International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Intelligent Security System for Commercial Establishments Based on the Internet of Things (IoT)

Dr. Osama Amin Marie

Submitted: 26/05/2023 **Revised**: 16/07/2023 **Accepted**: 30/07/2023

Abstract: The use of many different sorts of security systems in our day-to-day lives has suddenly skyrocketed at a rate that is exponentially higher than before. Everyone living in this day and age is aware of the critical need of implementing sufficient safety precautions in settings such as workplaces, organizations, and bank vaults. In the recent years, companies have become increasingly interested in installing surveillance cameras in an effort to create workplaces that are less prone to danger. However, in order for this technology to function well, a person has to continually watch it in order to discover any problems that may appear in the image that is being caught by the camera. The fundamental objective of this research is to develop methods that are capable of improving the performance of traditional security systems. The platform-based security system that is based on the internet of things (IoT) has the potential to communicate in real time with the device. Components of the system include the speech sensor/microphone, motion/activity sensor, LTE/Wi-Fi module, and camera. Each of these sensors is interfaced with the central processing unit (CPU), which is the most important part of the system. This entire financial system will employ the Internet of Things (IoT) in real time, which will make it possible for mobile devices and computers to remotely monitor the activities that are taking place at the location where the IoT device is situated. This will make it possible for the system to be more efficient. Additionally, it will record all of these activities and save them to the cloud storage account associated with the user. The property of the user or the customer is afforded an additional level of protection thanks to the Internet of Things-based security system's contribution. Security systems are designed to carry out particular tasks in response to a breach in a protected area when the breach occurs. In this paper, a notification will be issued to the concerned individual as a warning. At that time, the user will be able to take the right actions because they will have received the warning. The most significant advantage of applying this approach is that it enables one to exercise round-the-clock remote control over their home. One is able to monitor, get notifications, and notify in the case of an emergency from anywhere in the world using a mobile application that is connected to the cloud round-the-clock when utilizing a smart locker that is based on the Internet of Things (IoT). To be more specific, our goal is to develop an Internet of Things–based wireless smart security system that is not only lightweight and inexpensive but also extendable and adaptive. This system will make use of the integration of various advanced technologies in order to function properly. It is conceivable to use a combination of various technologies in a way that is synergistic to construct a smart security system, which would allow for the remote operation of a system in a house or company (for instance, to lock or unlock a system with the help of an SMS or app). This would be achievable from a remote location. The entire system was designed with consideration given to the many different types of door locks and lockers that are used in homes and businesses so as to provide these establishments with the maximum possible level of safety. Installation may thus be made in a way that is uncomplicated and efficient thanks to this. In addition to this, our technology will function as a technique for preventing theft or burglary, recognizing it when it occurs, and countering its effects.

Index-words : *Intelligent security systems; intelligent companies; automation; the internet of things; IoT; radio frequency identification; RFID; the global positioning system; GPS; the global system for mobile communication; GSM; short message service; SMS; cloud networking; fuzzy algorithm. Index Terms Intelligent security systems; intelligent businesses; automation; the internet of things; IoT; the global positioning system; GPS; the short message service; SMS; cloud networking; fuzzy algorithm.*

Introduction

The installation of a security system has swiftly become the most important task for anybody who owns or rents a home or workplace. In addition, it is imperative for each and every one of us to be able to call either our place of residence or our place of employment a safe and secure environment. The data that were published by the National Crime data Bureau (NCRB) indicate that there were a total of 622116 instances of theft, burglary, robbery, and

Assistant Professor, Computer Information System Department, Al Quds Open University
omarie@qou.edu

dacoity that were documented in the year 2015. This information was obtained from the records that were kept in 2015. The combined cost of all of these illegal activities was 4263.50 Crores. In a similar manner, 641851 incidents were reported in the year 2016, and their total worth was 7753.0 Crores. This figure represents a 45% increase in the value of the assets. Along with the growth of business sectors and financial institutions comes an increase in the prevalence of the problem of theft.

People in many regions of the world are facing a growing number of issues surrounding the safety of their banks and other financial institutions. These challenges can take many different forms. Lockers seen in today's banks and courier services are protected by security measures that are totally under the authority of banking authorities alone. When it comes to banks, the owners of the lockers do not know what is happening with their valuable possessions or lockers, and the same is true for delivery services. When valuables are taken from safe deposit boxes as a consequence of theft or burglary, banking institutions generally never assume responsibility for the lost items and do not provide any kind of compensation for the loss of the valuables.

This clause is the only thing that is consistent across all bank locker hiring agreements; it reads, "As per safe deposit memorandum of hiring locker, the bank will not be responsible for any loss or damage of the contents kept in the safe deposit vault as a result of any act of war or civil disorder or theft or burglary, and the contents will be kept by the hirer at his or her sole risk and responsibility." The bank will take all of these industry-standard precautions, but it does not accept any liability or responsibility for any loss or damage that may be incurred by objects that have been deposited with it in any manner, shape, or form. This is true despite the fact that the bank will carry out all of these precautions. Because this is what the bank has stated, tenants are being cautioned that it is in their own best interest to insure any precious belongings that they put in a safe deposit locker at the bank. This is because the bank has made this claim. There is a huge hole in this discussion that needs to be addressed.

Who are the individuals that may benefit from this?

