

A Review Of Iot-Based Home Security Solutions: Focusing On Arduino Applications

Hiranmaye Sarpana Chandu
Independent Researcher

Abstract- The rapid proliferation of Internet-enabled devices largely bestowed state-of-the-art transformation on home security solutions, especially with regard to the integration of IoT. This study discusses some IoT home security systems, with emphasis on applications using Arduino, and indicates the necessity of leveraging the existing infrastructures of IoT while designing affordable and effective solutions in security. The present study encompasses many aspects, including Wi-Fi, Bluetooth, Zigbee, MQTT, CoAP, HTTP, and various sensors on temperature, smoke, LPG, and IR, among others and also discusses about the advantages of using arduino in home security systems. Some Arduino-based systems also explore various IoT-based home security solutions, including intrusion detection, surveillance, access control, and smart alarm systems. This study will further elaborate on how home security systems have evolved, the benefits derived by using Arduino, and future research directions, focusing on an incorporation of AI and ML to develop these solutions.

Keywords- IoT, Arduino, home security, wireless communication, intrusion detection, surveillance, access control, smart alarms.

I. INTRODUCTION

Recent years have seen an explosion in the number of Internet-enabled gadgets. Everything that allows these internet-connected devices to communicate and share data is part of the IoT infrastructure. For this reason, including such an existing infrastructure into a design of a smart home security system is advantageous [1].

Although there has always been a need for home security, there has recently been an even greater demand to have impenetrable security for family members and possessions due to a sharp increase in small-time crimes like theft and robbery [2]. The IoT has a profoundly positive effect on human societies. The term "internet of things" (IoT) might imply different things to different individuals, but from any angle, it always refers to the network that allows various physical objects to exchange data with one another and establish connections with one another over the internet. From just monitoring various areas of the house to actively controlling them, the concept of the smarter life IoT has the ability and promise to soon have several applications in smart home security, which is promising. Integrating IoT with home security has allowed for global home monitoring[3].

The four sensors used by an IoT and Arduino-based home security system are temperature, smoke, LPG, and infrared sensing. Once collected, the data is sent to the Arduino, which has a built-in signal converter. The ESP8266 Wi-Fi module receives data transmissions from the Arduino. The ESP8266 is a communication chip that allows microcontrollers to establish TCP/IP connections, communicate over a wireless

network, and receive data. Sending data detected by these sensors to the IOT[4].

There is a programmable board called Arduino that is open-source. A single board computer that is both powerful and simple to operate, it has become rather popular in both the hobby and professional markets. Both a microcontroller and an Integrated Development Environment (IDE) are required to build and execute the programs, which are called sketches on the Arduino platform. Inputs may be anything from a sensor's light to a user's touch or even a tweet, and Arduino boards can transform this data into an output like a motor turning on, an LED lighting up, or even a web post [5].

In modern times, integration of technology into residential security systems has become imperative. The Arduino-based home surveillance system presented in this document offers a sophisticated yet cost-effective solution for monitoring gas, water, and fire hazards. By employing Arduino microcontrollers in conjunction with a variety of sensors, this system is capable of detecting potential threats and issuing timely alerts to homeowners via their mobile devices. The project calls for an Arduino, a motion detector, a buzzer, an LCD screen, and some basic code. As soon as it senses motion within its detection range, the alarm will go off. Additionally, it will transmit the signal to the Arduino, which will do the necessary processing, activate the alarm, and show a detection message on the screen [6].

1.1 Research contribution of work

This study comprehensively covers IoT-based home security solutions, with a special focus on Arduino applications, hence contributing significantly to the existing body of knowledge in the following key areas:

- This study presents reviews of some IoT-based home security systems, with emphasis on Arduino as the central platform. It talks about the integration of Arduino with IoT to provide information on how the integration of both technologies can be used to improve home security.
- This study also identifies and compares the most relevant wireless communication technologies (Wi-Fi, Bluetooth, ZigBee) and networking protocols (MQTT, CoAP, HTTP) for Arduino-based IoT security systems.
- The paper carries out a systematic review of the various IoT-based home security solutions based on Arduino, the paper provides a clear examination of how these solutions can be tailored toward effective home security, such as intrusion detection, surveillance, access control, and smart alarms.
- The study also identifies the trends and future research that have emerged in IoT-based home security. Specifically, it

highlights how higher-end technologies like AI and ML can be integrated in the near future to provide Arduino-based security solutions with extended capabilities.

