Home Automation System

Edited By
Dr. Prabhu T.

March 2023

CIIR Research Publications

Contents

Preface

The automated and computerized control of household activities, features, and appliances is referred to as "home automation." Simply said, it means you can simply manage the appliances and features in your house online to improve convenience, increase security, and even save household expenses. Continue reading to get the answers to some frequently asked questions regarding home automation technology and to obtain some suggestions for home automation improvements.

A network of hardware, communication, and electrical interfaces called home automation connects commonplace devices to one another through the Internet. Whether you're at home or thousands of miles away, you can control any gadget from your smartphone or tablet since they all have sensors and WiFi connectivity. No matter where you are, you may use this to switch on the lights, lock the front door, or even lower the heat. A home automation system is composed of three major components: sensors, controllers, and actuators.

Sensors can keep an eye on variations in temperature, sunshine, or motion. Then, according to your preferences, home automation systems may change those settings and more. Computers, tablets, and smartphones that are used to transmit and receive signals regarding the status of automated systems in your house are referred to as controllers. The actual mechanism or function of a home automation system is controlled by actuators, which may be light switches, motors, or motorized valves. They are set up to be triggered by a controller's remote instruction.

What advantages does home automation offer?

A home automation system's main objective is to simplify household operations. Think about a few of these advantages:

Remote control: You may manage your house using a laptop, tablet, or smartphone.

Comfort: Make your house more livable and pleasant by using home automation. Set up smart speakers to play music when you return home from work, pre-program your thermostat with your favourite settings to ensure that your house is always at a suitable temperature, or change the brightness or opacity of your lights according to the time of day.

Convenience: Schedule the automatic activation of devices at certain times, or access their settings remotely from any location with an Internet connection. You can focus on more essential things when you don't have to remember to lock the door behind you or turn out the lights.

Increased safety: Home automation security features like pressure sensors, carbon monoxide monitors, and smart fire detectors may help shield your house from tragedy.

Energy conservation: Home automation enables you to be more aware of your power use. Reduce the amount of time that lights are left on or decrease the temperature in a room when you leave it to reduce energy use.

Dr. Prabhu T.
Editor

CHAPTER 1

INTRODUCTION TO HOME AUTOMATION

Mrs. Aruna M.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore India
Email Id-aruna.m@presidencyuniversity.in

Automation is the use of electronics and communication methods to make systems smarter. Automation aims to combine into a cogent, entirely new system that offers communication, energy management, comfort, and security functions as well as increased efficiency and dependability. The term "home automation" describes the automated and electronic management of elements, functions, and appliances in a home. We can effortlessly handle our home's utilities and features online. A remote monitoring system is composed of three major components: sensors, motors, and actuators [1]–[3].

The world is happy to have technology that is always improving. The main goals of technology are to make things easier and more efficient. The Internet of Things is given a lot of significance in today's trendy society. Automation facilitates greater efficiency with less effort. We have had experience utilizing the Internet of Things to operate numerous appliances, including home automation using a Node Microcontroller. Because modern technology relies entirely on communication, speech is the most efficient form of communication. Even while technology is improving in our daily lives, there is no support emerging for those who are physically unable of using technology. The voice control of the devices is implemented via the speech-enabled home automation system. It mostly targets the elderly and physically challenged people. If the voice recognition is bad, the home automation won't operate. The user's voice will be sent into the microphone as input. The speaker's voice is picked up by the microphone and sent to the speech recognition module. Even when there are disruptions, it looks for the closest word. The operation is carried out if the command (ON/OFF) is supplied [4]–[6].

The benefit of a smart house

The following is a list of smart homes' benefits:

- **Cost savings:** Energy and water consumption are reduced through connected appliances including having to learn smart thermostats, smart sprinklers, Wi-Fi-enabled lighting, electricity monitoring outlets, and water heater modules.
- The remote control is possible for many household appliances, including ovens, refrigerators, deadbolts, and garage doors, using apps on smartphones and tablets. Most of the time, this control also works while we are away from home, so we can check on the cat from Costa Rica, shut the garage door from either the airport, or make sure we turned off the stove from the grocery store.
- **Convenience:** Perhaps the ultimate pleasure of the smart home is having our living room lights switch on as we get home, the radio playing our favourite song and the front opening as we approached with a bag full of groceries. But luxury isn't the only aspect of

ISBN 978-81-962236-0-1 March 2023

convenience. We can use smart locks to control who has access and when eliminating the need to be home or hand out a key. Similarly to this, a sensor may alert us when our refrigerator is running low on milk, and a Wi-Fi doorbell enables us to "answer" our door from almost anywhere.

- **Security:** There are several straightforward, networked security options for the smart home that are less costly than continuously manned security systems. Live video feeds, email notifications, and text messages may all be used to monitor Wi-Fi-enabled cameras, linked motion detectors, and smart smoke alarms from within or outside a house.
- **Safety:** Because they can connect with us directly, no matter where we are, smart sensors that can notice water leaks, low humidity, carbon monoxide, motion, heat, and any other environmental worry conceivable help prevent mishaps from becoming tragedies.
- **Longer senior independence:** Home automation technologies like voice-activated alarm systems and automated aural reminders are just a few examples of how seniors may live independently for longer. Additionally, when family members are unable to visit the elderly in person, they may use Wi-Fi-linked webcams with two-way communication to keep a watch on them.

Control system for a smart home:

In recent years, there has been a lot of interest in smart home systems as a way to improve and simplify people's lives. Each member of the family has their demands and leisure activities met by an appropriate home automation system that connects all of the equipment in the house into a network. The essence of the home-automation system is the centralization of instructions; networked gadgets may identify and communicate with one another. Recent technological development produced a significant number of intelligent and sophisticated systems that supported smart living technology. We will employ wireless home automation in our project, which relies on several technical platforms. Wi-Fi is one of these platforms; read on to learn more about it and how it is used.

Bibliography

[1] M. Weglarski, P. Jankowski-Mihułowicz, M. Chamera, J. Dziedzic, and P. Kwaśnicki, “Designing antennas for RFID sensors in monitoring parameters of photovoltaic panels,” *Micromachines*, 2020, doi: 10.3390/MI11040420.

[2] M. Shahroz, M. F. Mushtaq, M. Ahmad, S. Ullah, A. Mehmood, and G. S. Choi, “IoT-Based Smart Shopping Cart Using Radio Frequency Identification,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2986681.

[3] V. Mulloni and M. Donelli, “Chipless RFID sensors for the internet of things: Challenges and opportunities,” *Sensors (Switzerland)*. 2020. doi: 10.3390/s20072135.

[4] V. Pradana and H. L. Wiharto, “Rancang Bangun Smart Locker Menggunakan Rfid Berbasis Arduino Uno,” *El Sains J. Elektro*, 2020, doi: 10.30996/elsains.v2i1.4016.

[5] M. Ullah and B. Sarkar, “Recovery-channel selection in a hybrid manufacturing-remanufacturing production model with RFID and product quality,” *Int. J. Prod. Econ.*, 2020, doi: 10.1016/j.ijpe.2019.07.017.

[6] E. F. Adwar and W. Wildian, “Rancang Bangun Sistem Absensi Berbasis RFID Terkoneksi Website Menggunakan Bahasa Pemrograman PHP dan MySQL,” *J. Fis. Unand*, 2020, doi: 10.25077/jfu.9.3.311-317.2020.

ISBN 978-81-962236-0-1 March 2023

CHAPTER 2

WIRELESS HOME AUTOMATION

Dr. Prabhu T.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- prabhu@presidencyuniversity.in

Wireless communication does not use any cables, wires, or other electrical conductors; instead, signals are sent over the air. With the development of wireless technology, there are more chances than ever to link devices and build home automation systems that can manage anything from entertainment systems to heating and lighting systems. There are many different sorts of loads that may be used to regulate home Wi-Fi. The following protocols may be used to describe several wireless types:

- **Bluetooth:** A wireless connecting standard for a wide variety of electronic products, including mobile phones, processors, and many more. Since Bluetooth technology is built into many electronic items, including mobile phones, it is simple to use Bluetooth devices for wireless control. It establishes communication with various electrical gadgets and creates a personal network operating in the 2.4 GHz range.
- **Radiofrequency:** This frequency range is employed for the distribution and transmission of communications. The use of two RF modules allows us to manage household appliances (transmitter and receiver). It is one of electromagnetic radiation's wireless waves, with wavelengths ranging from 3 kHz to 300 GHz [1]–[4]. A more potent and far-reaching RF gadget is ZigBee.
- **Z-Wave:** This wireless home automation system is relatively new. The more Z-Wave gadgets we have in our smart home, the more robust our smart home network becomes. Works on a mesh network and consumes very little electricity. The gadget operates in the sub gigahertz band, or around 900MHz. Locks, lights, and thermostats can communicate with one another thanks to Z-Wave technology. This serves as the framework for our smart home and allows us to build one-touch scenarios that facilitate everyday tasks using our smartphone or tablet.

Similar to Wi-Fi, Li-Fi is a bidirectional, fast, globally connected wireless communication system. Li-Fi is perfect for providing restricted spaces with high-density wireless data coverage and for reducing radio frequency interference problems. The smart house may be managed locally or remotely by the user. There are two components to the suggested system. The PIC microcontroller is used for software implementation to control several devices. And the hardware component, which switches between numerous devices to control them depending on the user's demands.

Cloud-based: To meet the rising public demand, current home monitoring technology is continuously enhancing its adaptability by introducing updated features. The cloud server, which monitors and regulates user data and information as well as appliance status, is the first of the system's three primary components. The hardware interface module, which provides the proper

ISBN 978-81-962236-0-1 March 2023

interface to the actuators and other sensors that offer the physical service, is the second component. The home Server, which primarily configures the computer system and offers the user interface, is the third component. This system leverages cloud-based web services, which are primarily required for data security and accessibility. It offers a secure lighting control environment for the whole family while also being affordable, pleasant, and dependable [5]–[8].

Global System: The Global System for Mobile Communication (GSM) uses Short Message Service (SMS) text messages to operate household appliances including lighting, climate control, and security systems. Using the frequency bandwidths, the GSM protocol enables the user to operate the target system from a location other than a residence. The creation of the smart GSM-based house automation system has made use of the idea of digital signals and AT commands. Homeowners may use their mobile phones to remotely turn on or off any controlled household equipment and get feedback on their status.

