



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENSURING PRIVACY AND SECURITY WITH A USER FRIENDLY SMART HOME AUTHENTICATIN SYSTEM

Dr.M.SANGEETHA¹, Ramsanthosh.S², Sabari.S³, Vighneshwaran.P⁴
and Srivishal.V⁵

¹Head of The Department, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu, India

² Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu ,India

³ Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu ,India

⁴ Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu, India

⁵ Student, Computer Science and Engineering, V.S.B Engineering College, Karur,Tamilnadu, India

ABSTRACT

As smart home technology becomes more widespread, ensuring privacy and security in these systems is of utmost importance. This paper proposes a user-friendly authentication scheme that allows for secure and anonymous access to a smart home environmental control system. The scheme utilizes a combination of biometric authentication, one-time passwords, and encryption techniques to ensure the privacy of user information and the security of the system. The proposed scheme is evaluated through a series of experiments, and the results demonstrate its effectiveness in preventing unauthorized access and protecting user data. This authentication scheme provides a practical solution for homeowners who want to ensure the safety of their smart homes while maintaining user-friendliness and ease of use.

In this Smart home technology is a new Internet-of-Things (IoT) application that allows users to control home gadgets remotely. Because the user/home communication link is unsecure, secure communications in the smart home environment require an efficient and anonymous authentication mechanism. The smart home is an environment in which heterogeneous electronic gadgets and appliances are networked together to give smart services to individuals in a ubiquitous way. As houses become smarter, more sophisticated, and more reliant on technology, the requirement for an appropriate security mechanism with minimal human interaction grows. Recent severe security hacks have demonstrated how Internet-enabled smart homes may be transformed into highly dangerous places for different nefarious motives, resulting in privacy problems for individuals.

Authentication intelligence was used in this project to recognize and evaluate people and monitor them using our evolving technology. In the proposed work, we employ LBPH (local binary pattern) and machine learning approaches to minimize the recognize time of many items in less time while maintaining the optimal time complexity. If an unauthorized individual enters, it will capture and send an alert through email.

Keywords—ARDUINO UNO, IOT, CAMERA

INTRODUCTION

Smart homes have revolutionized the way we interact with our living spaces, allowing us to control everything from the temperature to the lighting with just a tap on our smartphone. However, with this convenience comes the risk of privacy and security breaches. Unauthorized access to a smart home's environmental control system can compromise the safety and comfort of the residents. Therefore, it is essential to have a robust user authentication system in place that ensures both security and anonymity. In this paper, we present a secure and user-friendly authentication scheme that guarantees privacy and protection against malicious attacks in a smart home environment.

A smart-home environment is used to aid people with various chores by adding automation to them, such as a smart meter, which may assist users by displaying real-time consumption of power, voltage, and load, as well as other related devices. These devices can be detect that UART to software programs. With these services, you may provide a secure home to the environmental.

In this article, we explore real-time facial recognition with the notion of safe locking automation using IoT for door unlocking system to give required security to our homes, offices, hospitals, banks, and so on, as well as associated control activities. We understand that security is a crucial concern for everyone in everyday life, thus we worked on this project to ensure security through the use of smart homes. Security precautions should be taken when using the Azure database. It employs picture capture in an embedded system based on the arduino uno and the Azure server architecture. The ATMEGA328P Microcontroller operates the web camera, capturing it and activating a relay to unlock the door. The system module has a secure facial recognition function for automated door unlocking. The camera captures a facial image and compares it to the image stored on our local machine.

LITERATURE SURVEY

[1] The most common modalities utilized by surveillance systems are discussed, putting emphasis on video, in terms of available resolutions and new imaging approaches, like High Dynamic Range video. The most important deep learning algorithms are presented, along with the smart analytics that they utilize.

[2] The traditional Closed-circuit Television (CCTV) system requires to be monitored all the time by a human being, which is inefficient and costly. Therefore, there is a need for a system which can recognize human activity effectively in real-time. It is time-consuming to determine the activity from a surveillance video, due to its size, hence there is a need to compress the video using adaptive compression approaches.

[3] Wireless Video Sensor Networks (WVSNs) provide opportunities to use large number of low-cost low-resolution wireless camera sensors for large-scale outdoor remote surveillance missions. Camera sensor deployment is crucial in achieving good coverage, accuracy and fault tolerance.