1.2 Structure of the paper

The structure of the paper are as follows: Section I contains the introduction and the work contribution, and Section II contains overview of IOT-based home security, then Section III contains arduino in IOT home security systems and then Section IV provides types of IOT-based home security solutions using arduino and, At last Section V and VI provides previous studies done on home security based on IOT, and conclusion and future scope respectively.

I. OVERVIEW OF IOT-BASED HOME SECURITY

Audio, video, or images may all be sent or received via the internet. The notion of remotely connecting and tracking physical items (things) over the Internet is known as the IoT. The concept can be appropriately applied to our home to make it safer, more intelligent, and automated. The usage of automation systems in homes and buildings is growing these days. can provide more comfort—especially when used in private residences. Security is an important factor to consider when talking about home automation. When it comes to home automation, home security is paramount. There has been tremendous growth in home security in the previous few decades, and there will be much more growth in the years ahead [7].

1.1 Concept of IoT

The network of physically connected items that are capable of exchanging data and communicating with one another without the assistance of a person is called the IoT. IoT has been dubbed a "Infrastructure of Information Society" as it allows us to collect data from a variety of sources, such as people, animals, automobiles, and kitchen appliances. The IoT allows for the incorporation of previously inaccessible physical objects into digital networks by means of embedded software, sensors, and networking gear, as long as these objects can be assigned an IP address. The IoT differs from the Internet in that it allows everyday objects equipped with embedded circuits to interact and communicate with one other using the current Internet infrastructure, going beyond basic Internet access [1].

1.2 Evolution of Home Security Systems

These days, technology advances and changes quickly. Certain aspects of the system must continually change in order to stay relevant as modern technology advances. Home security and monitoring systems were formerly dependent on human management. However, recent technological advancements, particularly in the area of the IoT, have given these systems a new lease of life. The concept and its implementation may be investigated by grasping the fundamentals of IoT-based home security. Once this has occurred, the technological idea may be developed. Many home security systems that use Bluetooth, RFID, Android applications, and short message services (SMS) as the communication connection have been created [2]. All of them have various approaches to home security systems but serve the same purpose: to monitor the security and safety of households [8].

II. ARDUINO IN IOT HOME SECURITY SYSTEMS

In many cases, smart homes are far safer than traditional houses. Simple home security systems that use automation and the cloud to identify intruders, alert you to suspicious activities, and make it simpler to safeguard your house and people in it are quite basic to construct. It's easy to master the fundamentals of cloud computing and begin constructing your own projects for

a wide variety of interesting uses with the aid of Arduino devices [9].

2.1 Introduction to Arduino Platform

This open-source hardware and software platform called Arduino might be useful for programmers, industrial artists, professionals, and everyone else who wants to make interactive devices and apps that are made for an interactive development environment.

A wide variety of sensors and inputs may provide signals to an Arduino. Arduino allows users to manipulate their surroundings by manipulating various actuators such as light sources, motors, and more. The "Processing" open-source programming language and integrated development environment forms the basis of the Arduino development environment, which allows users to program the microcontroller on the Arduino board. The programming language used to write these programs is called Arduino's "Wiring" framework, and the microcontroller itself can be seen in figure 1 [10].

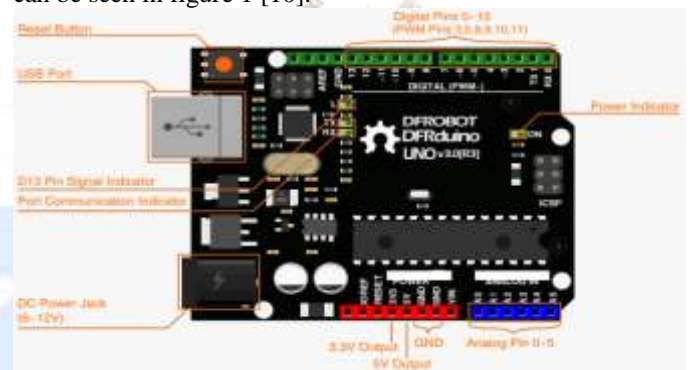


Figure. 1: Arduino platform

2.2 Advantages of Using Arduino for Home Security

Some benefits of using an Arduino Uno board are as follows [11]:

- It's user-friendly and straightforward. It is beginner-friendly since it is readily programmed.
- LED blinkers, robots, and many more projects are within the realm of possibility with Arduino Uno.
- Its several pins allow it to connect a wide variety of electrical components and increase its compatibility.
- As compared to other microcontroller boards, Arduino Uno boards are quite inexpensive.
- The extensive community of active Arduino users ensures that any support or assistance required for Arduino boards is readily accessible.