Wi-Fi: A personal computer may control appliances through Wi-Fi. The majority of WiFi devices employ the 2.4GHz band and frequency division multiplexing technology. To displace Ethernet via wireless communication across unlicensed bands, Wi-Fi is a wireless protocol. Because in-building Wi-Fi coverage is now almost universal, Wi-Fi is an obvious choice for IOT connection, but it is not necessarily the best option.

Bibliography

[1] M. Shahroz, M. F. Mushtaq, M. Ahmad, S. Ullah, A. Mehmood, and G. S. Choi, "IoT-Based Smart Shopping Cart Using Radio Frequency Identification," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2986681.

[2] V. Mulloni and M. Donelli, "Chipless RFID sensors for the internet of things: Challenges and opportunities," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20072135.

[3] F. Zhu, P. Li, H. Xu, and R. Wang, "A novel lightweight authentication scheme for rfid-based healthcare systems," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20174846.

[4] W. Shuaieb *et al.*, "RFID RSS fingerprinting system for wearable human activity recognition," *Futur. Internet*, 2020, doi: 10.3390/fi12020033.

[5] S. J. Thomas, "RFID for Everyone: An Easily-Accessible, Experimental UHF RFID Platform," *IEEE J. Radio Freq. Identif.*, 2020, doi: 10.1109/JRFID.2019.2941831.

[6] J. N. Luo and M. H. Yang, "A secure partial rfid ownership transfer protocol with multi-owners," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20010022.

[7] D. Noori, H. Shakeri, and M. Niazi Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment," *Eurasip J. Inf. Secur.*, 2020, doi: 10.1186/s13635-020-00114-x.

[8] Y. Shafiq, J. Henricks, C. P. Ambulo, T. H. Ware, and S. V. Georgakopoulos, "A Passive RFID Temperature Sensing Antenna with Liquid Crystal Elastomer Switching," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2969969.

CHAPTER 3

INTERNET OF THINGS (IoT)

Dr. Prabhu T.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- prabhu@presidencyuniversity.in

The Internet of Things is a key idea in Google Assistant-controlled home automation. With the introduction of cutting-edge methods for communicating between things and other things as well as between things and people, the Internet of Things (IoT) may link numerous sorts of products, including smartphones, personal computers, and tablets, to the internet.

The idea behind deploying IoT in the house is to automatically programme all of the gadgets that are already there. That is a smart house that is IoT-powered. Those tasks may be carried out with the push of a button rather than having to physically reach the gadget. Nowadays, the majority of smart IoT home automation gadgets let you manage them via an app or even your voice. Here, we get the information from the cloud and, while simultaneously displaying energy usage statistics on Blynk, turn on or off certain appliances following the information. IoT Components. An IoT solution is composed of these 5 fundamental elements. Objects (sensors), Networks (connectivity), Data, Information, and Operating Applications are the first three categories [1]–[3].

Home automation with IoT

All technologies that allow a device to be connected to the internet are collectively referred to as the "Internet of Things" (IoT). These systems rely on data gathering. The information is then utilised to monitor, manage, and transmit data to other devices through the internet. This enables certain activities to be initiated automatically whenever particular circumstances occur. IoT is used by a wide variety of devices. This allowed it to penetrate a variety of industries, including smart homes [4]–[6].

The idea behind deploying IoT in the house is to automatically programme all of the gadgets that are already there. That is a smart house that is IoT-powered. Those tasks may be carried out with the push of a button rather than having to physically reach the gadget. Nowadays, the majority of smart IoT home automation gadgets let you manage them via an app or even your voice.

IoT in home automation refers to all linked smart metres, security systems, thermostats, smoke detectors, presence detectors, and other sensors that are connected to home automation box-type devices. IoT home automation refers to the house doing certain tasks automatically. Wi-role Fi's in the Internet of Things: Different Internet of Things applications demand different levels of connection in terms of range, data speed, energy efficiency, and device cost. Due to the widespread availability of in-building Wi-Fi, it is often the logical option. Due to the popularity of its family of standards, Wi-Fi has the benefit of supporting a highly diverse range of profiles. It will thus be used in the majority of IoT contexts, either alone or in conjunction with other, more specific protocols or cellular. Some Internet of Things (IoT) applications, such as those for vehicles or those that use video, like those for linked security cameras, will need the wireless broadband

ISBN 978-81-962236-0-1 March 2023

network's capacity to meet other needs. Wi-Fi is in a unique position to serve both broadband and narrowband Internet of Things (IoT) applications from a single platform that can operate at various power consumption and signal range levels. To enable new scenarios in the URLLC (ultra-reliable low latency communications) category, this will emphasise IoT-focused characteristics such as latency and extremely high availability. Wi- Fi's in the IoT world is sometimes underestimated. Some IoT applications that need high bandwidth and low latency may be supported by Wi-Fi.

Wi-Fi home automation system:

Wi-Fi (short for Wireless Fidelity) is a wireless technology that transmits data across the air using radio frequency. Wi-Fi, which stands for Wireless Fidelity, is a wireless technology that utilises radio frequency to send data across the air and is used in home automation systems. Home automation systems employ Android-based applications and Wi-Fi for communication and appliance control, respectively. A smart home system enables real-time mobile monitoring of the state of home security as well as remote control of household equipment. Users can communicate with household appliances, as well as monitor and command equipment remotely.

Given its benefits over utilising a dedicated computer, this system employs an android smartphone to monitor and manage numerous home settings. There are two basic parts to this technology. The first is the server (webserver), which shows the system core and controls, maintains and monitors users' homes. Users and the system administrator may manage and control system code locally (LAN) or remotely (internet). The second component is the hardware interface module, which offers the sensors and actuators of the home automation system with the proper interface. The suggested system is scalable, which means that one server may handle several hardware interface modules as long as they are within the range of a Wi-Fi network, in contrast to the majority of home automation systems now on the market. The system supports a large variety of home automation devices, including security and power control components. Comparing the suggested system to commercially existing home automation systems, the proposed system is superior in terms of flexibility and scalability.

Bibliography

[1] S. J. Thomas, “RFID for Everyone: An Easily-Accessible, Experimental UHF RFID Platform,” *IEEE J. Radio Freq. Identif.*, 2020, doi: 10.1109/JRFID.2019.2941831.

[2] D. Noori, H. Shakeri, and M. Niazi Torshiz, “Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment,” *Eurasip J. Inf. Secur.*, 2020, doi: 10.1186/s13635-020-00114-x.

[3] M. Veigt, E. Hardi, M. Koerdt, A. S. Herrmann, and M. Freitag, “Investigation of using RFID for cure monitoring of glass fiber-reinforced plastics,” *Prod. Eng.*, 2020, doi: 10.1007/s11740-020-00972-x.

[4] O. Adepoju, “Internet of Things (IoT),” in *Springer Tracts in Civil Engineering*, 2022. doi: 10.1007/978-3-030-85973-2_8.

[5] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A Literature Review,” *J. Comput. Commun.*, 2015, doi: 10.4236/jcc.2015.35021.

[6] M. Q. Aldossari and A. Sidorova, "Consumer Acceptance of Internet of Things (IoT): Smart Home Context," *J. Comput. Inf. Syst.*, 2020, doi: 10.1080/08874417.2018.1543000.

ISBN 978-81-962236-0-1 March 2023

CHAPTER 4

BASIC HOME AUTOMATION APPLICATIONS

Dr. Prabhu T.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- prabhu@presidencyuniversity.in

Users can manage and control many parts of their homes via remote home monitoring. These include controlling lights, locks, fans, and other devices from a laptop, tablet, or smartphone. They also feature motion detection, water leak detection, and temperature monitoring to prevent theft and fire. The advent of specialised equipment, such as water heaters to speed up the process of boiling water for baths and computerized washing machines to eliminate the need for human laundry, has automated many home tasks. Homes are wired for electrical power, doorbells, TV outlets, and telephones in industrialised nations. The light goes on in the separate application when someone enters the room. With modern technology, space can detect a person's presence and identify them. It may also adjust the appropriate lighting, temperature, television stations, or music levels by taking into consideration the day next week, the time of day, and other such criteria.

This project suggests such a low-cost solution. The Google Assistant, IFTTT, Blynk, and the Node Micro-controller serve as the device's main building blocks, together with a relay board with four relays. The Google Assistant receives orders in natural language speech. Since every component is linked to the internet through WiFi, this system falls under the umbrella of the Internet of Things.

The hardware can connect to the router. These two groups make up the system design. Additionally, it would be able to switch on and off certain devices, such as lights and fans. It's referred to as the "Control Unit." The software of the design is made up of Google Assistant, the Blynk app, and the IFTTT app, which are all incorporated into the Android smartphone. The microcontroller NodeMCU and the obtained as a result make up the control unit. Transistors are used on the relay board to command the relays. An Android device's Blynk app connects to the microcontroller and uses the internet to transmit the appropriate signal [1]–[3].

This system's hardware architecture comprises a smartphone and Node MCU. Internet-based wireless communication is used to connect the Node MCU and the smartphone. Google Assistant, a speech recognition capability integrated into the Android operating system, is used to create smartphone applications that may be used to voice-command household appliances. This programme turns the user's voice command into text, which it then sends to the Blynk libraries, which are linked to the Node MCU via the IFTTT website, which stands for "IF THIS THEN THAT" and is a platform for building simple conditional statements known as "applets."

One benefit of a voice-controlled smart home system is that a user simply has to say the appliance's name into their smartphone's microphone to turn it ON or OFF. By doing this, users can quickly and effortlessly operate their home appliances. A speech recognition programme offered consumers a user-friendly interface and the option to integrate additional household equipment.

ISBN 978-81-962236-0-1 March 2023

Every structure that uses electrical appliances and equipment may utilise this home automation system [4], [5].

Voice Commands:

The "mind" of home automation is the voice control system. This control system ensures the person's comfort and safety while doing a variety of household tasks including security, heating, ventilation, lighting, entertainment, and other home systems. The voice control system research is introduced in this chapter. We'll introduce the voice command general from the outset. The voice will then be introduced to us. Then, to learn more about our investigation into voice control, we'll talk about speech recognition, beginning with its definition, applications, and workings. After getting a sense of the speech recognition algorithms, we will learn about natural-language processing and how it performs before discussing its benefits and drawbacks. Finally, we will discuss voice recognition software, particularly software for intelligent personal assistants. Voice control is an interface that allows users to enter commands into a system using voice communications. In this scenario, the user talks into a microphone, and a computer with speech recognition software analyses what he says to identify the command that should be performed.