- Houses
- Businesses and organizations, including factories, offices, and warehouses, as well as hotels and temples
- Banking Systems
- Techniques pertaining to money and finances
- Courier/postal systems
- Collection Delivery Points, often known as CDPs (also shortened to just CDPs),
- Customizable Vault or SAFE
- The Cash Drawer is another name for the Treasury box.
- Organisation TILL
- Personal wallet or money clip
- The abbreviation "PPC" refers to a "personal protected closet."
- A variety of locks and latches
- Flight Baggage Trackers
- A method for the administration of stock control

For instance, if the house is left unattended for the most of the day and the rate of home invasions is at its highest because it is difficult to keep constant watch over the house, then the house has a greater risk of being broken into. Another situation that calls for the installation of a home security system is one in which an elderly person is left alone or children are in the care of baby-sitters, caregivers, or servants. In either of these scenarios, the elderly person or children are at increased risk of being victimized. In light of this, the installation of a home security system is not only necessary but also desired for the benefit of the homeowners' peace of mind and convenience. Your home will be converted into a "smart home" so that you may accomplish this objective via the utilization of sophisticated remote monitoring and interaction that is simple and straightforward with the system. The purpose of a smart system is to govern and monitor the environment of a building, regardless of whether the structure in question is a residence or a place of business. Because you are able to keep a close watch and remain connected at any time and in any location, you will experience less tension as a result of this ability.

These locker modules offer purchasing options twenty-four hours a day, seven days a week or completely automated distribution of products, keys, and electronic gadgets. As a result, they are particularly useful for locations such as shopping centers, hotels, airports, railway stations, car rental stations, and buildings with a high level of security. In addition, they are able to distribute products, keys, and electronic gadgets. In recent years, smart locker banks have been surfacing all over the world as a solution for last mile parcel delivery. This technology has been used by postal services on a local and global scale. The elimination of the dangers that are connected to unattended delivery is the major purpose of the solutions that have been proposed here. As part of their last-mile delivery operations in North America and Europe, several of the most successful companies in the logistics sector, including UPS, InPost, DHL, and Amazon, are using locker stations.

The lives of people all around the world are growing easier as a direct result of the rapid advancements that have been made in digital technology. Almost everything can now be done automatically. Because having access to the internet is now so vital to people's life on a day-to-day basis, cutting individuals off from the internet might leave them feeling powerless and alienated. The term "Internet of things" (IoT) is a concept that describes the process of connecting anything with an ON and OFF switch to the internet. This action is referred to as "the Internet of things." This encompasses a wide range of products, including mobile phones, home automation systems, wearable gadgets, and pretty much anything else that springs to mind. In addition to this, it makes it possible to remotely sense and operate devices throughout the architecture of a network.

The Objective of the Article

The objective of this article is to design and create a straightforward, dependable, and strong security and theft control system that is capable of providing a low power surveillance solution. This solution will enable users to effectively monitor their lockers by receiving fast video alerts upon the detection of any motion within the locker. The only way out of this mess is to create and develop such a system, and that is the purpose of this paper: to design and develop such a system. There is no other viable route out of this situation. It is possible for the information that was taken by the owner to be quickly transferred to the police officers that were present. The traditional locking mechanism that is utilized for lockers will be the subject of this investigation so that novel approaches may be developed to improve upon it. To phrase this another way, a typical locker system comprises of a lock set that calls for the use of a key in order to lock and unlock the locker. A locking system of this type may be broken into with relative ease, and the activity that is going place at the location is neither notified nor monitored unless there is someone there at the location themselves. This in turn suggests that it is not monitored or that it is impossible to keep an eye on it at all times. The traditional locking system does not preserve data such as the times the lock is opened and closed, the total number of times it has been opened and closed, or the names of the persons who have access to the lock and have taken the products out. These are all examples of data that might be saved by the typical locking system. In a nutshell, we are able to affirm that there are no records because there are none maintained.

In this body of work, we take into consideration all of the pertinent facts, and then we give solutions for the problem that are based on the internet of things (IoT). From this central site, it is possible to see and make changes to all of the records. When a system of this sort is utilized, the location of the locker may be monitored at all times, and the user will be notified through text message in the event that there is an urgent situation.

When it is constructed, this security lock system that is based on a platform connected to the Internet of Things has the potential to incorporate interaction in real time.

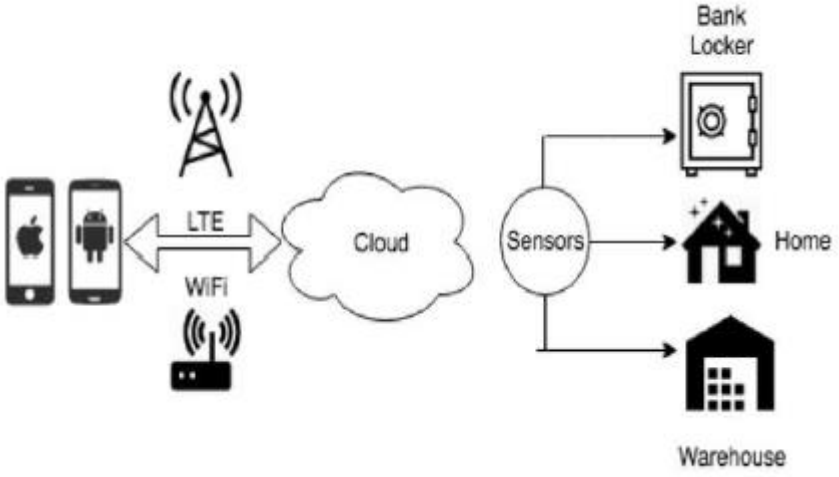

Fig. 1. The reasoning for a Smart Security System that incorporates the Internet of Things into its operation.