III. TYPES OF IOT-BASED HOME SECURITY SOLUTIONS USING ARDUINO

Home security is a must-have in today's world. There must be a body to ensure our safety and security in light of the fact that crime is on the rise. While everyone is aware that there are state-of-the-art security systems on the market, not everyone can afford them. Consequently, we want to develop practical electronic gadgets that can detect the motion of invaders and alert the user in order to provide a possible security solution [12]. Some solutions based on the IoT for security are as follows:

3.1 Intrusion Detection Systems

IDS are a powerful tool for protecting cybersecurity systems against potential intrusions. An increase in data generation is associated with an increase in the chance of various forms of intrusion attacks. In light of the rapid advancement of networking technologies and the growing count of cyber dangers, it has become essential to guarantee appropriate

cybersecurity. Cybersecurity is based on the idea that malicious actions and unauthorized access to computer networks may be detected and stopped. Internet IDS ability to monitor network traffic and identify security flaws is vital. Improving IDS' accuracy and efficacy via the use of ML algorithms to the field of networking cybersecurity is an exciting prospect. IDS models powered by ML can sift through mountains of network data in search of unusual patterns and adjust to new types of attacks with ease. By identifying previously unseen assaults and decreasing false positives, this method has the ability to strengthen the overall security posture.

3.2 Surveillance and Monitoring Systems

A common security tool for keeping an eye on the community and spotting criminal activity is closed-circuit television, or CCTV. Nevertheless, the capacity of CCTV systems to detect criminals is restricted. This is so that security staff may manually evaluate the video footage that CCTV systems normally merely capture. This may be an arduous and labour-intensive procedure that results in lost chances to locate and detain offenders. CCTV systems are made more capable by smart surveillance systems, which make use of cutting-edge technologies like computer vision, AI, and ML. Video footage may be automatically analysed by smart surveillance systems to spot suspicious activity or possible security threats. This may speed up the process of identifying criminals and enable security staff to concentrate on important areas and possible dangers.

Smart surveillance systems may be built using OpenCV, a popular open-source computer vision library. Among the many image and video processing tools and techniques provided by OpenCV are those for object identification, face recognition, and license plate recognition. These techniques may be used to automatically analyse video footage in order to spot suspicious activity or possible security threats. OpenCV, for instance, may be used to create intelligent security systems that can recognise cars that have been reported stolen or automatically identify persons carrying weapons[13].

3.3 Access Control Systems

A credential is a kind of proof that an access control system employs to provide access to an individual. The credential might be something that is carried, like a card or token, something that is known, like a personal identification number, or something that the authorised person has, such a fingerprint or iris (the colored portion of the eye). Access is either given or refused based on a degree of verification after the credential has been input, swiped, presented, or scanned. One door to hundreds of doors or alarms worldwide may be controlled by an access control system, which has many operating modes and scopes. A mechanically or electronically checked code is entered at a single door keypad, which is at the low end of the access control spectrum. The majority of access control systems work with card-based credentials, which may be scanned using an electronic reader or swiped. These solutions are applicable to thousands of doors and sensors linked via the company's computer network, not just a handful. Biometric authentication is used by the safest access control systems [14].

3.4 Smart Alarm Systems

Security is a crucial aspect to take into account while discussing home automation. Perhaps the most significant aspect of home automation is home security. Home security has come a long way in the previous several decades, and it's just going to get better from here on out. The old definition of a home security system was an alarm that would go off in case of a gas leak, fire or burglary; however, modern smart homes can do much more. Thus, our primary goal is to create a system that can notify the

owner and other people via their smartphones of an intruder break-in. Additionally, the owner will be able to remotely set the alarm to go off or on using simply his smartphone. Customers will be able to better secure their homes with this technology by simply putting the devices on doors or windows and monitoring their actions using smartphones [1].