The platforms for voice control in home automation provide a hands-free approach to handling lights, thermostats, door locks, and other devices. The voice control is useful if everyone at home is busy, such as when they are juggling five things at once, have wet hands, or full arms, or are simply in the central portion of something else when the house phone rings, they need more light, or they want to change the channel on the TV or switch to a different song. Sure, they could stop what they're doing, tidy up, set something down, or otherwise make themselves more accessible to the different controllers. However, it would be simpler, quicker, and more practical to just instruct the house to undertake the work and have it manage all household chores. Thanks to the large range of voice-controllable gadgets that are readily available. Using hands-free home control through interactive voice assistants and smart speakers from Josh.ai, Apple, Amazon, and Google are not only feasible but rather pleasurable [6], [7].

Bibliography

[1] W. H. Yen, H. R. Ke, and W. P. Yang, “An infrastructure for creating web automation applications,” 2021.

[2] M. L. Y. Sin, V. Gau, J. C. Liao, and P. K. Wong, “Electrothermal fluid manipulation of high-conductivity samples for laboratory automation applications,” *JALA - J. Assoc. Lab. Autom.*, 2010, doi: 10.1016/j.jala.2010.05.004.

[3] P. M. B. Mansingh and M. Yuvaraju, “Improved data transmission using Li-Fi technology for home automation application,” *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02072-1.

[4] Y. P. Cheng, C. W. Li, and Y. C. Chen, “Apply computer vision in GUI automation for industrial applications,” *Math. Biosci. Eng.*, 2019, doi: 10.3934/mbe.2019378.

[5] R. D. Lorenz, “Robotics and Automation Applications of Drives and Converters,” *Proc. IEEE*, 2001, doi: 10.1109/5.931495.

[6] M. Attaran, "The impact of 5G on the evolution of intelligent automation and industry digitization," *J. Ambient Intell. Humaniz. Comput.*, 2021, doi: 10.1007/s12652-020-02521-x.

[7] M. Collotta, G. Scatà, and G. Pau, "A priority-based CSMA/CA mechanism to support deadline-aware scheduling in home automation applications using IEEE 802.15.4," *Int. J. Distrib. Sens. Networks*, 2013, doi: 10.1155/2013/139804.

CHAPTER 5

VOICE EXPLANATION

Dr. Manikandan M.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- manikandan.m@presidencyuniversity.in

However, sound does not propagate in a vacuum. Sound propagates as waves that vibrate, which determines the properties of diffuse sound. The speed of sound changes depending on the medium since it is quicker in solid media than liquid media and faster in Liquid media is invasive. Mechanical waves are waves that pass via physical media and cannot propagate in the absence of a physical medium. In physics, the sound is characterized as a longitudinal mechanical wave. When a wave's path of propagation coincides with its direction of vibration, we may say that the wave is longitudinal [1]–[3].

Living things communicate with one another through sound. For instance, when a person speaks, their vocal cords vibrate as they release air from the lungs in certain amounts, causing distinct waves to emerge from the lips until the letters are uttered. Loudness induces a sense of anxiety at the other end.

Speech Synthesis:

A subject of computational linguistics and computer science known as "speech recognition" or "voice recognition" explores approaches and technologies that allow computers to recognise and translate spoken language into text. To decipher human speech, comprehend verbal orders, and carry them out. Voice recognition software is often used to control devices, issue instructions, or write without the need for a keyboard, mouse, or button presses. It is often referred to as speech-to-text, computer voice recognition, or automated speech recognition (ASR). It draws on expertise and research from the domains of computer science, linguistics, and computer engineering.

Customers may connect with technology by speaking directly to it using voice recognition systems, which enable hands-free requests, reminders, and other basic functions. A speaker must "train" (also known as "enrol") certain voice recognition systems by reading text or a small vocabulary to the device. The accuracy of speech recognition is improved by the system's analysis of the individual's voice and utilisation of that information. "Speaker-independent" systems are those that don't need training. Training-based systems are referred to be "speaker-dependent".

Applications for speech recognition include voice user interfaces like voice dialling (for example, "call home"), call routing (for example, "I would like to make a collect call"), demotic appliance control, search keywords (for example, "find a podcast where particular words were spoken"), simple data entry (for example, "enter a credit card number"), preparation of structured documents (for example, a radiology report), identification of speaker characteristics, and speech-to-text processing (for example, word processor (usually termed direct voice input) [4]–[6].

ISBN 978-81-962236-0-1 March 2023

Speaker identification, often known as voice recognition, relates to recognising the speaker rather than what they are saying. In systems that have been trained on a particular person's voice, interpreting speech may be made simpler by being able to identify the speaker. It can also be used to authenticate or verify a speaker's identity as part of a security procedure.

From a technological standpoint, speech recognition has a lengthy history and has seen several significant technological advancements. Recent developments in deep learning and big data have improved the area. Not only has there been an increase in academic papers published on the topic, but more significantly, the global industry has adopted several deep learning techniques for creating and implementing voice recognition systems [7]–[9].

Uses for speech recognition

The usage of digital assistants and speech recognition technology has fast expanded from our mobile phones to our homes, and its applications in sectors like business, banking, marketing, and healthcare are soon becoming clear.

In the office

In the workplace, speech recognition technology has advanced beyond jobs that formerly required people to do them and into the inclusion of basic tasks to boost productivity as

- Look up papers or reports on your PC.
- Use data to create a graph or tables.
- The details you wish to be included in a document should be dictated.
- Printing requests for documents.
- Video conferencing may begin.
- Plan your meetings.
- Take down minutes.
- Make your trip plans.

Bibliography

[1] S. Thiruvengadam and S. Gokulakrishnan, “Library Management System using RFID,” *Int. J. Comput. Appl.*, 2020, doi: 10.5120/ijca2020920561.

[2] S. N. R. Kantareddy *et al.*, “Perovskite PV-Powered RFID: Enabling Low-Cost Self-Powered IoT Sensors,” *IEEE Sens. J.*, 2020, doi: 10.1109/JSEN.2019.2939293.

[3] J. Su, A. X. Liu, Z. Sheng, and Y. Chen, “A partitioning approach to RFID identification,” *IEEE/ACM Trans. Netw.*, 2020, doi: 10.1109/TNET.2020.3004852.

[4] G. N. Kumar, M. Prasanna Kumar, K. Praveen Kumar, R. Radha, and M. G. Shanthi, “Automatic Library Door Opening System Using RFID,” *Int. J. Sci. Res. Eng. Dev.*, 2020.

[5] P. López-Matencio, J. Vales-Alonso, and J. J. Alcaraz, “LBTM: Listen-before-talk protocol for multiclass UHF RFID networks,” *Sensors (Switzerland)*, 2020, doi: 10.3390/s20082313.

[6] B. Rahmadya, R. Sun, S. Takeda, K. Kagoshima, and M. Umehira, "A framework to determine secure distances for either drones or robots based inventory management systems," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3024963.

[7] T. Libby, "The influence of voice and explanation on performance in a participative budgeting setting," *Accounting, Organ. Soc.*, 1999, doi: 10.1016/S0361-3682(98)00043-9.

[8] D. Kingston, N. G. Moghaddam, and D. L. Dawson, "How do differential explanations of voice-hearing influence attributions and behavioral intentions towards voice-hearers?," *Psychiatry Res.*, 2016, doi: 10.1016/j.psychres.2016.01.039.

[9] F. Rolland and D. D. Steiner, "Test-taker reactions to the selection process: Effects of outcome favorability, explanations, and voice on fairness perceptions," *J. Appl. Soc. Psychol.*, 2007, doi: 10.1111/j.1559-1816.2007.00282.x.

CHAPTER 6

BANKING MANAGEMENT

Dr. Manikandan M.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- manikandan.m@presidencyuniversity.in

The goal of the financial services and banking industries is to make customer interactions using voice recognition less difficult. Voice-activated banking might significantly cut down on the requirement for in-person customer support, which would also decrease labour expenses. Customer happiness and loyalty may increase as a result of a personalised banking assistant. Banking might be improved via speech recognition: Without having to unlock your phone, ask for information about your position, transactions, and spending patterns, Pay your debts. Obtain details on your transactional history [1]–[3].

Within Marketing:

Voice search can provide advertisers with a new approach to connecting with their target audience. Marketers should watch for emerging patterns in customer information and behaviour given the shift in how consumers will engage with their devices. Data - With voice recognition, marketers will have access to a new kind of data to analyse. A person's vocabulary, speech habits, and accent may all be utilised to understand them.

Voice recognition infographics,

Today, automated speech recognition (ASR) software applications are used to do this on a computer. Many sectors, including healthcare, the military (such as F-16 fighter planes), telecommunications, and personal computers employ ASR programmes (i.e. hands-free computing) location, age, and other demographic data about customers, such as their cultural background [4]–[6].

- Behaviour: While speaking allows for lengthier, more conversational searches, typing requires a certain amount of brevity. To keep on top of these developments, marketers and SEO specialists may need to concentrate on creating conversational content and long-tail keywords.
- Users could become more impatient and more reliant on using the internet as their primary information source as a result of this quick search method. As a result, the duration
- Users' time spent staring at screens may reduce. Marketers should think about what this would entail for mostly visual content since there might be a move towards emphasising material that is aural and information-heavy.

Medical Care

Hands-free, instant access to information may considerably improve patient safety and medical effectiveness in a setting where seconds count and sterile working conditions are a concern. Benefits comprise:

ISBN 978-81-962236-0-1 March 2023

Nurses might be instructed specifically or have procedures reiterated to them swiftly obtaining information from medical records. The number of patients on a floor and the number of available units are two administrative facts that nurses might inquire about. Parents may seek information on common sickness symptoms, when to see the doctor, and how to care for a sick kid at home.

- Reduced paperwork
- Decrease in data entry time.
- Enhanced processes.

The Internet of Things allows for Right now, one of the most well-known uses of voice-activated in the internet of things is in automobiles. By 2020, it is anticipated that one in every five vehicles will be online. The benefits of this might alter how we operate our cars and interact with them, ultimately reducing driver distraction. Application of digital assistants in vehicles: Hands-free message listening.