By utilizing the mechanism for locking it (illustrated in Figure 1). Components of the system would include a camera that also has a microphone, a push switch that also functions as a light sensor, and an LTE/Wi-Fi module that is connected to a CPU through an interface. This complete efficient and low-cost system will make use of the internet of things (IoT) in real time, which will make it possible for mobile devices and computers to monitor activities taking place at the location where the locker is placed remotely from a distance. The user's own cloud storage account is where the recordings of these actions will be kept once they have been saved.

The property of the user or the customer is afforded an additional level of protection thanks to the Internet of

Things-based security system's contribution. In the task that is being done right now, a warning notification is sent to the person who ought to be concerned in order for the user to take out the necessary processes. The key advantage of utilizing this system is that it enables you to exercise remote control over your locker at any time of the day or night. Using a mobile application that is connected to the cloud, a person with a smart locker that is powered by the Internet of Things (IoT) is able to monitor the locker, get notifications, and provide information in the case of an emergency from any location on the planet. When one takes these steps, they are able to monitor the activity stream (which is also referred to as the timeline) and receive notifications anytime the software detects movement in the data.

Individual security systems are only capable of performing a certain set of functions, which can render them inefficient, expensive, unreliable, and challenging to upgrade. Due to this constraint, monitoring, controlling, managing, and maintaining any small to large scale security system may be an incredibly difficult undertaking. Security systems that are automated and wireless protect information that is critical and sensitive, personal items, and material assets against acts of vandalism, theft, and unlawful entrance. There is not enough that can be done to safeguard them via the activities of individuals or through the use of technology methods. Therefore, electronic sensor-based protective security system devices are the right choice for use in applications that are portable or mobile. Not only are these devices an excellent complement to the steps that have been taken, but they are also an ideal choice in general.

It is difficult to safeguard or secure the interiors or the inside of a structure since the most susceptible parts are the ceilings, doors, walls, and windows of the building. When you have the technology of wireless security systems, it is reliable to preserve critical data and materials by utilizing proper sensors. These sensors help detect any unwanted attempts or assaults and then trigger an alarm when they find them. Because of this, it is now feasible to secure critical data and materials by utilizing appropriate sensors. Using a museum as an example, guarding precious items from unauthorized and unidentified individuals becomes difficult for the sensor systems since the sensors must transmit the alarm signal to both off-duty and on-duty authorities, as well as visitors and the thief, as an alert. This makes securing precious things from unauthorized and unidentifiable persons difficult for the sensor systems. Additionally, the burglar must be aware that the alarm signal has been activated in order for the theft to be successful. As a consequence of this, the degree to which the demand for safeguarding items may be supplied is inversely proportional to the degree to which a security system that is more trustworthy and accurate can be constructed.

The Internet of Things (IoT) is a rapidly evolving and emerging technology in which everything that may be enhanced by a connecting system is wirelessly networked to people all over the world. This technology is expected to have a significant impact on society in the near future. The Internet of Things is a more reliable platform than other similar systems due to the fact that it is composed of a number of distinct ecosystems, each of which contains a distinct collection of capabilities and functions. An electronically created sensor system is located at one end of the system, and at the other end is the home or industrial automated system, automated vehicles, which hold the sensitive data. Both the beginning and the end of the system are available. It is anticipated that the Internet of Things will cause widespread disruption across practically all existing business sectors and provide a significant number of doors to hitherto unexplored industry opportunities. The Internet of Things will play a role in the improvement of public safety in the not-too-distant future.

This acts as inspiration for the team to build a safe and secure locking solution that is compatible with the IoT platform. consumers who own this locker will be able to use their mobile or computer devices, from anywhere in the world, to monitor and stay informed about any suspicious conduct taking place on a cloud platform. This system will be accessible to consumers who own this locker.

Related Work

Jivani and colleagues [1] developed solutions without having a security system in place, which means they were not able to prevent robbery, fire, or any other unfavorable scenario from occurring. Ming Yan and his colleagues [2] designed and prototyped an innovative smart living system that they termed the home lighting control system. The system made use of an Android smartphone that was equipped with bluetooth. There was no such thing as a smart security system that existed back then [3]. After that, Murali Krishna [4] developed a wireless home automation system for bluetooth using FPGA. This system's goal is to facilitate wireless communication of data over a relatively small distance, and it does so by offering a necessary platform that combines ease of use with the capacity to exert control. In particular, the technology is designed to facilitate the wireless transmission of information within a very close proximity. David et al. [5] investigated the same subject as the research [4], but their work includes additional sensors and pins that are able to determine if a door is open or closed. When the sensor determines that the locker door is open, it will cause an interrupt to be generated and