IV. TECHNOLOGIES AND PROTOCOLS IN ARDUINO-BASED IOT SECURITY

The proliferation of advancements in several technical domains, including communication technologies, sensors, embedded systems, microelectronic circuits, and mobile operating systems, has led to an increase in the quantity of devices capable of connecting to the Internet. Nowadays, smart objects and gadgets account for the majority of Internet traffic [15]. The IoT is a global system of networked computing devices that can sense their environment, recognize items, and exchange information via predefined protocols. Applications for IoT are many and include smart buildings and cities, security, traffic, health, energy, disaster detection, agriculture, and industrial. Using various network interfaces and protocols, IoT devices with a wide range of application domains may establish a connection with the biggest network, the Internet[16]. Therefore, the IoT is a global system of interconnected physical items that can be sensed and interacted with at any time and from any location via the use of electronic devices. The general layout of such an IoT network is seen in Fig. 2.

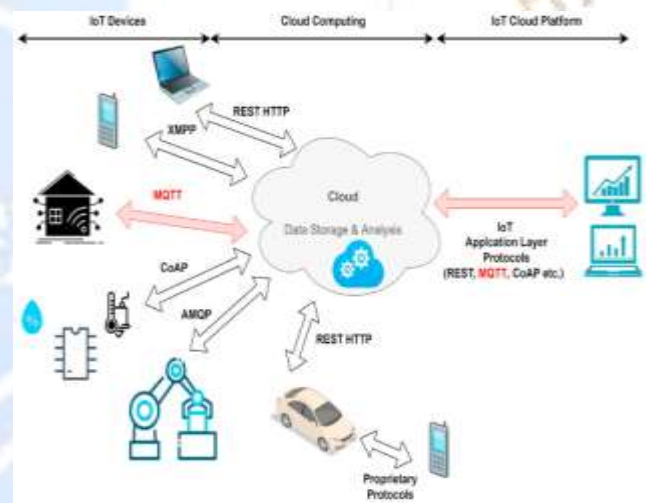


Figure. 2: General IoT system architecture.

4.1 Wireless Communication Technologies (Wi-Fi, Bluetooth, Zigbee)

There was a brief discussion of these three technologies. There was also discussion of the three technologies' aspects that are required to fully understand this research [17].

4.1.1 Wi-Fi

The IEEE 802.11 standard defines a WLAN. The maximum indoor and outdoor ranges for IEEE 802.11(b, g, n) are 32 and 95 meters, respectively, while the data transfer rates are 11 and 54 Mbps in low band mode [11]. When compared to 802.11a and 802.11g, the IEEE 802.11n standard uses twice as much radio spectrum. However, compared to 802.11b and g, IEEE 802.11a, c offers twice the range and data transfer speeds of up to Gbps. Low band Wi-Fi operates in the 2.4 GHz ISM band, and high band Wi-Fi operates in the 5 GHz range. Data rates of up to 54 Mbps are achievable in the ISM band with the use of overlapping 22 MHz channels modulated digitally using BPSK and QPSK. Two channels do not overlap if their channel numbers are five digits different. The maximum allowable EIRP for Wi-Fi is 20 dBm, or 100 mW.

4.1.2 Bluetooth

The IEEE 802.15.1 standard defines a proprietary open wireless technology for data transmission over short distances. It communicates via the ISM Band, which operates between 2400 and 2480 MHz, and has short wavelengths. WPANs are being embraced primarily as a replacement for cable technology. One of the radio protocols used by Bluetooth is FHSS, or frequency hopping spread spectrum. It uses all seventy-nine channels, with each channel operating at 1 MHz, as it fills the whole ISM band. The Bluetooth technology makes use of GFSK, EDR, $\pi/4$ -DQPSK, and 8 DPSK modulation schemes. This technology's transmit power determines the transmit distance. The maximum transmission distance for a Class 1 device with a 100-mW output power is 100 meters, and for a 25-mW device, it is 10 meters.

4.1.3 Zigbee

Home automation, healthcare, telecom services, and remote control are just a few of the many fields that have found use for this specification's low-cost, low-power digital radios. Just like Wi-Fi and Bluetooth, ZigBee uses the ISM radio band to communicate. Transfer speeds of 250 kilobits per second. The ZigBee standard (IEEE 802.15.4) specifies the physical and medium access control layers for low-rate wireless PANs and permits transmissions up to 10 meters. The 2.4 GHz spectrum is divided into sixteen non-overlapping channels, each with a width of 2 MHz, according to this standard. A maximum of sixteen ZigBee networks may therefore coexist in the same physical location and simultaneously. Support for frequency hopping in the "ZigBee Pro" Standard has been added to the most recent ZigBee version. In the event that one channel has an overload, a ZigBee PAN may switch to the other channel. The communication paradigm requires the allocation of work among several devices housed in different ZigBee nodes, which comprise a network.