- Manage the radio.
- Help with navigating and guiding.
- Observe voice instructions.

Voice Recognition Works

Computer voice recognition programmes need the analogue-to-digital conversion of analogue audio into digital signals. A computer needs a digital vocabulary or database of words or syllables, as well as a quick way to compare this information to signals, to decode signals. When the software is executed, the speech patterns are put into memory from storage on the hard drive. Pattern recognition is the process of comparing these saved patterns to the A/D converter's output using a comparator.

In reality, the amount of random access memory available on the computer where a speech recognition application is installed closely correlates with the size of the program's effective vocabulary. If the full vocabulary can be put into RAM, as opposed to scanning the hard drive for part of the matches, speech recognition software will operate much more quickly. Additionally, processing speed is important since it influences how quickly the computer can look for matches in the RAM. Although speech recognition began on PCs, it has now spread to mobile devices, home assistants, and other consumer and commercial items. Speech recognition technology was able to into consumer pockets because of the widespread use of smartphones, and voice recognition technology entered homes thanks to products like Google Home and Amazon Echo. Many consumer goods that were not previously smart have gained a technical layer thanks to voice recognition and the expanding range of internet of things sensors. The businesses developing voice recognition software will have more data and details to feed into the machine learning that drives voice recognition systems, increasing the capabilities and accuracy of the voice recognition products as uses for voice recognition technology expand and more users interact with it.

Speech Recognizing Software:

ISBN 978-81-962236-0-1 March 2023

Spreadsheets and database tables are two examples of organised data that computers excel at handling. But people often speak to one another using words, not tables. Computers are unfortunate by this. Unstructured text in English or another human language makes up a large portion of the world's information. Therefore, we'll go into further detail on how to teach a computer to comprehend unstructured writing and get data from people.

Natural Language Processing, or NLP for short, is the branch of research that focuses on the interactions between human language and computers. It is at the nexus of computational linguistics, artificial intelligence, and computer science. NLP is a clever and practical method for computers to comprehend, evaluate, and extrapolate meaning from human language. Simply described, natural language processing, or NLP, is the area of artificial intelligence that focuses on making it possible for computers to comprehend and analyse human languages. So that a computer can comprehend unstructured language and extract data from it, let's examine how NLP works on mobile phones' speech recognition technology

Intelligent virtual assistants (IVA) or intelligent personal assistants (IPA) are significant developments that have integrated seamlessly into the process of widespread digitization. These IPA are now present in every modern technology, including smartwatches, tablets, and smartphones. An artificial intelligence-based (AI-based) tool called an IPA is a software agent that may carry out activities or provide services on behalf of a person in response to requests or enquiries.

Some virtual helpers can understand human speech and reply with synthetic voices. Users may handle other simple activities, ask inquiries to their assistants, and use voice commands to control home automation equipment and media playing. The conversation systems are based on an idea that is similar yet different. A "personal assistant," "digital assistant," "intelligent agent," and "voice assistant" are some names for it. With Siri in 2011, Apple made the idea more well-known, and Google, Microsoft, and Amazon soon followed. In addition to calling and setting alarms, reminders, and calendar appointments, virtual assistants may also switch on lights, music, and other smart home appliances. Results get increasingly individualised with time. The first kind of artificial intelligence that millions of people utilise regularly is virtual assistants.

Bibliography

[1] M. Leo, S. Sharma, and K. Maddulety, “Machine learning in banking risk management: A literature review,” *Risks*, 2019, doi: 10.3390/risks7010029.

[2] E. Principles, “Pathways To Sustainable Banking Management,” *Ann. Univ. Oradea Econ. Sci.*, 2010.

[3] S. S. Mahdy, “Risk management in Islamic banking,” *Qual. - Access to Success*, 2012, doi: 10.9790/5933-0803012739.

[4] N. Andleeb, M. Fauzi Ahmad, and S. Aziz, “Organizational Culture and Knowledge Sharing in Banking Management,” in *Banking and Finance*, 2020. doi: 10.5772/intechopen.92728.

[5] A. Elzamly, B. Hussin, S. A. Naser, K. Khanfar, M. Doheir, A. Selamat, and A. Rashed, “A

new conceptual framework modelling for cloud computing risk management in banking organizations," *Int. J. Grid Distrib. Comput.*, 2016, doi: 10.14257/ijgdc.2016.9.9.13.

[6] S. Suharli, A. Wahab, and A. Hamid Habbe, "Application Of Islamic Economic Principles In Realizing Management Banking Without Interest," *Dinasti Int. J. Educ. Manag. Soc. Sci.*, 2022, doi: 10.31933/dijemss.v3i2.1071.

CHAPTER 7

VOICE USER INTERFACE

Dr. Manikandan M.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- manikandan.m@presidencyuniversity.in

The use of speech input in the voice user interface (voice UI) is crucial for improving the usability of tiny portable devices like mobile phones. The smaller size, short battery life, and high cost of these devices place restrictions on more conventional methods of interaction (such as keyboard and display). Man-machine interfaces are thought to interact naturally via speech. Voice user interfaces are now being extensively used and accepted in commercial applications after decades of study and development. In the next years, it is anticipated that the worldwide spread of embedded devices would reinforce this tendency even further. Automatic speech recognition is a key piece of technology for voice user interfaces [1]–[3].

Speech recognition, voice analysis, and language processing are all combined into one personal assistant. When a user requests that a personal assistant conduct an action on their behalf. To identify an appropriate response, this information is compared with a repository of the programme using a cutting-edge algorithm. Distributed computers in cloud networks host this database. Because of this, the majority of personal assistants need a strong Internet connection to function. The software's database grows and is optimised with an increase in queries, which enhances speech recognition and shortens the system's response time. Voice assistants can operate a comprehensive digital infrastructure provided by major corporations like Amazon, Google, Microsoft, and Apple.

Using Google Assistant

Google Assistant is a virtual assistant that uses artificial intelligence and is largely accessible on Android, Google Home, Wear OS, Android TV, and other smart home devices. Although keystroke input is also allowed, users communicate with Google Assistant mostly via natural speech. The Assistant can do web searches, create reminders and alarms, change hardware preferences on the user's device, and display data from the user's Google account. Additionally, according to Google, the Assistant will allow transferring money, making purchases, and recognise tunes in addition to being able to recognise items and identify them using the camera on the device.

Building on the already-existing Google Voice instructions, Google Voice Assistant was created to be more conversational, friendly, and personalised. The Google Voice Assistant is known as Google Assistant. Designed At first, Google Assistant carefully selects informational tidbits that are relevant to you. He was able to provide you with the information that is important to you since he was aware of your workplace, meetings, vacation plans, favourite sports teams, and areas of interest. These individual components are combined with several voice commands by Google Assistant. Regardless of the input mode you choose, the discussion will continue whether you use text or voice.

ISBN 978-81-962236-0-1 March 2023

After pronouncing the wakeup phrases "OK Google" or "Hey, Google," the Google Assistant delivers voice commands, voice search, and speech-triggered device control, enabling us to carry out a range of activities. It is designed to enable conversational exchanges between us.

Control our smart home and gadgets. Get access to our calendar and other personal data. Find information online, including reservations at restaurants, travel plans, weather, and news.

- Adapt our music
- Play content on our Chromecast or other appropriate devices.
- Timer and reminders for running
- Schedule a meeting and send messages.
- launch the applications on our phone
- Please read our alerts.
- Real-time translations of speech
- play video games

We may ask for follow-up information without saying "Hey Google" if there is a constant discussion. Instead, once we begin conversing with Google, it waits for a response without always requiring a trigger word. Google can distinguish between distinct speech profiles, so it can respond appropriately based on who is speaking to it. Additionally, we have the option to make many requests at once. Name-calling, phone book searches, command-and-control, and more recently huge vocabulary dictation are a few examples of mobile phone apps that use integrated ASR. In the context of mobile devices, several technical obstacles must be addressed, including those caused by environmental noise, the limits of current hardware platforms and financial restraints, and the need for extensive language support. Additionally, for user adoption, mobile ASR systems must reach a nearly flawless performance level. This chapter analyses the use of embedded ASR in mobile phones and discusses particular problems with language creation, noise robustness, embedded platforms, and embedded implementation. Throughout the chapter, several useful solutions are provided with accompanying experimental data a smart personal helper [4]–[6].

Bibliography

[1] Q. Ma, R. Zhou, C. Zhang, and Z. Chen, “Rationally or emotionally: how should voice user interfaces reply to users of different genders considering user experience?,” *Cogn. Technol. Work*, 2022, doi: 10.1007/s10111-021-00687-8.

[2] H. S. Koo, “Design and Implementation of Command-and-Control Voice User Interface for Server Management Systems,” *Trans. Korean Inst. Electr. Eng.*, 2021, doi: 10.5370/KIEE.2021.70.1.207.

[3] Q. N. Nguyen, A. Ta, and V. Prybutok, “An Integrated Model of Voice-User Interface Continuance Intention: The Gender Effect,” *Int. J. Hum. Comput. Interact.*, 2019, doi: 10.1080/10447318.2018.1525023.

[4] L. Zhang, S. Tan, Z. Wang, Y. Ren, Z. Wang, and J. Yang, “VibLive: A Continuous Liveness Detection for Secure Voice User Interface in IoT Environment,” 2020. doi: 10.1145/3427228.3427281.

[5] A. K. Ostrowski, V. Zygouras, H. W. Park, and C. Breazeal, "Small group interactions with voice-user interfaces: Exploring social embodiment, rapport, and engagement," 2021. doi: 10.1145/3434073.3444655.

[6] E. Corbett and A. Weber, "What can i say? Addressing user experience challenges of a mobile voice user interface for accessibility," 2016. doi: 10.1145/2935334.2935386.

ISBN 978-81-962236-0-1 March 2023

CHAPTER 8

INTRODUCTION TO HOME AUTOMATION AND SECURITY SYSTEM

Ms. Akshaya M. Ganorkar
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- akshayamganorkar@presidencyuniversity.in

The term "Internet of Things" (IoT) refers to actual physical things or collections of things that include sensors, computing power, software, and other technologies that can connect to and exchange data with other gadgets and systems through the Internet or other communications networks. The term "Internet of Things" (IoT) is misleading since gadgets only need to be individually accessed and linked to a network, not the public internet. The fusion of several technologies, including computers, sensors, embedded systems, machine learning, and networking, has led to the evolution of the Internet of Things. The Internet of things is essential to the traditional domains of embedded systems, wireless sensor networks, control systems, and home automation [1]–[3].