[4] The nature of directional sensor network demands novel algorithms and solutions. In directional sensor networks, this paper starts from the concept and characteristics of directional sensing model, and then summarizes up the sensing properties and behaviors of directional sensors.

[5] This provides an opportunity for aiding transport planners and policy-makers to plan transport systems and cities more responsively. However, there are currently limitations when it comes to understanding the secondary activities of individual commuters. Accordingly, in this paper, we propose a framework to detect and infer secondary activities from individuals' daily travel patterns from the smart card data and reduce the use of conventional surveys.

[6] This letter proposes a preliminary setup based on imaging techniques to assist in solving the camera placement problem. The proposed setup computes the camera coverage in a two-dimensional digitized floor-plan. Additionally, a pixel wise line drawing routine analyzes the ray's visibility from the viewpoint to the width of the field of view.

[7] The study of land use/land cover (LU/LC) changes is very important to have proper planning and utilization of natural resources and their management. Traditional methods for gathering demographic data, censuses, and analysis of environmental samples are not adequate for multicomplex environmental studies

[8] Data redundancy caused by correlation has motivated the application of collaborative multimedia in-network processing for data filtering and compression in wireless multimedia sensor networks (WMSNs). This paper proposes an information theoretic image compression framework with an objective to maximize the overall compression of the visual information gathered in a WMSN.

[9] Face recognition is one of the most challenging applications of image analysis and pattern recognition. Face recognition methods perform well on the images that are collected with careful cooperation of the subjects. Whereas, the challenges of change in illumination, expression, pose make this problem harder.

[10] This paper first analyzed advantages and disadvantages of various background modeling methods in video analysis applications and then compared their performance in terms of quality and the computational cost. The Change detection.Net (CDnet2014) dataset and another video dataset with different environmental conditions (indoor, outdoor, snow) were used to test each method.

PROPOSED METHOD

Watchman and bank officer images are taught to our processor in our suggested method. The video is continually recorded by the processor. If an unfamiliar individual attempts to enter the room, the camera will evaluate and communicate data through email using machine learning. We utilized the Local binary pattern algorithm in this project (LBPH). Face detection and identification will be investigated by LBPH. We will use AI and OpenCV to find people in real time in this suggested system. Following picture acquisition, it must be pre-processed and compressed. The model is trained using images. It is learned by extracting the desired pattern from the image using feature extraction. The image is then compressed using

feature fusion and dimension reduction for dependable and real-time performance. When an unauthorized individual attempts to enter, the door does not open and an alarm is sent through email. The information is shown on an LCD screen.

SOFTWARE DESCRIPTION

ARDUINO IDE

To develop computer code and upload it to the physical board, the Arduino IDE (Integrated Development Environment) is utilized. The Arduino IDE is really straightforward, which is probably one of the primary reasons Arduino has become so popular. We can safely say that compatibility with the Arduino IDE is currently one of the most important requirements for a new microcontroller board. Several valuable features have been introduced to the Arduino IDE over the years, and you can now manage third-party libraries and boards from the IDE while maintaining the simplicity of programming the board.

Arduino programming basics

Sketch

The first new phrase is from the Arduino sketch software. Structure, Values (variables and constants), and Functions are the three major components of Arduino programming. Let us begin with the structure, which has two basic functions:

Setup() function As a drawing begins, the setup() method is invoked. It is used to initialize variables, pin modes, and begin accessing libraries, among other things. The setup function will only execute once when the Arduino board is powered on or reset.

The **Serial.begin(9600);** instruction opens the serial port, allowing the board to send output for display by the serial monitor (see the "Output" sub-section below).

function loop()

Following the setup() method, which initializes and sets the initial settings, the loop() function performs exactly what its name implies: it loops sequentially, enabling your application to modify and respond. It is used to operate the Arduino board actively. The Serial.println(sensorValue); statement is used to show a value read from an analog pin (see "Understanding microcontroller Pins" sub-section below).