communicated to the processor. This in turn causes the camera to begin recording when it is aimed in the suitable direction when it is oriented in the appropriate direction. The camera, which is linked to the processor, initiates a connection with or has a discussion with the cloud. Following this, a notification is sent to the user's mobile app in order to inform them to the event. The user is able to log in to their account and have access to the live video footage from any point in the world when they utilize the Mobile App. This is possible from any device that can access the Internet. The graphic included a representation of the supplementary attributes. 2. The LTE/Wi-Fi module is interfaced with the CPU and the board so that it may serve the goal of making the complete device capable of gaining internet connection. The mobile application that is stored in the cloud will be able to communicate with the device, send data to, and receive data from the device when the device is connected to the internet. The microphone, in addition to assisting with voice recognition of the user, may capture potentially suspicious behavior and can also record the user's voice. The processor is the component that is responsible for ensuring that communication is maintained with all of the external interfaces and components in order to ensure that the right module may be activated at the appropriate time. The General Purpose Input/output pin, more commonly referred to as the GPIO pin, serves as an interface that may be found on either the central processing unit (CPU) or the microcontroller. Included in this package are, among other things, face recognition, hand recognition, and leg recognition. Buildings that are associated with public safety, including but not limited to police stations, fire stations, and ambulance stations, as well as local hospitals and blood banks, Web application with regular notifications, five user accounts, and five user logins, Mobile App SMS/MMS, You can reach us by either e-mail or phone., Activity Feed (the actions that have been carried out), Including, but not limited to, Whatsapp, Facebook, and Youtube. functionality. An email notification system was incorporated by the authors in a way comparable to that described in [6] and [7]. In addition, Anusha et al. [8] underlined the fundamental objective of home automation and security as being to help disabled and elderly folks by supporting them to handle house appliances and notifying them in crucial conditions backed by android system methodology. This goal was highlighted as being the primary purpose of home automation and security. The basic goal of both home automation and security systems is to accomplish this. Priyanka and her colleagues [9] describe a security system that is capable of monitoring both a residential and a business location simultaneously. In order to identify the presence of trespassers, the controller is outfitted with a passive infrared (PIR) sensor device. Afterwards, a picture is taken by a camera that is likewise linked to the controller. This photo is taken immediately after the previous one. After that, the photograph is sent out by e-mail, and in addition to that, a buzzer alert is sent so that other people are aware of what has happened. Haque et al. [10] developed a method that makes use of a personal computer as the primary controller for a variety of electrical devices and home appliances. Visual Basic 6.0 was the programming language that was utilized throughout the construction of this system. In order for the system to be able to detect spoken words, components of the Microsoft speech engine were incorporated into the system. Timers and voice commands are two different ways that home appliances may be controlled and operated. The names Amrutha and et. al. [11] developed a system that detailed the voice recognition technique that could be utilized to run the home appliances. This system was referred to as the speech recognition system. The initial notion conceived by Haques served as the impetus for this project. When it comes to the company, the other parties might be able to [12].

Design and Implementation

A typical block diagram is shown in Figure 3, and it consists of the following components: a push switch, a light sensor, a motion sensor, a camera, a microphone, and an LTE/Wi-Fi module. All of these components are interfaced with either the central processing unit (CPU) or the microcontroller. The sensor, which will be installed in the door of the locker and connected to the general-purpose input/output (GPIO).

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

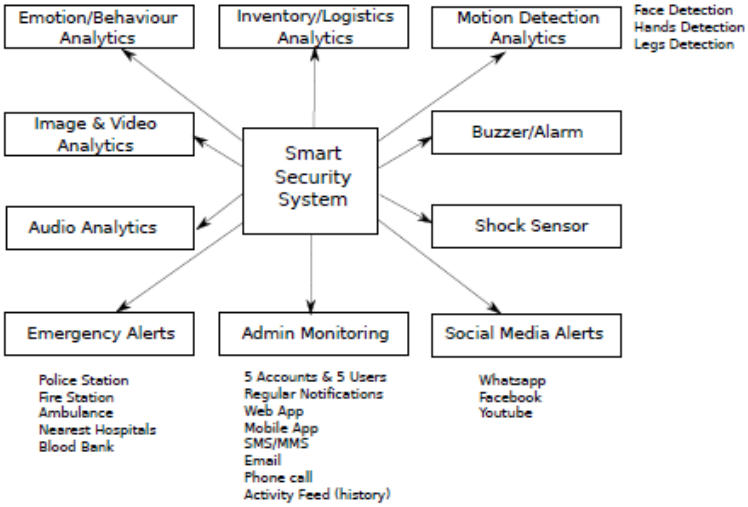

Fig. 2. A depiction in the form of a schematic of an all-encompassing intelligent security system for buildings or organizations

Hardware Design:

- In order to provide live streaming capabilities of audio and video data through Wi-Fi, the design makes use of a microcontroller in conjunction with the most cutting-edge wireless and audiovisual technology.
- The following are able to be recorded and aired thanks to this feature:
- Video - 720p @ 15FPS
- PCM audio with 16 bits per second and a frequency of 11025 hertz Offers support for the RTP and RTSP protocols respectively.
- Access to Wi-Fi networks operating on the 802.11 b/g/n protocol is made available through SimpleLinkTM.
- Integrated provisioning that enables a speedy and uncomplicated connecting of the device to a Wi-Fi network
- Modes of Advanced Technology for the Saving of Power

Embedded Software Design

The most important function that the embedded software will be able to do is to. Get the gadget ready to detect motion and check that it is still functioning properly. Motion should trigger the activation of the video camera, and when motion is detected, the camera should be set to record both live video and audio.