The IoT-based Home Automation system seeks to use internet protocols to operate all of the smart home's appliances, as the name indicates. Home automation attempts to provide users more access to home gadgets, lighting options, and improved energy conservation with optimal use of energy by putting control of running common household electrical equipment at their fingertips. The idea goes beyond simple lighting solutions to include complete management over home security, as well as temperature, humidity, moisture monitoring devices, and much more. The idea of home management, which might encompass lighting, sensing, and security systems, includes IoT devices as a key component. The house automation system is adaptable since it can be enlarged, convenient, and user-friendly thanks to the bespoke dashboard's simple and intuitive user interface [4]–[6]. Additionally, it uses less energy and provides home security features and intrusion prevention by continually watching the house and informing the user in the event of an intruder.

- Create a system for home automation.
- Create a unique online dashboard to show the status and real-time data from numerous sensors without the need for a third-party platform.
- Implementing networking, IoT, and internet technologies in real life can help you fully grasp these ideas.

Web Dashboard

The real-time data from the sensors is shown without the need for a third-party platform, in contrast to most modern models of the project. A custom dashboard website made using HTML, JS, and CSS is used to display data and update sensor status. This offers the chance to add or delete certain devices from the automation system, alter the dashboard's design to better suit the requirements of the user, and provide flexibility by modifying minor codes to make it genuinely unique.

Security System

The If This Then That (IFTTT) platform's API is used in this project's magnetic door sensors and motion sensors, such as the MH SR602, to continually monitor the house for infiltration and alert the user if there is a security breach.

Scalability

The bespoke dashboard website and home automation system are meant to be expandable and customizable. A wide range of features, including gas detection, water level detection, ambient light sensing, camera

ISBN 978-81-962236-0-1 March 2023

monitoring, and others, can be added with minimal code and circuitry changes, and the functionality and user interface of the custom dashboard website can be expanded to best accommodate the added functionality.

Programming for microcontrollers and sensor technologies

The Wi-Fi module receives data from a network of several sensors that make up the home automation system. To store, process, and deliver the data on the customs website dashboard, the microcontroller is coded in C++ using the Arduino IDE and several libraries. The ESP8266, which is a microcontroller and Wi-Fi board, is the first Wi-Fi board, device, and sensor that was researched and utilised in the project.

- Motion sensor MHSR02 and magnetic door sensor MC38 for home security
- DHT 11 soil moisture sensor and temperature and humidity sensors to read different factors

Web Technologies

Web technology describes the numerous methods and tools used in the process of interacting with various internet-connected devices. B.Tech. Electronics and Communication Engineering / June 2022 the web technologies researched and utilised in the project to create the custom website dashboard.

- Hypertext Markup Language, or HTML. The code for the custom dashboard website is called HTML, which combines markup language and hypertext.
- Cascading Style Sheets, or CSS, is a straightforwardly constructed language that makes it easier to show web pages. It enables you to add styles, such as colours and effects, to custom dashboard websites, enabling distinctive customisation.
- The programming language JavaScript is used to add functionality to items, such as describing what should happen when a button is pushed and many other things.
- In a custom dashboard website, AJAX is utilised to interact with the server without reloading the page, improving user experience.

Networking

Data such as temperature, humidity, and the condition of each sensor inside the system are sent and exchanged through networking to the custom dashboard website. To construct, maintain, and operate the network, several ideas and protocols are researched and employed, including:

- Wi-Fi facilitates the creation of the network linking the ESP8266, the sensors, and the custom dashboard website.
- The networking protocol employed in the project is TCP/IP.
- If there is a security breach in the home security subsystem, IFTTT offers the application programming interface to alert the user.

Bibliography

[1] G. Anitha, M. Sathya, S. Suganeswar, and G. Vignesh Raja, “Retraction: Bluetooth Based Home Automation and Security System,” *Journal of Physics: Conference Series*. 2021. doi: 10.1088/1742-6596/1916/1/012106.

[2] V. Graveto, T. Cruz, and P. Simões, “Security of Building Automation and Control Systems: Survey and future research directions,” *Comput. Secur.*, 2022, doi: 10.1016/j.cose.2021.102527.

[3] N. A. Al-Shareefi, S. A. Abbas, M. S. Alkhazraji, and A. A. R. Sakran, “Towards secure smart cities: design and implementation of smart home digital communication system,” *Indones. J. Electr. Eng. Comput. Sci.*, 2021, doi: 10.11591/ijeecs.v21.i1.pp271-277.

[4] W. A. Jabbar, T. K. Kian, R. M. Ramli, S. N. Zubir, N. S. M. Zamrizaman, M. Balfaqih, V. Shepelev, and S. Alharbi, "Design and Fabrication of Smart Home with Internet of Things Enabled Automation System," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2942846.

[5] R. K. Kodali, V. Jain, S. Bose, and L. Boppana, "IoT based smart security and home automation system," 2017. doi: 10.1109/CCAA.2016.7813916.

[6] S. Pirbhulal, H. Zhang, M. E. E. Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y. T. Zhang, and W. Wu, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors (Switzerland)*, 2017, doi: 10.3390/s17010069.

CHAPTER 9

ESP8266 WIFI BOARD (MICROCONTROLLER) AND SENSORS

Ms. Akshaya M Ganorkar
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- akshayamganorkar@presidencyuniversity.in

An esp8266 is a WiFi MCU (Micro-controller Unit) with high integration that is used to create end-point IoT (Internet of Things) applications. It is referred to as a standalone wireless transceiver, which is utilised to provide internet connectivity to several embedded system applications. The ESP8266 Wi-Fi module was created by Espressif Systems to provide both TCP/IP functionality and Microcontroller access to any Wi-Fi network. It offers solutions to satisfy IoT industry needs for cost, power, productivity, and design [1]–[3]. The RF transmitter and receiver, analogue transmitter, amplifiers, filters, digital baseline, power supplies, external circuitry, and other required components are all incorporated into one Wi-Fi module. The microcontroller needs a series of AT (ATtention) instructions to connect with the ESP8266 Wi-Fi module. As a result, it is designed with AT commands software to enable Arduino Wi-Fi features, and it also enables loading other software to create custom applications on the module's memory and CPU. Based on the Tensilica Xtensa Diamond Standard 106 micro, this module's CPU runs at an efficient 80 MHz [4]–[6].

The graphic below displays the pin configuration/pin diagram for the ESP8266 Wi-Fi module. There are two ways the ESP8266-01 Wi-Fi module operates. As follows:

- Flash Mode: The module executes the software that is put onto it when the GPIO-0 and GPIO-1 pins are active high.
- UART Mode: The module operates in programming mode with the aid of either serial communication or an Arduino board when GPIO-0 is active low and GPIO-1 is active high.

Specifications for the ESP8266 Wi-Fi Module. Below are the specs or characteristics of the ESP8266 Wi-Fi module.

- It is a strong Wi-Fi module that is inexpensive and readily accessible in a small size.
- It operates at 80 MHz and is based on the L106 RISC 32-bit CPU core.
- It simply needs a 3.3 Volt power source.
- The 100 m Amp current usage.
- The Input/Output (I/O) voltage may go up to 3.6 Volts.
- It uses 100 mA of current.
- The maximum source current for input and output is 12 mA.
- The internal 32-bit low-power MCU operates at 80 MHz.
- Flash memory has a 513 kb size.
- It may be used as a station, an access point, or both.
- It permits deep sleep at less than 10 microamps.

ISBN 978-81-962236-0-1

It enables serial communication so that it may work with several development platforms, including Arduino. Either AT commands, the Arduino IDE, or Lua scripts are used to programme it. It is a 2.4 GHz Wi-Fi module that supports open networks, WPA/WPA2, and WEP authentication. It makes use of the I2C (Inter-Integrated Circuit) and SPI serial communication protocols (Serial Peripheral Interface). It offers analogue to digital conversion with 10 bits. PWM is a kind of modulation (Pulse Width Modulation). UART may be enabled on GPIO2 for transmission-only purposes and on specific pins. It is an IEEE 802.11 b/g/n Wi-Fi module with an inbuilt TR switch, a power amplifier, a balun, and matching networks.

- The instruction RAM size is 32 KB.
- The instruction cache RAM capacity is 32 KB.
- User-data RAM size is 80 KB.
- ETS systems-data RAM is 16 KB in size.

A door or window security system may be installed with the MC-38 MC-38 Wired Door Window Sensor Magnetic Switch Home Alarm System. When they have moved apart from one another, it generates a signal that may be supplied to the microcontroller to carry out the required operation.

The MC-38 sensor is the optimum sensor for the application since it has the following attribute.

- Simple installation; Effective concealing
- Magnetic sensor alarm, which uses a built-in magnet to operate the circuit switch.
- Sound the alarm when someone enters your premises. May be utilised in residences, hotels, workplaces, etc.
- Excellent for both domestic and professional usage.
- Integrated into the door or window frame.
- Specifications
- A 100 mA rated current.
- Voltage rating: 200 VDC.
- Working range: more than 15 mm, less than 25 mm.
- Power rating: 3 W.
- Size: 28 x 15 x 0.9 cm.

All living things that have a body temperature higher than 0 degrees Celsius release heat through their bodies in the form of infrared radiation, also known as thermal radiation. To human sight, this Radiated energy is invisible. Using a PIR sensor that is intended for this purpose, these Signals may be detected. The term passive about a passive infrared (PIR) sensor means that it does not produce or emit any energy for detection.

- Features
- Sensing Range: 3M to 5M
- Adjustable delay
- High level output, H=3.3V, L=0V; Power supply DC:3.3V–15V
- 20 uA for quiescent current

ISBN 978-81-962236-0-1 March 2023

Working

Pyroelectric sensors, the main component of PIRs, can detect amounts of infrared radiation. The circular metal container with the rectangular crystal in the middle is shown in the PIR element. Each item releases a little amount of low-level radiation, with hotter things producing more radiation. The sensor is divided into two slots that are connected in such a way that their effects cancel one another out. The output will fluctuate high or low if one part detects more or less IR radiation than the other. A comparator circuit is used to compare the input signals from the PIR element's two terminals after they have been amplified by an amplifier circuit. A lens covers the PIR element to extend the operating range.