4.2 Networking Protocols (MQTT, HTTP, CoAP)

There are several message protocols from which to choose depending on the different needs of the IoT system. Multiple communications protocols are essential to the IoT future, since no one protocol can handle all potential use cases. As a result, in order to identify the best match scenarios for IoT systems, it is vital to have a discussion about the generally recognised and upcoming messaging protocols. Three of them are covered in the section below [18]:

4.2.1 MQTT (Message Queuing Telemetry Transport Protocol)

MQTT is one of the most ancient methods of M2M communication. It was first introduced in 1999. It was developed by Arlen Nipper of Eurotech's Arcom Control Systems Ltd and Andy Stanford-Clark of IBM. For low-overhead M2M communications on unstable networks, this publish-subscribe messaging protocol is ideal. Published messages from one MQTT client to another may be subscribed to by other clients or stored for possible future subscriptions. Every message is sent to a recipient, sometimes known as an address in certain cases. Subscribers are able to follow numerous subjects and will get all published messages for each topic. Because MQTT is a binary protocol, modest message payloads up to 256 MB in size are often required, along with a fixed header of 2 bytes. The MQTT protocol uses TLS/SSL for security and TCP as a transport mechanism. Client and broker communication is thus connection-oriented. The three levels of QoS that MQTT offers for dependable message delivery are another really useful feature. The biggest networks of tiny devices that need monitoring or management from an Internet-based back-end server is best suited for MQTT. Neither device-

to-device communication nor multicast data delivery to several recipients are intended uses for it.

4.2.2 CoAP (Constrained Application Protocol)

A lightweight M2M protocol called CoAP was created by the IETF's CoRE Working Group. Both the publish/subscribe variation known as resource/observe and the request/response architecture are supported by CoAP. Whereas MQTT employs topics, CoAP utilises Universal Resource Identifiers (URI). A publisher publishes data to the URI, and a subscriber joins the queue to access the resources signalled by the URI. By using the URI, every subscriber to a publication may be alerted whenever the publisher adds new data. The length of message payloads and the 4-byte fixed header are the main components of the binary protocol known as CoAP; nevertheless, the web server or programming approach determines the maximum size. DTLS ensures security, and UDP is the transport protocol used by CoAP. And hence, clients and servers communicate using less reliable connectionless datagrams. To provide two distinct QoS tiers, nevertheless, it makes use of "confirmable" or "nonconfirmable" communications. Whereas, the receiver is required to respond to confirmable messages with an ACK packet, but not nonconfirmable ones. With the help of content negotiation, which is a feature of CoAP, clients and servers may develop autonomously, adding new representations of resources without impacting one another.

4.2.3 HTTP (Hyper Text Transport Protocol)

Originally created by Tim Berners-Lee, HTTP is mostly utilized as a web message system. Eventually, the IETF and the W3C worked together to improve it, and in 1997, it was released as a standard protocol for the first time. The RESTful Web architecture that is supported by HTTP is request/response. When compared to CoAP, HTTP makes use of URIs instead of topics. Data is sent and received between the server and the client using the URI. Since HTTP is text-based, web servers and programming techniques, and not the protocol itself, determine the size of message payloads and headers. When it comes to transport protocols, HTTP always utilises TCP and employs TLS/SSL for security. Consequently, connection-oriented communication occurs among a client and server. Further assistance is needed for QoS since its definition is not clear. Many features, including persistent connections, chunked transfer encoding, and request pipelining, contribute to HTTP's prominence as a protocol for online interactions.

V. LITERATURE REVIEW

There are many studies done previously on the home security systems using arduino based on IOT some of them are discussed below:

This study [19], explores a home automation system that is built on the IoT that allows for home security, room air quality monitoring, and emergency support. A smartphone app allows for remote monitoring, and the system's mainboard is the NodeMCU module. After prevent mishaps, a device can detect not only air quality but also CFCs used in air conditioning systems. The technology is designed to quickly cut electricity to the property in the case of an unwanted incident and inform the client via their mobile app of the house's status.