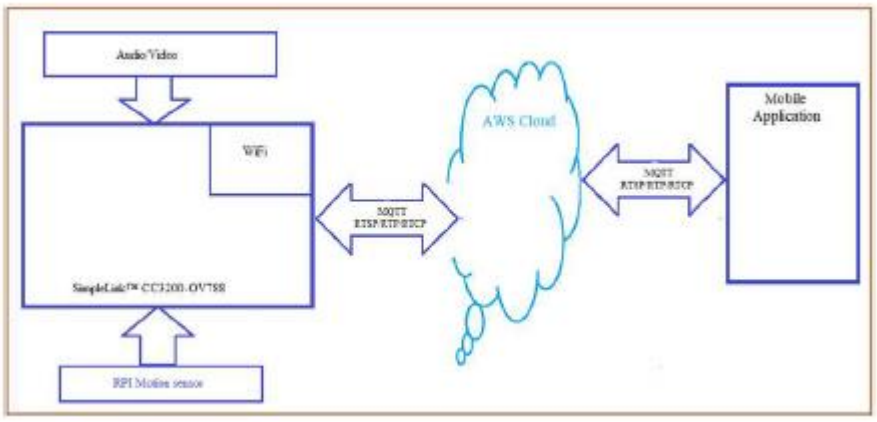

Fig. 3. A depiction in the form of a schematic of an all-encompassing intelligent security system for buildings or organizations

- Be able to transmit live video to a cloud server that has been configured to use the RTP protocol in conjunction with the RTSP protocol and the RTCP protocol.
- Maintain consistent 15-minute intervals for the transmission of device heart beats to the cloud using MQTT.
- Users should be able to request capabilities for live broadcasting.
- Have the capability to upgrade and download the firmware from a distant location. The most recent firmware updates will be distributed to the appropriate devices by way of the cloud; moreover, the devices should be able to upgrade themselves wirelessly.

Boot Up Design

- An altered distribution of Linux, known as Ubuntu, will serve as the basis for the device's operating system. As soon as it is powered on, the electronic device will immediately link itself to the Wi-Fi network that broadcasts the clearest signal.
- Connects to the cloud by utilizing the messaging protocol MQTT.
- The cloud receives the power up message and broadcasts it, and then the cloud sends the same message to the mobile application that has been subscribed to a certain locker.
- The background process will create an RTSP server.
- Performs the initial setup of the motion sensor and configures the GPIO interrupt to fire anytime the CPU detects any motion. This step is required before the motion sensor can be used.
- Performs an initialization of the camera module before recording a ten-second video clip that is subsequently transferred to the cloud via RTP in the format that has been specified.

In the event that any of the aforementioned procedures produced a problem, the device need to perhaps send that error to the cloud over MQTT, presuming that the connection to MQTT was successful. In that scenario, it will be the user's responsibility to manually check for and address any issues that may have arisen as a result of the situation.

After the device has successfully booted up and run its own self-test, it will send a message to the cloud over MQTT with the subject line "Boot Up successful."

After this, the device should go into a sleep mode, with the exception of the motion detecting unit, which should continue to function normally so that it can detect motion. After being forced to wake up once every 15 minutes on its own, the device will then publish its heart beat to the cloud via MQTT before resuming its sleep state.

Audio and Video Streaming There are two possible outcomes that will determine how the live streaming of video and audio will be carried out. First, in reaction to any motion that is recognized, and second, in response to a request made by the user through the mobile application. Whenever there is any motion that is identified. Streaming live content determined by the detection of motion. The device will wake up and initialize the relevant hardware components after motion has been detected and the device has been activated. At that moment, the camera will have been set off to begin sending data via live feed after having been activated.

After the audio and video data have been split using the RTP protocol into proper RTP packets, those packets will be transferred to the cloud that has been built up using Wi-Fi connection using the UDP protocol. The cloud will be set up.

The camera on the device is turned off and the gadget enters a sleep mode when the door to the locker is closed. The motion sensor is the only part of the device that remains active so that it may continue to detect any activity. After the motion has been stabilized, this step will take place.

The live broadcast is then saved to the cloud, and after that, it is made available on the mobile application for users who have registered for that locker (Figure 6).

Mobile application design

The mobile application will offer support for both the Android and iOS mobile operating systems. Before any configurations on the device or in the cloud can be created or the device itself handled, the user will need to download and install this application first (Fig. 4).