Bibliography

[1] Z. Wu, K. Qiu, and J. Zhang, "A smart microcontroller architecture for the internet of things," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20071821.

[2] T. Nguyen, S. Z. Andreasen, A. Wolff, and D. D. Bang, "From lab on a chip to point of care devices: The role of open source microcontrollers," *Micromachines*. 2018. doi: 10.3390/mi9080403.

[3] A. Latif, H. A. Widodo, R. Rahim, and K. Kunal, "Implementation of line follower robot based microcontroller atmega32a," *J. Robot. Control*, 2020, doi: 10.18196/jrc.1316.

[4] H. Kusumah and R. A. Pradana, "Penerapan Trainer Interfacing Mikrokontroler Dan Internet Of Things Berbasis Esp32 Pada Mata Kuliah Interfacing," *J. CERITA*, 2019, doi: 10.33050/cerita.v5i2.237.

[5] Y. M. Yusof, A. Ayob, M. H. Md Saad, H. M. Affandi, and A. Hussain, "Need analysis for the development of a microcontroller instructional module programming literacy," *Bull. Electr. Eng. Informatics*, 2020, doi: 10.11591/eei.v9i2.2077.

[6] W. A. Salah and B. A. Zneid, "Evolution of microcontroller-based remote monitoring system applications," *Int. J. Electr. Comput. Eng.*, 2019, doi: 10.11591/ijece.v9i4.pp2354-2364.

CHAPTER 10

C++ (ARDUINO PROGRAMMING)

Ms. Srilakshmi K. H.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- srilakshmi@presidencyuniversity.in

C++ is used to create the Real Time Operating System for microcontrollers used in Internet of Things devices. Many consider the object-oriented programming language C++ to be the finest one for developing complicated applications. 1. The general-purpose, case-sensitive, statically typed, compiled, free-form programming language C++ enables procedural, object-oriented, and generic programming. C/C++ is the foundation of the IDE used to programme the ESP8266 - Arduino IDE [1]–[3].

Internet Technologies

The various web technologies that were utilised to create the web dashboard are described in this section.

Language for Hyper Text Markup (HTML)

The code that creates a webpage is called HTML. It is a hypertext document, which means that it may connect to other documents or files. The term "markup" describes data in an electronic document that is not often shown to the user (like the HTML code of a website). Using HTML, every website is created. Tags are used by HTML to show material [4]–[6].

The webpage is shown by the browser once it understands the hypertext.

This document is designated as HTML5 by the DOCTY PEhtml > declaration. The root element of an HTML page is the HTML element. The language of the document is specified via the lang property. The document's metadata is included in the "meta" element. The character set used in the document is specified by the charset property. A title for the document is specified by the title > element. The content of the viewable page is included in the body element. A big heading is defined by the h1 element. The paragraph is defined by the p element. The document type declaration!DOCTY PEhtml > must be at the top of every HTML document. Beginning with HTML and ending with /HTML, an HTML document is itself. Between "body" and "/body," in an HTML page, is the viewable portion.

- CS1 Style Sheets (CSS)
- The website is styled and designed using CSS. CSS is used for things like adding colours, font styles, font sizes, etc.
- Outside CSS
- If there is an external CSS, the HTML may connect to the external.css file.
- using the HTML tag linkrel = "stylesheet"href = "style.css" >

ISBN 978-81-962236-0-1 March 2023

The most popular and practical way to include CSS in a document is this one. Multiple web pages may be linked together so that they are all styled using the same CSS style sheet. Figure 3.2: Description of the website rendered using external CSS. An HTML button element gains functionality thanks to this code.

Button with ID "btn"

Click the "Me" button. When the HTML "button" element is clicked, a pop-up warning is intended to appear. JavaScript may also be written inside by connecting to an external.js file or using the style HTML element. In this project, JavaScript also has a significant function since it facilitates communication between the ESP8266 and the application level.

XML and JavaScript are asynchronous (AJAX)

To connect with the server, the client utilises HTTP. POST/GET requests may be sent asynchronously to the server using the HTTP AJAX protocol. Asynchronous implies that rather than updating the whole website, just the portion of it that is handling the GET/POST operation does so. The XMLHTTPRequest(XHR) object is used to send HTTP requests using JavaScript.

The XHR object's use is shown in the excerpt that follows xhr.open creates a connection to the provided URL and sends an HTTP GET request there. var xhr = new XMLHttpRequest () ; xhr. open ("GET", "http: / / url / example. t x t ") ; xhr. send (); The server may answer a request with a basic text response, media, or a file.

Network

TCP/IP and the whole 802.11 b/g/n WLAN MAC protocol are implemented by ESP8266. It enables the Distributed Control Function's Basic Service Set (BSS) STA and SoftAP activities (DCF).

MAC

The ESP8266EX Wi-Fi MAC automatically performs the following low-level protocol operations:

virtual Wi-Fi interfaces

- Station mode, SoftAP mode, and promiscuous mode of the infrastructure BSS
- Immediate Block ACK, Clear To Send (CTS), and Request To Send (RTS)

Defragmentation

- TKIP (MIC, RC4), WEP (RC4), CCMP (CBC-MAC, counter mode), and CRC
- Automatic beacon surveillance (hardware TSF)
- Support for Bluetooth coexistence with dual and single antennas and possible simultaneous reception (Wi-Fi/Bluetooth) functionality
- Other WiFi capabilities
- Station/SoftAP/SoftAP+Station Wi-Fi Mode
- WPA/WPA2 security is two.
- Use of WEP/TKIP/AES encryption

ISBN 978-81-962236-0-1 March 2023

- IPv4, TCP/UDP/HTTP, and Network Protocols 802.11b power: +20 dBm
- 802.11 g: +17 dBm
- 802.11 n: +14 dBm
- 6. Rx 802.11 b sensitivity: -91 dbm (11 Mbps)
- 802.11 g: –75 dbm (54 Mbps) (54 Mbps)
- 802.11 n: –72 dbm (MCS 7) (MCS 7)

TCP/IP protocol firmware is implemented by the ESP8266 application layer. The project's application layer protocols include HTTP.

HTTP

An application-layer protocol called Hypertext Transfer Protocol (HTTP) is used to send hypermedia content like HTML. Although it was created for web browser and web server communication, there are other uses for it as well. In the traditional client-server architecture used by HTTP, a client first establishes a connection, sends a request, and then waits for a response. Because HTTP is a stateless protocol, the server does not save any information (state) between requests. This project uses HTTP message headers to request certain server actions (here ESP8266). Headers in HTTP messages are used to define resources, server or client behaviour, or both.

In this project, sending data to the server mostly uses the HTTP POST technique. The POST method changes the server side (such as turning an LED on/off) by sending data to the server.

Web-Sockets

An ongoing connection between a client and server is called a Web-Socket. Through a single TCP/IP socket connection, Web-Sockets provide a bidirectional, full-duplex communication channel that runs via HTTP. The Web-Socket protocol's primary function is to make it easier for clients and servers to exchange messages. The Web-Socket connection that was established lasts as long as any of the involved parties decide to stop utilising it. The second party won't be able to communicate once the first party terminates the connection since the connection is immediately severed at its front. For Web-Socket to establish the connection, HTTP must be supported. Speaking of its usefulness, it forms the backbone of contemporary web application development when it comes to synchronised traffic and flawless data streaming. Updates are transmitted instantly using WebSockets as opposed to HTTP, where you must continuously request them. While removing HTTP's latency issues, Web-Sockets maintain a single, permanent connection. For real-time updates, Web Socket is used. Instead, there would be a delay in the updating of sensor information if HTTP polling techniques were used with AJAX.

Bibliography

[1] C. C. Lu, J. C. Hong, F. F. Chen, and S. Y. Ma, “Elementary school students learn arduino programming to assemble sensory-controlled works,” *Int. J. Inf. Educ. Technol.*, 2020, doi: 10.18178/ijiet.2020.10.4.1374.

[2] N. A. Pramono, O. Ghaisyani, B. A. Purwandani, and F. I. Sofyan, “Application of Arduino

Programming Using ML8511 UV Sensor Hookup Guide to Learning the Effect of Ultraviolet's Level," *J. Disruptive Learn. Innov.*, 2020, doi: 10.17977/um072v2i12020p37-44.

[3] E. Pratidhina, D. Rosana, and H. Kuswanto, "Designing Physics Hands-On Experiment for Distance Learning Using Arduino and Block-Based Programing Language," *TEM J.*, 2022, doi: 10.18421/TEM111-47.

[4] R. G. Govender and D. W. Govender, "A Physical Computing Approach to the Introduction of Computer Programming among a Group of Pre-service Teachers," *African J. Res. Math. Sci. Technol. Educ.*, 2021, doi: 10.1080/18117295.2021.1924440.

[5] S. Hassan, M. Z. I. Jumari, M. A. A. Sahari, M. A. M. Bahtiar, M. H. Jaafar, M. A. M. Nadir, M. S. M. Zakaria, M. S. Yusof, M. Ismon, H. Zakaria, M. A. Azmi, N. M. Yusof, and M. S. Ikhsan, "A study of sensor signal danger detector system using arduino programming method," 2021. doi: 10.1063/5.0044356.

[6] G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, and N. Weldin, "Taking Arduino to the Internet of Things: The ASIP programming model," *Comput. Commun.*, 2016, doi: 10.1016/j.comcom.2016.03.016.

CHAPTER 11

FILE SYSTEM AND MANAGEMENT

Ms. Srilakshmi K. H.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- srilakshmi@presidencyuniversity.in

Even if the file system and the programme are both stored on the exact flash chip, programming a new sketch won't change the contents of the file system. This makes it possible to save sketch data, configuration settings, or content for Web servers via the file system. The SPIFFS file system is another name for this. The original file system, SPIFFS, is perfect for programmes with limited RAM and storage that use lots of little files, care about static and dynamic wear levelling, but don't need complete directory support. The flash's filesystem overhead is also quite low [1]–[3].

The ESP8266 SPIFFS implementation has to take into account the chip's limitations, namely its little RAM. Due to its reduced system requirements, SPIFFS was chosen, however, this came at the expense of various limits and simplifications. SPIFFS only keeps a "flat" list of files; it does not support folders. The functions that deal with directory listing, such as opener ("/website"), essentially only filter the file names and preserve the ones that start with the required prefix (/website/), in contrast to conventional file systems where the slash character "/" is not permitted in file names. The maximum length for file names is similarly 32 characters [4]–[6].

