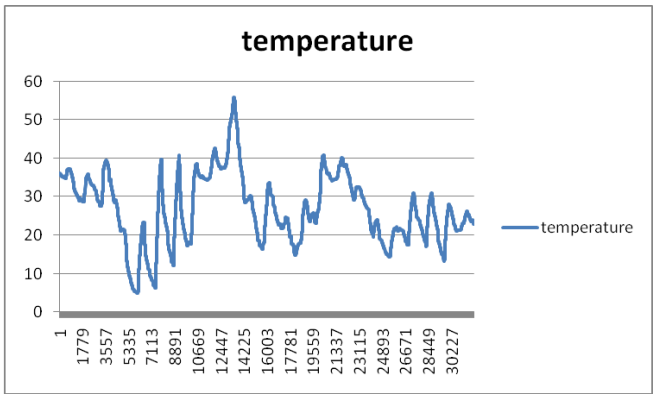

FIG. 2. TEMPERATURE

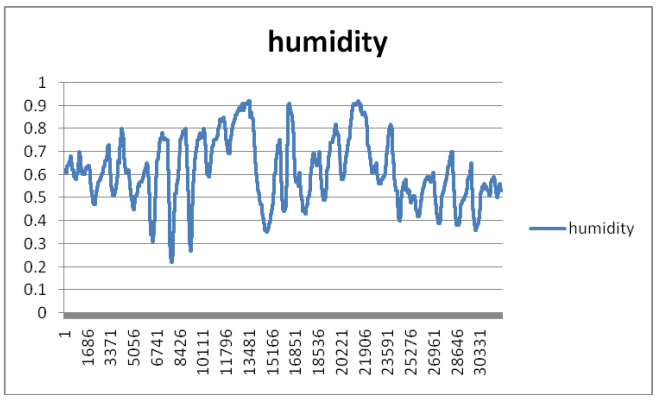

FIG. 3. HUMIDITY

Figures 2 and 3 show graphs of temperature and humidity over time for a single day and at a specific moment, which are updated as the temperature and humidity of the room change. Temperature and humidity sensors are used to collect the data for these graphs, which are then sent to the internet for additional analysis. The tenants of a home can examine the home environment from anywhere and take the necessary actions as needed with the aid of these data. When one travels to the office in the morning without thinking about anything other than merely going to work on time, it helps one to keep on top of life and saves money and energy.

V. CONCLUSION

Computer IoT-based home automation and security is quite useful for consumers who are far away. Any house can be monitored and controlled using the prototype described in this study. All internet-based apps are built on top of this IoT-based architecture. This research's technology is a low-cost IoT application solution. It is composed of light, user-friendly, and reasonably priced modules. It also makes information access and operation straightforward. Users can access files from any computer in the world thanks to it. Because objects produce more data than people do, it expands the advantages of internet productivity to include things as well as people. Our system can be used for a variety of reasons, some of which are given below. It is a prototype that offers a reliable, affordable, and efficient IOT application solution to the entire world. An oversight system for healthcare keeps track of the patient's health.

keeping an eye on the crowd Traffic management is crucial for intelligent transportation systems and path optimization. In order to reduce risks and maintain the structure, infrastructure monitoring is used to keep track on the building's infrastructure. Water management system to keep an eye on, among other things, leaks and water quality. An SCADA system is in charge of watching the grid station. Surveillance system. An environment monitoring system is used, for instance, to track noise or air pollution. A smart greenhouse system may have its properties controlled online. IoTs have the potential to revolutionize the field and make it a smart field in a number of other ways.

REFERENCES

[1] J. Stragier, L. Hauttekeete, L. Marez, Introducing Smart Grids in Residential Contexts: Consumers' Perception of Smart Household Appliances, Belgium, pp. 1-2, 2010

[2] P. Waher, Learning Internet of Things, Birmingham, pp. 1-3, 2015

[3] J. Chase, The Evolution of the Internet of Things, Texas Instruments, Texas, pp. 1-3, 2013

[4] D. Zhang, L. Yang, H. Huang, Searching in Internet of Things: Vision and Challenges, Busan, 2011

[5] K. Lueth, The 10 most popular Internet of Things applications right now, https://iot-analytics.com/10-internet-of-things-applications/, pp. 1, February 2015

[6] Nest Developers Documentation, http://developers.nest.com/, Last Access: April 20th 2016

[7] Philips Hue Developer Program, http://developers.meethue.com/, Last Access: April 20th 2016

[8] IoTivity, http://www.iotivity.org/, Last Access: April 24th 2016

[9] Lou Frenzel, Electronic Design, What's the difference between ZigBee and Z-Wave?, pp. 1, March 29th 2012

[10] D. S. Tudose, A. Voinescu, M.-T. Petrareanu, A. Bucur, D. Loghin, A. Bostan, and N. Tapus, "Home automation design using 6LoWPAN wireless sensor networks," in 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–6.

[11] Apple HomeKit, http://www.apple.com/ios/homekit/, Last Access: April 24th 2016

[12] Z-Wave Smart Lock, http://danalock.com/, Last Access: May 2016.

[13] The Oplink Connected Alarm Shield, http://www.oplinkconnected.com/, Last Access: May 2016.

[14] Samsung SmartThings Home Monitoring Kit, http://www.samsung.com/, Last Access: May 2016.

[15] 50 Best smart home Security Products, http://safesoundfamily.com/blog/50-best-smart-home-security-products/, Last Access: May 2016

[16] S. Kunwar and P. Sharma, "Social media: A new vector for cyber attack," 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), 2016, pp. 1-5, doi: 10.1109/ICACCA.2016.7578896.

[17] D. Herrick, "The social side of 'cyber power'? Social media and cyber operations," 2016 8th International Conference on Cyber Conflict (CyCon), 2016, pp. 99-111, doi: 10.1109/CYCON.2016.7529429.

[18] Statista. "Number of social media users worldwide from 2010 to 2021 (in billions)," 2017. [Online]. Available: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[19] C. Wuest, "The Risks of Social Networking," Symantec Corporation, Mountain View, CA, USA, 2010.

[20] P. Gundecha and H. Liu, "Mining social media: A brief introduction," New Directions in Informatics, Optimization, Logistics, and Production (Informs, 2012), pp. 1–17.

[21] R. Hekkala, K. Va€yrynen, and T. Wiander, “Information security challenges of social media for companies,” ECIS, p. 56, 2012.