The Framework for Mobile Application Architecture

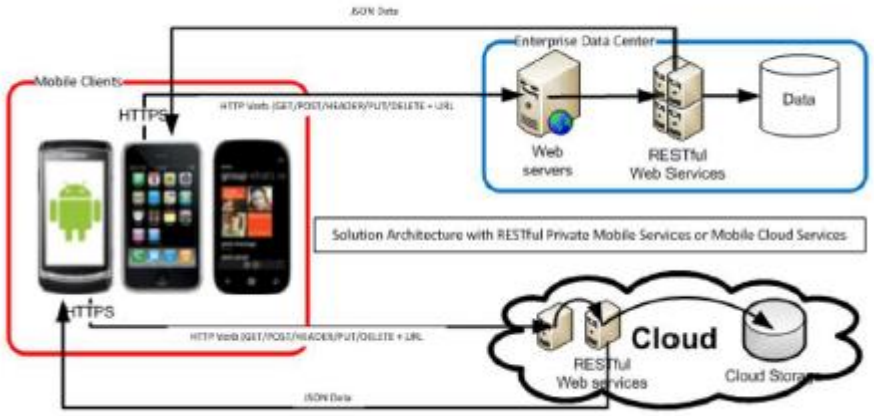

Fig. 4. Application architectures for mobile devices used in intelligent surveillance systems

Design Strategies, Frameworks, and Elements

The development of the mobile application is now taking place within the context of the Angular 2 framework. CSS was leveraged to get the desired look and feel for the mobile application. Bootstrap also makes use of CSS. A REST service is what's responsible for handling the communication that has to take place between the mobile device and the backend server. The HTTP protocol is used for all client-side communication with the REST service. A Tomcat server, which is itself housed on Amazon's cloud infrastructure, is responsible for providing hosting for the REST service. For the purpose of transferring data between the locker board and the Amazon server, the communication protocol known as MQTT is implemented.

The message will be sent to the Registered Mobile from the GCM server after first being received from the Amazon server. Google Cloud Messaging, which is abbreviated as GCM and stands for "Google Cloud Messaging," is used for the transmission of alerts to mobile devices.

OAuth, which in turn utilizes one of the user's existing accounts (such as Google Sign-on, Facebook, etc.), is used to authenticate the user. In other words, OAuth uses the user's current accounts to authenticate the user. The Google Sign-on service is being included into our application. GCM is the storage location for the authentication data that are required in order to get the token id for the device.

The data persistance is handled by Postgres, which is the database being employed. The cloud storage provided by Amazon could include a copy of this database.

For the live video streaming, a video streaming server is used (the Wowza live streaming is now in the process of being finished), and the live video streaming is being done in real time.

OAuth

OAuth is an open authorization protocol that enables client applications to contact HTTP services such as Facebook and GitHub, amongst others, in order to obtain access to the resources that are controlled by the respective owners of such resources. OAuth was developed by the Internet Engineering Task Force (IETF). It makes it feasible to transfer resources kept on one website to another website without having to use the credentials of either website. This makes it possible to move resources across websites.

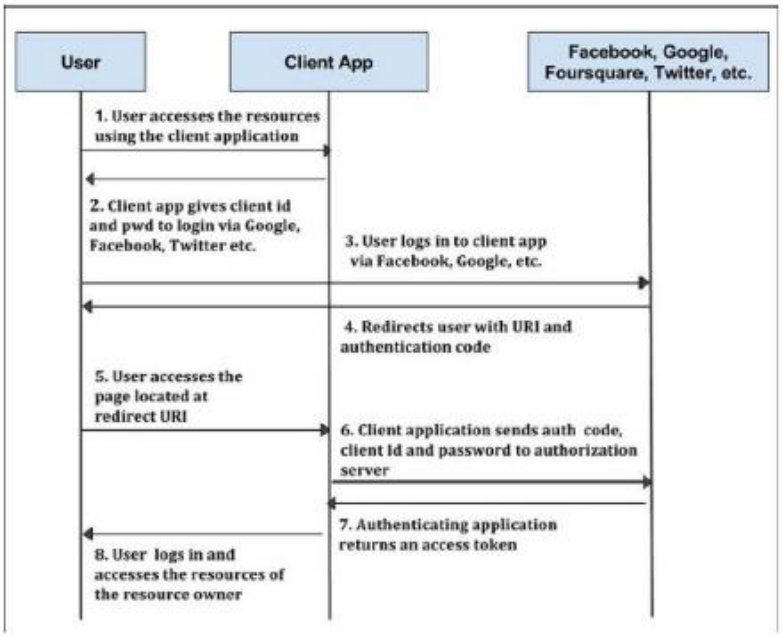

Fig. 5. A data flow diagram for a smart security system that operates through the usage of a mobile application

A Method for the Transmission of Notifications

You may send notification messages to desktops as well as mobile devices by utilizing the GCM push notification service. This allows you to reach a wider audience. GCM is a messaging protocol that allows users to transmit messages securely across several platforms. It is compatible with multiple platforms. Cloud Functions for GCMlets will automatically carry out backend code in response to events that are created by Firebase features and HTTPS requests. The environment in which the code is executed is one that is kept up to date (Fig. 5), and the code itself is stored in the cloud at Google.

IoT Data Analytics

Thingspeak.com is the platform that is employed for the purpose of executing analyses on the data that is acquired by various devices that are connected to the Internet of Things. The information that we provide by way of the mobile app in the form of data and activities is transmitted to Thingspeak. From there, the information is transmitted to the WIFI module. From there, the information is transmitted to the Controller. After then, the analytics are carried out in Thingspeak so that the users or analysts may be presented with insights.

Results and Analysis

An environment that emulated real-time events served both as the setting for the generation and analysis of the outcomes. The Raspberry pi Microcontroller, which was used to develop the prototype and was pre-installed with Linux OS, is currently being shadowed on a cloud platform, which will be tracking the heartbeat of the controller. After the device has been powered on, it immediately begins the process of booting up the system, connects to the cloud by way of the Wi-Fi module, turns on the motion sensor, and then waits for motion to be detected before continuing. The cloud will send a notification to the device or microcontroller, and the activation of the device or microcontroller will be dependent on the detection.