- The ESP8266 has two filesystems for using the onboard flash: LittleFS and SPIFFS.
- LittleFS.h little fail-safe files system (LittleFS) was created to get over SPIFFS file system's restrictions.
- Benefits of LittleFS
- Littlefs is built to withstand sporadic power outages and has power loss resilience. The filesystem will revert to the last known good state if power is lost, and all file operations have strong copy-on-write guarantees.
- Wear levelling across dynamic blocks is provided by littlefs, which was created with flash in mind. Littlefs can also recognise faulty blocks and get past them.

Littlefs is designed to operate with a limited amount of memory and is based on bounded RAM/ROM. Because RAM utilisation is absolutely constrained, it does not alter as the filesystem expands. The filesystem only supports customizable buffers that may be specified statically, and there is no unlimited recursion.

- Start the file system using SPIFFS.begin().
- littleFS.begin() - Launch the littleFS file system
- ArduinoJson.h
- A library for JSON data serialisation and de-serialization. It's used to transmit sensor data to the client.
- illustrative serialisation code
- On an ESP-8266, this straightforward software builds a Websocket client and server.

ISBN 978-81-962236-0-1 March 2023

Operation of the Web Dashboard and the Home Automation and Security System.Working on the Home Automation and Security System and Web Dashboard in Chapter

Config.Json

As stated in section 3.4.2, the ESP8266 uses the supplied ssid and password to attempt to connect to the WiFi network using the following line of code: WiFi.begin (ssid, password). There are two ways to provide it with the password and ssid. a) By incorporating it directly into the main code.

- Placing it in a 'config'-named json file.

It would be necessary to load the code each time the credentials were updated if it were hard coded into the main programmer. There are just a limited amount of write cycles available for the ESP8266, making this very impractical. By storing the credentials in a json file, this issue may be solved. In this way, when the ESP8266 boots up or restarts, it opens the configuration file in read-only mode, reads the credentials, and then uses those credentials to connect to the network.

System Initialization

When a computer starts up or restarts, the following occurs:

- The void setup () function receives control. In this function, ESP loads libraries and file systems in addition to setting the pin modes.
- It calls the LittleFS.begin() function of the LittleFS library to mount the LittleFS file system. If the filesystem cannot be mounted, the setup procedure is terminated and an error is returned. Afterwards, the board would need to be restarted.
- If the file system is successfully mounted, the attempt Connection () function is finally called. This action gives that function control.

Starting the access point and connecting to the network

- The loadConfig() method is used to load the credentials within the attempt connection () procedure.
- Using the LittleFS file system, open the config.json file in read-only mode.
- Return false if the file is not accessible.
- If the file is accessible, go to step c, where you'll read the file and input the SSID and password into the appropriate variables. Get back true.
- : Use the SSID and password that the loadConfig function has established to connect to the network.
- If a network with those credentials is located, Step A connects to that network. Now an ESP8266 server. We may access the saved sites on it.
- The beginAccessPoint() function is called and the board begins as an access point if no network is identified. Here, we may sign in and enter our WiFi password.\

Bibliography

[1] J. Chen, C. Zhang, Y. Yan, and Y. Liu, “FileWallet: A File Management System Based on IPFS and Hyperledger Fabric,” *C. - Comput. Model. Eng. Sci.*, 2022, doi:

10.32604/cmes.2022.017516.

[2] O. Eck and D. Schaefer, “A semantic file system for integrated product data management,” *Adv. Eng. Informatics*, 2011, doi: 10.1016/j.aei.2010.08.005.

[3] H. V. Gamido, M. V. Gamido, and A. M. Sison, “Developing a secured image file management system using modified AES,” *Bull. Electr. Eng. Informatics*, 2019, doi: 10.11591/eei.v8i4.1317.

[4] K. A. Kovalchik, S. Colborne, S. E. Spencer, P. H. Sorensen, D. D. Y. Chen, G. B. Morin, and C. S. Hughes, “RawTools: Rapid and Dynamic Interrogation of Orbitrap Data Files for Mass Spectrometer System Management,” *J. Proteome Res.*, 2019, doi: 10.1021/acs.jproteome.8b00721.

[5] S. R. Mashwani and S. Khusro, “360° semantic file system: Augmented directory navigation for nonhierarchical retrieval of files,” *IEEE Access*, 2019, doi: 10.1109/ACCESS.2018.2890165.

[6] G. Albacite, D. R. Macua, A. J. Diolata, and N. Sobejana, “Android-based File Management System,” *SSRN Electron. J.*, 2021, doi: 10.2139/ssrn.3780535.

CHAPTER 12

PORT FORWARDING

Ms. Srilakshmi K. H.
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- srilakshmi@presidencyuniversity.in

The ecosystem of the project effectively creates home automation with a network of various sensors and microcontrollers that store, process, and serve the intended data on the customs website dashboard, home security that protects the home by continuously monitoring for intrusion and notifying the user if there is a security breach, and the custom dashboard website that displays the data and status of various sensors and aids in managing the entire ecosystem.

Port forwarding,

Port forwarding should be utilised if the user wishes to use the home automation and security system remotely but is not connected to the home Wi-Fi to which it is linked. By associating a router's public, wide-area network (WAN), internet protocol (IP) address with a private, local area network (LAN), IP address for a device on that private network, port forwarding enables computers in private networks to connect with other public or private computers or services over the internet. The user may connect to the system by using a public IP that has been configured by the designers after port forwarding [1]–[4].

Scaling As previously mentioned, the home automation system and custom dashboard website are designed to be personalised and made to be scalable. A wide range of sensors, functionalities, and features can be further added by minor changes to the lines of codes to upscale or downscale the system to better suit user needs on home or industrial needs.

Data encryption uses cyber security to convert plaintext (unencrypted) data into cypher text (encrypted). With the use of an encryption key and a decryption key, users may access encrypted data. It may be included as an extra feature to secure the ecosystem from hacking, to fight against brute force and cyberattacks, including malware and ransomware, and to safeguard privacy and autonomy. The hashing algorithm and other encryption methods may be used to encrypt data [5]–[7].

Data encryption is a technique for ensuring the secrecy of data by encoding it into ciphertext, which can only be decoded using a special decryption key that is either produced at the moment of encryption or previously. To make sure that keys are only given to or used by authorised users, data encryption is often used in combination with authentication services during data storage and transfer.

The need for security is greater than ever since data is now easier to obtain and more appealing to attackers. In addition, many firms must comply with data protection regulations, many of which specifically calls for the usage of encryption. Encryption contributes to data integrity in addition to the obvious advantages of improved security, privacy protection, and preventing illegal access.

ISBN 978-81-962236-0-1 March 2023

In addition to guarding against unauthorised change, encryption may be used to confirm the legitimacy and source of data.

Encryption: Symmetric vs. Asymmetric

Depending on how and by whom data is meant to be accessed, several types of encryption are used.

Synchronous encryption (Private Encryption Key)

A single, private key is used for both encryption and decryption in symmetric encryption. It is quicker than the encryption process and is most effective when employed by one person or in closed settings. The transfer of the key is necessary when using symmetric techniques with numerous users in complex platforms, such as across a network, and thus presents a risk of theft. AES is the most widely used kind of symmetric encryption.

Asymmetric Cryptography (Public Encryption Key)

Asymmetric encryption employs paired, mathematically linked public and private keys that can only be used in conjunction. Data can be encrypted with either key, but it can only be unlocked with the matched key. Multiple users and open networks, such as the Internet, employ asymmetric encryption because the public key may be freely exchanged without running the danger of information theft. ElGamal, RSA, DSA, and PKCS are the most popular asymmetric encryption algorithms. Depending on the use case, there are several secure encryption algorithms to select from, but the most popular ones are:

Triple DES (3DES or TDES) encrypts, decrypts, and re-encrypts data three times to provide a greater key length than the obsolete DES algorithm. With increased security, it may be operated with one key, two keys, or three separate keys. Since 3DES employs a block cypher, it is susceptible to attacks like block collision.

One of the first public-key methods is RSA, which employs asymmetric one-way encryption. Due to its lengthy key length, RSA is well-liked and commonly utilised online. It is used by browsers to establish secure connections across insecure networks and is a component of numerous security protocols, including SSH, OpenPGP, S/MIME, and SSL/TLS.

One of the quickest algorithms, Twofish, is available in key sizes of 128, 196, and 256 bits for greater security. VeraCrypt, PeaZip, KeePass, and the OpenPGP standard are among the greatest examples of free applications that utilise it. Elliptic Curve Cryptography (ECC) is a development over RSA that offers improved security with a lot lower key lengths. The SSL/TLS protocol makes use of the asymmetrical technique ECC.

The Advanced Encryption Standard (AES) has been adopted as the encryption standard by the US government. AES is a block cypher technique using symmetric keys. It uses an increasing number of rounds of encryption and comes in capacities of 128, 192, and 256 bits. It was designed for simple hardware and software implementation.

ISBN 978-81-962236-0-1 March 2023

A symmetric cypher with a key length that ranges from 32 to 448 bits is called blowfish. The key length that is chosen will affect how well this method performs. Since Blowfish is a block cypher, data is encrypted in set blocks of 64 bits each.

Format Preserving Encryption (FPE) is a kind of encryption that also accomplishes content anonymization. It keeps the data's current format while encrypting it. For instance, if a customer ID has two letters and ten numbers, the resultant unencrypted form will consist of the same quantity and kind of characters but will change them to other characters to safeguard the original data.

Standards for Data Encryption

Some guidelines control how data encryption methods are used in businesses. Here are two crucial guidelines. According to the US Federal Information Security Management Act, the FIPS standard was created (FISMA). They are designed with the US federal government in mind, and many US institutions and agencies need FIPS-level encryption. In the private sector, many people have voluntarily accepted FIPS as a reliable standard for the encryption of sensitive data.

Bibliography

[1] S. S. H. Hajjaj and K. S. M. Sahari, "Establishing remote networks for ROS applications via Port Forwarding: A detailed tutorial," *Int. J. Adv. Robot. Syst.*, 2017, doi: 10.1177/1729881417703355.