In this study [20], a low-cost home automation and security system that utilises the IoT to keep the house safe even when its owners aren't there by controlling several switches around the house. An Arduino board, a NodeMCUESP8266MOD microcontroller, and a security system with RFID, motion detectors, gas and flame alarms are all part of the suggested system. When compared to similar products,

our suggested system's USD 31 price tag is much more affordable when considering the cost of modules and sensors.

This study [21] brings an IoT-based smart home framework to market. A system for remotely monitoring humidity and temperature has been integrated into the smart house. Additionally, controls for lighting, ventilation, and irrigation pumps may be found. When certain conditions are satisfied, it is feasible to remotely monitor and interact with home appliances using a smartphone app in conjunction with an IoT platform (Thing Speak) and the Blynk Application. Included in this effort as well have been home security and fire systems.

In this study [22], show a comprehensive solution that can verify visitors, notify the owner of an invasion, and issue fire danger notifications. The components of our system include a camera, a 3x4 keypad, an Arduino Uno microcontroller, a PIR and ultrasonic sensor, and a Raspberry Pi 3B++MQ2 gas detection module. As a last step, iris recognition is used for the purpose of person authentication. They utilised Efficient Net-B1 with the SDGR optimiser for 300 epochs. The model achieved a validation accuracy of 97.66% and a training accuracy of 99.80%.

In [23], The suggested system incorporates the idea of the IoT with sensors such as gas sensors (MQ2), PIR sensors, and temperature sensors to provide home protection. It uses the GSM module to automatically notify the user of any danger. One of the best ways to keep intruders at bay is to install a PIR (passive infrared) sensor at night, which can detect human motion. The suggested layout has great potential due to its adaptable security features and intelligent power use.

In this study [24], a surveillance system that is simple to setup and operate, secure, and cost-effective has been suggested. The 3G/GPRS Shield (SIM5215A) module receives an alarm notice from the Arduino Mega Board in the event that an intrusion is detected. Two connections are established: one with the internet server over 3G/GPRS, and the other with the user's mobile phone using GSM. A number of test scenarios have confirmed that the suggested system works as intended.

The target of this study [25], is to install an easy-to-use system that can detect gas leaks and possible house invasions. Utilising a MQ-5 gas sensor for leak detection, a PIR sensor for intruder detection, and the IFTTT Web-hooks service for email and SMS alerts, the system is fully functional. An alert will go out via the buzzer as soon as the Arduino picks it up. The technology quickly notifies the user by email and text message.

In [26], describes the design of an affordable "smart" door sensor that may notify an Android app user of a door opening event in a home or business environment. In order to connect to a web server that utilises a RESTful API, the suggested design employs a Raspberry Pi 2 board and an Elegoo Mega 2560 MCU board, which are both compatible with Arduino. The implementation involves many computer languages. They also go over some of the door sensor's limitations, such the fact that it might be affected by interference from other RF devices, and its potential future uses.

This table 1 provides an overview of the methodologies used, key achievements, limitations faced, and potential future directions for improving the proposed IoT-based home security systems.