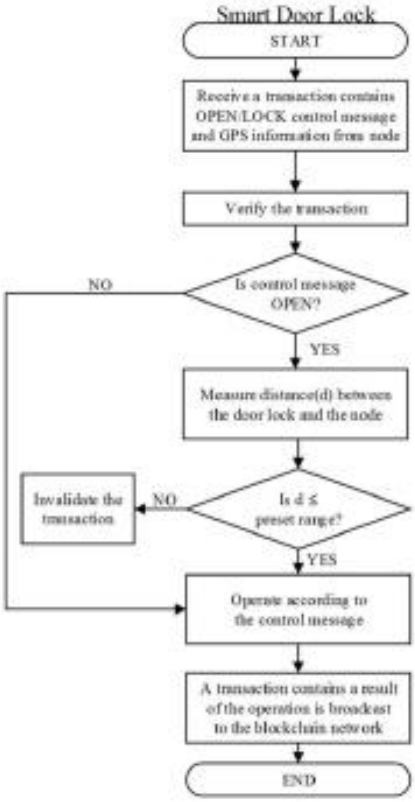

Fig. 6. Control Algorithm for Security Locks That Are Intell

the Mobile Application in addition to a text message that was delivered to the mobile device that was registered by utilizing a GSM module. The creation of the prototype is based on the generic application, which acts as the basis for the development. If the user does not make a request to watch the live relay, a video alert will be given to them whenever any detection is made, even if they have not asked to see it.

When a user first visits the Mobile App (shown in Figure 7), they will be requested to register and create a one-of-a-kind account for themselves by following the on-screen instructions. It is necessary to use the same credentials that were used at the first registration in order to access subsequent logins. It would be incredibly helpful for consumers if they were able to register several items or smart lockers under a single account. This would make the process much more streamlined. The mobile application has a pull-down menu that gives users the ability to see live or recorded video, as well as logs of when they signed in and when they logged out, amongst other possibilities.

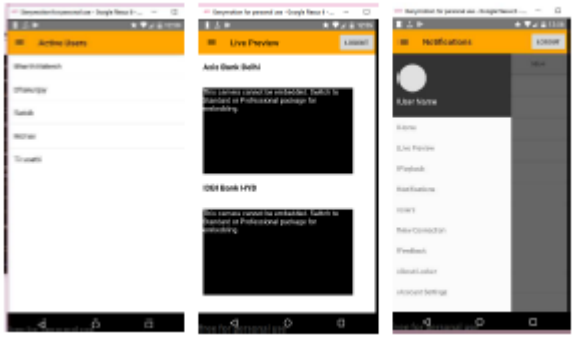

Fig. 7. Application for Intelligent Mobile Devices Concerning Safety

The IoT analytics are maintained up to current, the user's actions and use are sent to the cloud, and all of the data are preserved in order to enable the User Interface to be studied by utilizing the Mobile App. As a result of the characteristics of the live relay broadcast, there is always some degree of delay. This lag in timing is due to a variety of various factors, including the connectivity and speed of the internet, amongst others.

Conclusion and Directions for Future Work

Our system will be able to distinguish selected and sensitive phrases used by people working inside an organization by making use of technology such as machine learning (ML) and artificial intelligence (AI). This functionality will be accessible going forward. Internet of Things (IoT) technology that is powered by artificial intelligence (AI) is able to process enormous volumes of data generated by a large number of devices and deal with sophisticated data or relativity challenges. Implementing Internet of Things (IoT) technologies that are driven by artificial intelligence (AI) with the intention of boosting the productivity of intelligent enterprises is the objective. It entails exercising cognitive control over the many systems that are required in order to run a business successfully. Artificial intelligence (AI) in smart business devices should be able to interpret raw sensor data from your phone and any other connected devices into a pattern of behavior that is helpful to customers. This pattern of behavior can then be used to make business decisions. That is to say, artificial intelligence in devices that have learnt your patterns and can begin to predict the experience that most effectively fulfills your requirements at any given moment. In order to be deemed really intelligent, Internet of Things devices and apps need to incorporate user-aware artificial intelligence. In order to identify potential robbers based on the information that is currently available, our system will examine human behavior and eye movements, in addition to applying facial recognition algorithms. If a user who is restricted from accessing the network makes an effort to do so despite the restriction, the system will send an alert to the administrator. Blockchain, a decentralized ledger technology, will be included into the development of the totality of the new security system.

A network, a distributed database of records, or a public ledger of all of the transactions, messages, and notifications that have been carried out and exchanged among the many people who are involved may be thought of as the blockchain. Blockchains can also be thought of as a public record of all of the activities that have taken place. After obtaining the unanimous consent of the overwhelming majority of users who are connected into the system, each transaction that is entered in the public ledger is considered to have been properly verified. After data has been inputted or registered, it is not possible to erase it; this feature, which is known as data integrity, safeguards against the unintentional loss of data. By mandating that each transaction be digitally signed with the participant's private key that was used to initiate the transaction, authentication assures that each transaction is valid and protects against fraudulent activity.