[2] M. S. Suprayogi and P. T. Pungkasanti, "Pemetaan Subdomain Pada Cloud Server Universitas Semarang Menggunakan Metode Port Forwarding dan Reverse Proxy," *KINETIK*, 2017, doi: 10.22219/kinetik.v2i1.133.

[3] N. Verma, M. Kashyap, and A. Jha, "Extending Port Forwarding Concept to IOT," 2018. doi: 10.1109/ICACCCN.2018.8748430.

[4] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, "Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS," *Techno.Com*, 2021, doi: 10.33633/tc.v20i3.4615.

[5] R. P. Pratama, "Remote PC Wake-On Design Manufacture in Mujahidin Mosque at Candi Mendut," *Motiv. J. Mech. Electr. Ind. Eng.*, 2021, doi: 10.46574/motivection.v3i3.97.

[6] R. K. Ansah, K. Obiri-Yeboah, and G. Akipelu, "Improving the freight transport of a developing economy: a case of Boankra inland port," *J. Shipp. Trade*, 2020, doi: 10.1186/s41072-020-00065-z.

[7] G. Chinnadurai and H. Ranganathan, "Balancing and control of dual wheel swarm robots by using sensors and port forwarding router," 2017. doi: 10.1109/AEEICB.2017.7972371.

CHAPTER 13

INFORMATION TECHNOLOGY SECURITY EVALUATION COMMON CRITERIA (CC)

Mrs. Renuka Bhagwat
Assistant Professor, Department of Electronics and Communication Engineering,
Presidency University, Bangalore, India
Email Id- renuka@presidencyuniversity.in

CC is a collection of worldwide criteria for confirming that product security promises hold up during testing and is not an encryption standard. Initially, outside of CC's purview, encryption is now gradually being covered by the security guidelines established for the project. To enable vendor-neutral, third-party supervision of security solutions, CC criteria were developed. Vendors voluntarily submit their products for assessment, and either the whole product or specific functions are looked at. When a product is assessed, its attributes are subjected to up to seven levels of scrutiny and contrasted with a predetermined set of criteria based on the kind of product [1]–[3].

Data at Rest vs. Data in Transit Encryption

Data must always be safeguarded since it is important whether it is being sent between users or stored on a server. The condition of the data will determine how that protection is implemented.

Transit Data Encryption

When data is travelling between devices across public networks, the Internet, or from a laptop to a thumb drive, it is said to be in transit. Due to the need for previous decryption and the inherent weaknesses of the transfer technique itself, data is more vulnerable during transmission. End-to-end encryption, which protects data privacy even if it is intercepted, encrypts data as it is being sent [3]–[5].

At-Rest Data Encryption

When data is stored on a storage device and is not being utilised or transported, it is said to be at rest. Due to access restrictions imposed by device security measures, data stored at rest is often less susceptible than while it is in transit, but it is not immune. It often includes more valuable information as well, making it a more alluring target for thieves.

By lengthening the time it takes to access information and extending the amount of time needed to detect data loss, ransomware attacks, remotely erased data, or changed credentials, encrypting data at rest reduces opportunities for data theft caused by lost or stolen devices, unintentional password sharing, or unintentional permission granting [5], [6].

In a nutshell, yes, encrypted data may be compromised. Attackers may breach data encryption systems in a variety of ways. Malware on endpoint devices: Many endpoint devices offer full disc encryption as one of their encryption options. Using malware, an attacker may get access to an endpoint device and use the device's keys to decrypt the data.

ISBN 978-81-962236-0-1 March 2023

Attackers often use brute force techniques to test a variety of keys in an attempt to crack an encryption system. The size of the key has a direct bearing on the likelihood of success. Because of this, 256-bit encryption keys are required by the majority of encryption standards. Some encryption methods, however, use weak cyphers that are susceptible to brute force assaults. Through the use of a process called cryptanalysis, attackers may access data by identifying a flaw in the encryption itself.

Side-channel attacks include searching for design flaws or defects that enable users to decrypt data or stop it from being encrypted without compromising the integrity of the encryption itself. Social engineering attacks: Using phishing or other social engineering techniques to deceive a privileged individual into revealing the key may be the simplest approach to stealing encrypted data. Insider threats: A serious hazard to encrypted data is the potential for high-ranking employees to turn against their employer and exploit their position to steal data. Inconsiderate users who disregard security guidelines are another source of insider danger. Even with these dangers, encryption is a reliable and robust security tool. However, given the likelihood that encryption will be broken, it must be seen as an additional layer of security and not the sole one that businesses utilize to safeguard their data.

Cloud-Based Encryption

A company might benefit from the cloud provider's encryption capabilities while storing data there. The majority of cloud service companies provide encryption as a service, either as part of their core offerings or as a stand-alone one. Many firms may fulfil their compliance duties in the cloud thanks to cloud-based encryption, which is practical.

It's important to know precisely what the cloud provider provides before implementing cloud-based encryption: How strong the encryption is and if it satisfies the demands of the organization. There are many approaches for key management, including client-controlled encryption keys and completely managed encryption keys.

How to configure end-to-end encryption so that data is secure throughout transit from the cloud to end users and back.

A key element of any cloud security plan is cloud encryption. However, businesses need to be mindful of these significant issues: End-users may find cloud encryption challenging, particularly when end-to-end encryption is complete.

Integrating cloud encryption with systems operating on-premises or on endpoint devices may be challenging. Because cloud encryption requires a lot of computing power, consumption must be monitored. The cost of the cloud may potentially be significant, depending on the pricing scheme. Care must be taken while managing keys since improper key security render encryption worthless and render data unusable if encryption keys are lost.

Key Characteristics of Data Encryption Products

Solutions that allow an organisation to adopt encryption broadly are known as data encryption solutions. Advanced encryption algorithms are included, as well as management tools for

deploying encryption, managing keys and passwords, establishing access controls, and keeping track of how encryption is used across the company.

Data encryption programmes must be user-friendly or, even better, entirely transparent so that no human interaction is required for the encryption of sensitive data. Additionally, they must be very scalable to handle increasing data quantities and swift to assure little to no influence on worker productivity.

Strong encryption standards: AES, which uses a 256-bit key, is now the industry standard for encryption. Data encryption at rest refers to data stored at rest on file servers, databases, staff workstations, and cloud storage. To encrypt sensitive data, the solution must be able to access all of these data storage places. Data encryption in transit - The solution should be able to use transport layer security (TLS), an encrypted protocol that assures message authenticity and prevents eavesdropping, to encrypt data transfers.

Granular controls: the solution should allow the organization's sensitive data to be encrypted just when it is necessary, rather than requiring encryption of all data repositories. It may, for instance, permit the encryption of certain file types, programmes, storage devices, or directories. Key management is a crucial aspect of managing encryption. The solution should make it simple to create encryption keys, provide them to the owners of the data, back up those keys, and delete them when access is denied. Policies must be automatically enforced, and solutions must enable organizations to set encryption policies. For instance, actions like emailing or storing a file in portable storage may be prohibited until the employee encrypts the information. Always-on encryption - Many systems provide for the encryption of important information, ensuring that it is maintained everywhere the files travel, even whether they are copied, emailed, or changed.

Types of Data Encryption Trends

Here are a few themes that are probably going to influence how data encryption develops in the future:

Use Your Encryption

A BYOE security architecture for cloud computing enables users of cloud services to control their encryption keys and encryption software. Another name for it is "Bring Your Own Key" (BYOK). Customers may instal virtualized instances of their encryption software alongside cloud-hosted business apps using BYOE.

Cryptography as a Service (CaaS)

Pay-per-use encryption is a service provided by cloud providers under the EaaS subscription model. In addition to addressing regulatory issues, this method gives clients some control over managing their encryption for the protection of data in multi-tenant setups. These services often provide database encryption, file encryption, or full disc encryption (FDE).

Encryption for Cloud Storage

ISBN 978-81-962236-0-1 March 2023

A service in which cloud storage providers encrypt all data before it is stored in the cloud. On-premises encryption is comparable to this, but there are several key distinctions. To match the degree of secrecy of their self-managed encrypted data, cloud clients should take an effort to learn the provider's rules and practises around encryption and key management.

Encryption from end to end (E2EE)

E2EE makes a guarantee that an attacker who spies on a channel of communication cannot view the data sent between them. Because attackers may access material both before and just after it is encrypted by the client and decoded by the server, using Transport Layer Security (TLS) to establish an encrypted channel between web clients and web servers does not always ensure E2EE.

Field-level security

The ability to encrypt data in certain fields on a web page, such as credit card numbers, social security numbers, bank account numbers, and health information, is known as field-level encryption.

Encryption over a sequential link

Data is encrypted as it leaves a host, decrypted on the next network connection (which might be a host or a relay point), and then encrypted once again before being sent to the following link. The data is encrypted at each connection using a new key or method, and the process is repeated until the data reaches the recipient.

In-Network Encryption

Utilizing cryptographic services at the network forwarding layer is this technique (level 3 in the OSI model). This is situated below the application layer and above the data link layer. Internet Protocol security is used to accomplish Level 3 encryption (IPsec). It provides a foundation for private communications in IP networks when combined with several IETF standards.

Bibliography

[1] Common Criteria, “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model,” *Common Criteria*, 2017.

[2] Ccra, “Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components,” *Security*, 2012.

[3] C. Criteria, “Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components,” *Security*, 2017.

[4] P. J. Graydon and T. P. Kelly, “Using argumentation to evaluate software assurance standards,” *Inf. Softw. Technol.*, 2013, doi: 10.1016/j.infsof.2013.02.008.

[5] D. Simić-Draws, S. Neumann, A. Kahlert, P. Richter, R. Grimm, M. Volkamer, and A. Roßnagel, “Holistic and law compatible IT security evaluation: Integration of common criteria, ISO 27001/IT-grundschutz and KORA,” *Int. J. Inf. Secur. Priv.*, 2013, doi: 10.4018/jisp.2013070102.

[6] A. Bialas, "Common criteria related security design patterns-validation on the intelligent sensor example designed for mine environment," *Sensors*, 2010, doi: 10.3390/s100504456.

ISBN 978-81-962236-0-1 March 2023

Publisher
M/s CIIR Research Publications
B-17, Sector-6, Noida,
Uttar Pradesh, India.
201301
Email: info@ciir.in

March 2023
ISBN 978-81-962236-0-1