Table 1: Related work summary for IoT-based home security systems

Reference	Methodologies	Achievements	Limitations	Future Work
[19]	IoT-based home automation system using NodeMCU module, mobile app for remote monitoring, detects air quality and CFCs	Provides home safety with manual override, detects CFCs and air quality, turns off power in emergencies.	Limited to specific air quality and CFC detection, lacks integration with advanced security features.	Add advanced security features like motion detection.
[20]	Arduino, NodeMCU ESP8266MOD, RFID, motion detection, flame and gas alarms, Android app with voice commands.	Low cost (USD 31) home automation system with faster operating delays compared to market devices.	Focuses primarily on cost-efficiency, lacks advanced security measures like video surveillance.	Integrate video surveillance, enhance security features.
[21]	IoT platform (Thing Speak), Blynk app for remote monitoring of home appliances and security systems.	Remote control of lights, fans, irrigation pumps, and home security via mobile app.	Limited to basic security; lacks complex intrusion detection mechanisms.	Incorporate advanced fire and intrusion detection systems.
[22]	Raspberry Pi 3B+, MQ2 gas sensor, PIR and ultrasonic sensors, Arduino Uno, webcam, iris recognition.	Uses ultrasonic sensors for improved motion detection, modular smoke sensors, high accuracy iris recognition.	PIR and ultrasonic sensors may still have limitations in certain environments.	Improve accuracy in diverse environmental conditions.
[23]	IoT with MQ2 gas, PIR, temperature sensors, GSM module for alerts, smart power consumption for home security.	Provides automatic alerts for hazards like fire and intruders, efficient power consumption.	GSM-based communication may have reliability issues in remote areas with poor network coverage.	Explore alternative communication methods (e.g., Wi-Fi, 4G).
[24]	Arduino Mega, PIR and microwave sensors, 3G/GPRS Shield for server and GSM communication.	Fault-tolerant surveillance system, reliable intrusion detection using heat signatures.	GSM-based communication may experience delays in real-time alerts.	Improve real-time communication, explore alternative networks.
[25]	MQ-5 gas sensor, PIR sensor, IFTTT Web-hooks for alerts, Arduino detects motion and gas leakage.	Efficient detection of gas leaks and intrusions with automatic email/SMS alerts.	Basic detection methods, does not cover fire or more advanced security measures.	Integrate additional sensors (e.g., smoke, fire) and improve detection accuracy.
[26]	IoT-based smart door sensor using Elegoo Mega 2560 MCU, Raspberry Pi 2, RESTful API, Android application for alerts.	Cost-effective door monitoring system with alerts for door open events via Android app.	Susceptible to RF interference, lacks advanced home security integration.	Reduce RF interference, integrate with full home security system.

VI. CONCLUSION AND FUTURE SCOPE

This study has explored some IoT technologies and their integration into Arduino-based platforms as a means of developing advanced, yet cost-effective solutions for home security. In the study, it has been highlighted that using existing IoT infrastructure allows for the development of systems capable of enhancing home safety through intrusion detection, surveillance, access control, and smart alarms efficiently. The

study investigates the various wireless communication technologies, networking protocols, and sensor integrations that Arduino can be used with, making it the versatile and accessible key element in such systems. In general, represented particularly by Arduino, IoT-based home security solutions appear to offer a promising direction toward renewing residential security, making it more adaptive, scalable, and user-friendly.

The future of IoT-based home security systems, particularly Arduino-based systems, holds great promise for advancement. Merging the capabilities with upcoming technologies like AI and ML can only further increase capabilities, making the systems not only more intelligent in threat detection but predictive in analytics and automatic in response. With the development of more sophisticated sensors and enhanced communication protocols, even more robust and secure solutions are likely to come up in home automation. Since such technologies are continuously improved, a great potential for devising highly personalized and responsive security systems to cater to specific needs of various households is likely to give way to smart homes that are much safer.