Specifically, intelligent systems for businesses are of the highest relevance owing to the fact that they are tightly tied to the safety of the employer. This connection makes them particularly important. On the other hand, the information that is sent and received by the many smart systems that are now in use is vulnerable to being hacked and falsified. We need to develop this system that is built on blockchain in order to address these security concerns, particularly when these systems analyze certain events that are occurring around themselves by using data given through sensors and then acting on the knowledge that they have gleaned from that assessment. In addition, the distributed ledger technology (blockchain) system provides authentication, as well as non-repudiation and the integrity of data. Because of this function, a user who has not been given permission to participate in the blockchain network is unable to do so. By utilizing this approach as a guide, more advancements can be made in the following areas: [13][14][15][16][17][18].

References

[1] M. N. Jivani, "Gsm based home automation system using app- inventor for android mobile phone," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 3, no. 9, 2014.

[2] M. Yan and H. Shi, "Smart living using bluetooth-based android smartphone," *International Journal of Wireless & Mobile Networks*, vol. 5, no. 1, p. 65, 2013.

[3] V. Govindraj, M. Sathiyanarayanan, and B. Abubakar, "Customary homes to smart homes using internet of things (iot) and mobile application," in *Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On*. IEEE, 2017, pp. 1059–1063.

[4] B. M. Krishna, V. N. Nayak, K. REDDY, B. Rakesh, P. KUMAR, and N. Sandhya, "Bluetooth based wireless home automation system using fpga." *Journal of Theoretical & Applied Information Technology*,vol. 77, no. 3, 2015.

[5] N. David, A. Chima, A. Ugochukwu, and E. Obinna, "Design of a home automation system using arduino," *International Journal of Scientific & Engineering Research*, vol. 6, no. 6, pp. 795–801, 2015.

[6] S. Manohar and D. M. Kumar, "E-mail interactive home automation system," *International Journal of Computer Science and Mobile Com-puting*, vol. 4, no. 7, pp. 78–87, 2015.

[7] R. Suryavanshi, K. Khivensara, G. Hussain, N. Bansal, and V. Kumar, "Home automation system using android and wifi," *International Journal Of Engineering And Computer Science*, vol. 3, no. 10, 2014.

[8] S. Anusha, M. Madhavi, and R. Hemalatha, "Home automation using atmega328 microcontroller and android application," *International Re- search Journal of Engineering and Technology*, vol. 2, 2015.

[9] P. Priyanka and D. K. S. Reddy, "Pir based security home automation system with exclusive video transmission," *International Journal Of Scientific Engeneering and Technology Research, ISSN*, pp. 2319–8885, 2015.

[10] S. Haque, S. Kamruzzaman, M. Islam *et al.*, "A system for smarthome control of appliances based on timer and speech interaction," *arXiv preprint arXiv:1009.4992*, 2010.

[11] S. Amrutha, S. Aravind, S. S. Ansu Mathew, R. Rajasree, and S. Priyalakshmi, "Speech recognition based wireless automation of home loads-e home," *International Journal of Engineering Science and Innovative Technology (IJESIT)*, vol. 4, no. 1, 2015.

[12] M. Saifuzzaman, A. H. Khan, N. N. Moon, and F. N. Nur, "Smart security for an organization based on iot," *International Journal of Computer Applications*, vol. 165, no. 10, pp. 33–38, 2017.

[13] M. Sathiyanarayanan and K. S. Kim, "Multi-channel deficit round- robin scheduling for hybrid tdm/wdm optical networks," in *Proc. ofthe 4th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT 2012)*, St. Petersburg, Russia, Oct. 2012,pp. 552–557.

[14] M. Sathiyanarayanan and B. Abubhakar, "Dual mcdrr scheduler for hybrid tdm/wdm optical networks," in *Proc. of the 1st International Conference on Networks and Soft Computing (ICNSC 2014)*, Andra Pradesh, India, Aug 2014, pp. 466–470.

[15] M. Sathiyanarayanan and B. Abubakar, "Mcdrr packet scheduling algorithm for multi-channel wireless networks," in *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*. Springer, 2015, pp. 125–131.

[16] M. Sathiyanarayanan, S. Azharuddin, and S. Kumar, "Four different modes to control unmanned ground vehicle for military purpose," vol. 2, no. 3, pp. 3156–3166, 2014.

[17] M. Sathiyanarayanan, V. Govindraj, and N. Jahagirdar, "Challenges and opportunities of integrating internet of things (iot) and light fidelity (lifi)," in *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. IEEE, 2017, pp. 137–142.

[18] M. Sathiyanarayanan and C. Turkay, "Challenges and opportunitiesin using analytics combined with visualisation techniques for finding anomalies in digital communications," in *ICAIL DESI VII Workshop*, 2017.

[19] Abdul Rahman, Artificial Intelligence in Drug Discovery and Personalized Medicine , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[20] Nair, K. S. S. . (2023). Rapidly Convergent Series from Positive Term Series. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 79–86. https://doi.org/10.17762/ijritcc.v11i3.6204

[21] Timande, S., & Dhabliya, D. (2019). Designing multi-cloud server for scalable and secure sharing over web. International Journal of Psychosocial Rehabilitation, 23(5), 835-841. doi:10.37200/IJPR/V23I5/PR190698