Reference

- [1] A. Anitha, "Home security system using internet of things," in *IOP Conference Series: Materials Science and Engineering*, 2017. doi: 10.1088/1757-899X/263/4/042026.
- [2] Oladunjoye John Abiodun and Okwori Anthony Okpe, "Smart Home Security using Arduino-based Internet of Things (IoT) Intrusion Detection System," *World J. Adv. Res. Rev.*, vol. 22, no. 3, pp. 857–864, 2024, doi: 10.30574/wjarr.2024.22.3.2000.
- [3] P. P. Patil, A. Fabian, H. Waghmode, and R. Barkul, "Home Security System using Arduino Uno (Implementation)," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2022, doi: 10.22214/ijraset.2022.42134.
- [4] Narsaiah Domala et al., "IoT Based Home Security System Using Arduino," *Proceeding Int. Conf. Sci. Eng.*, 2023, doi: 10.52783/cienceng.v11i1.312.
- [5] K. S. Kaswan, S. P. Singh, and S. Sagar, "Role of Arduino in real world applications," *Int. J. Sci. Technol. Res.*, 2020.
- [6] V. C. Rathod and A. S. Bangal, "IoT Based Home Surveillance System Using Arduino," *Int. Res. J. Mod. Eng. Technol. Sci.*, no. 03, pp. 1149–1153, 2024, doi: 10.56726/irjmet50234.
- [7] M. Subart, N. Y. Salim, and D. V. Paul, "IoT Based Home Security System," *Ijarcece*, vol. 8, no. 4, pp. 179–187, 2019, doi: 10.17148/ijarcece.2019.8430.
- [8] M. Azlan Abu, S. Fatimah Nordin, M. Zubir Suboh, M. Syazwan Md Yid, and A. Faiz Ramli, "Design and Development of Home Security Systems based on Internet of Things Via Favoriot Platform," 2018.
- [9] "Create a safer home with Arduino," blog.arduino.cc.
- [10] Zait Anat, "An introduction to arduino uno pinout," *Circuito.ioblog*, p. 78, 2018.
- [11] A. Gupta, "What is Arduino Uno?," naukri.com.
- [12] A. Anand, A. Kumar, and V. Sharma, "IOT Based Home Security Smart System Using Arduino," 2024.
- [13] G. Karuna, A. S. Reddy, K. Vishal, E. Pavan, and G. S. Negi, "Smart and Sustainable Surveillance System," in *E3S Web of Conferences*, 2023. doi: 10.1051/e3sconf/202343001030.
- [14] S. Smith, J. Ellis, and R. Abrams, "Central Alarm Stations and Dispatch Operations," in *The Professional Protection Officer: Practical Security Strategies and Emerging Trends*, 2010. doi: 10.1016/B978-1-85617-746-7.00008-0.
- [15] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.
- [16] S. C. R. V. Bhavik Patel, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, Kishore Mullangi, "Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering," *Eng. Int.*, vol. 10, no. 2, pp. 117–130, 2022.
- [17] R. Chaloo, A. Oladeinde, N. Yilmazer, S. Ozelik, and L. Chaloo, "An overview and assessment of wireless technologies and coexistence of ZigBee, bluetooth and wi-fi devices," in *Procedia Computer Science*, 2012. doi: 10.1016/j.procs.2012.09.091.
- [18] G. P. Naik and A. U. Bapat, "A Brief Comparative Analysis on Application Layer Protocols of Internet of Things: MQTT, CoAP, AMQP and HTTP," *Int. J. Comput. Sci. Mob. Comput.*, 2020, doi: 10.47760/ijcsmc.2020.v09i09.014.
- [19] A. Z. M. T. Kabir, A. M. Mizan, P. K. Saha, K. M. M. R. Songlap, A. J. Ta-Sin, and N. A. Chisty, "IoT based smart home automation and security system using mobile app with assistant robot for developing countries," in *2021 International Conference on Electronics, Information, and Communication, ICEIC 2021*, 2021. doi: 10.1109/ICEIC51217.2021.9369770.
- [20] M. H. Bhuiyan, R. K. Ahad, A. J. Haque, M. F. Monir, and T. Ahmed, "An Affordable and Effective IoT-Based Home Automation and Security System for Everyone," in *EUROCON 2023 - 20th International Conference on Smart Technologies, Proceedings*, 2023. doi: 10.1109/EUROCON56442.2023.10198937.
- [21] F. Alsuhaym, T. Al-Hadhrami, F. Saeed, and K. Awuson-David, "Toward Home Automation: An IoT Based Home Automation System Control and Security," in *2021 International Congress of Advanced Technology and Engineering, ICOTEN 2021*, 2021. doi: 10.1109/ICOTEN52080.2021.9493464.
- [22] H. Nagdewani and P. S. Mehra, "A Complete Internet of Things based Home Security System," in *2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022*, 2022. doi: 10.1109/ICCSEA54677.2022.9936168.
- [23] V. Karnatak, S. Mittal, A. K. Mishra, and N. K. Pandey, "IoT Based Energy Efficient Smart Home Security," in *Proceedings - 2023 3rd International Conference on Innovative Sustainable Computational Technologies, CISCT 2023*, 2023. doi: 10.1109/CISCT57197.2023.10351475.
- [24] M. Z. Saeed, R. R. Ahmed, O. Bin Samin, and N. Ali, "IoT based Smart Security System using PIR and Microwave Sensors," in *MACS 2019 - 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics, Proceedings*, 2019. doi: 10.1109/MACS48846.2019.9024813.
- [25] P. Kaur and N. Sharma, "An IOT Based Smart Home Security Prototype Using IFTTT Alert System," in *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, COM-IT-CON 2022*, 2022. doi: 10.1109/COM-IT-CON54601.2022.9850500.
- [26] C. Davidson, T. Rezwana, and M. A. Hoque, "Smart Home Security Application Enabled by IoT:: Using Arduino, Raspberry Pi, NodeJS, and MongoDB," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNCS*, 2019. doi: 10.1007/978-3-030-05928-6_5.