PYTHON

Python is a popular high-level general-purpose programming language. Guido van Rossum invented it in 1991, and the Python Software Foundation expanded on it. It was created with code readability in mind, and its syntax lets programmers to communicate their notions in fewer lines of code. Python is a programming language that allows you to work fast and efficiently integrate systems. Python has two major versions: Python 2 and Python 3. Both are pretty distinct. It is used for server-side web development, software development, mathematics, and system programming. Python may be used to build web applications on a server. Python may be used in conjunction with software to develop processes. Python has the ability to connect to database systems. It also has the ability to read and change files.

Python may be used to manage large amounts of data and conduct complicated mathematical calculations. Python may be used for quick prototyping as well as full-fledged program development.

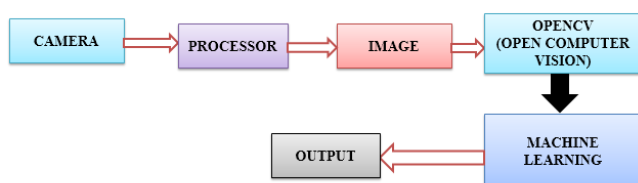
Python runs on a variety of systems (Windows, Mac, Linux, Raspberry Pi, etc). Python has a basic grammar that is comparable to that of the English language. Python's syntax enables programmers to build programs with fewer lines than other programming languages. Python is an interpreter-based language, which means that code may be executed as soon as it is written. This implies that prototyping can be accomplished quickly. Python can be processed procedurally, object-orientedly, or functionally.

LANGUAGE FEATURES EXPLAINED

Unlike C and C++, there are no distinct compilation and execution phases. Run the application directly from the source code. Python internally turns source code into byte codes, which are then translated into the native language of the computer being used to run it. There is no need to bother about linking and loading libraries, etc. Python applications that are platform independent can be written and run on a variety of operating systems. Python may be used on a variety of platforms, including Linux, Windows, Macintosh, Solaris, and others. Open Source and Free; Redistributable Advanced Language There is no need to worry about low-level issues like managing the program's memory with Python. Simple Closer to the English language; Simple to learn. Greater focus should be placed on the solution to the problem rather than the syntax. Embeddable Python can be used within a C/C++ software to provide users with scripting capabilities. Robust: Outstanding handling characteristics Built-in memory management approaches Supportive Library the Python Standard Library is quite large. Python's "batteries included" concept; it can aid with regular expressions, documentation generation, unit testing, threading, databases, web browsers, CGI, email, XML, HTML, WAV files, encryption, GUI, and many other things. Apart from the standard library, there are several alternative high-quality libraries available, such as the Python Imaging Library, an incredibly easy image processing toolkit.

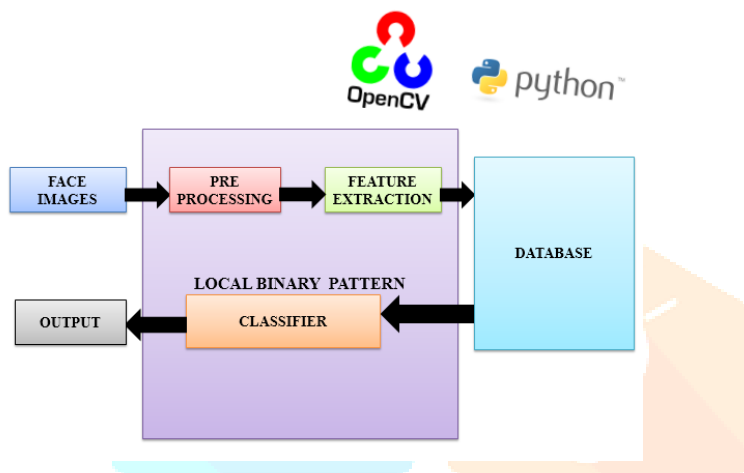


SOFTWARE BLOCK DIAGRAM



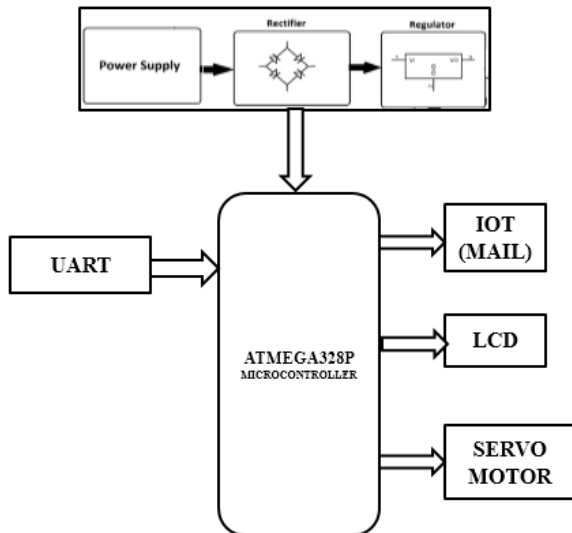
EXPLANATION:

- The images of the authorized person are trained into the processor by capturing images through camera.
- The images are stored in database for detecting the unknown persons.
- OpenCv acts as a tool for image processing and performing face detection of the unknown person.
- These processes are carried under machine learning platform and gives the detected output

**EXPLANATION**

- For unknown person detection and classification Local Binary Pattern (LBP) is used.
- The images are preprocessed. In preprocessing stage the image size, noise and color are modified as per the requirement for efficient face detection.
- The preprocessed image is given for feature extraction. Then the images are compared and classified with the images in database.
- The classified images gives the output as whether the person is authorized to enter.

HARDWARE BLOCK DIAGRAM



HARDWARE BLOCK DIAGRAM

HARDWARE EXPLANATION

This project is beneficial for security in any location. As described in the block diagram, first I photograph a UART in order to process the software procedure. In other words, compare the images at the camera to the photos in the database. If the images are matched, the servo motor will open the door. If the pictures are not matched, the picture sent to the mail through IOT, and shown on the LCD to the UNKNOWN PERSON ENTER.

METHODS

MODULE LIST

- Power Supply
- ATMEGA328P Microcontroller
- NodeMCU
- Lcd
- Servo motor Motor

MODULE DESCRIPTION

POWER SUPPLY

A power supply that converts AC line voltage to DC power must accomplish the following duties efficiently and affordably:

1. Rectification: Convert the incoming alternating current line voltage to direct current voltage.
2. Voltage transformation: Provide the proper DC voltage level.

3. Filtering: Smooth the rectified voltage's ripple.

4. Regulation: Maintain a steady output voltage level regardless of line, load, or temperature variations.

5. Isolation: Electrically isolate the output from the input voltage source.

6. Protection: Avoid destructive voltage spikes from reaching the output; supply backup power or shut down in the case of a brown-out. With 100% conversion efficiency, an ideal power supply would provide a smooth and consistent output voltage independent of differences in line voltage, load current, or ambient temperature. compares an actual power supply to an ideal power supply and defines several power supply concepts.

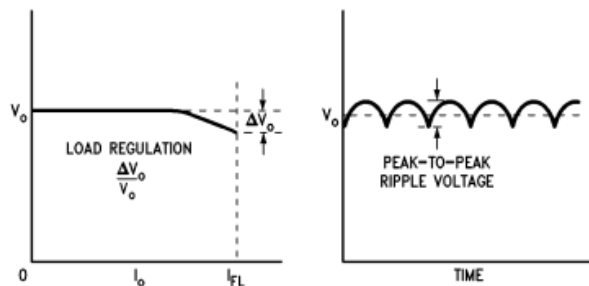


FIGURE. 1. Idealized Power Supply

LINEAR POWER SUPPLIES

Depicts two popular linear power supply circuits in use today. To decrease ripple voltage to capacitor C1, both circuits use full-wave rectification. Although the bridge rectifier circuit has a basic transformer, current must pass through two diodes. Because there is only one diode voltage loss, the center-tapped design is favored for low output voltages. Schottky barrier diodes are often used for 5V and 12V outputs because they have fewer voltage drops than equivalently rated ultra-fast kinds, increasing power conversion efficiency. Yet, for the same input voltage, each diode must resist double the reverse voltage that a diode experiences in a full-wave bridge.

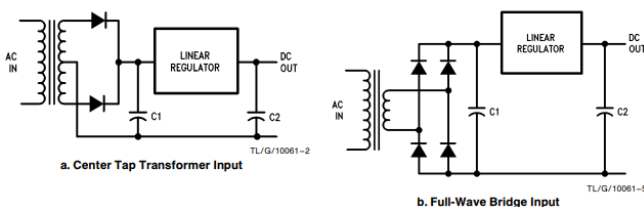
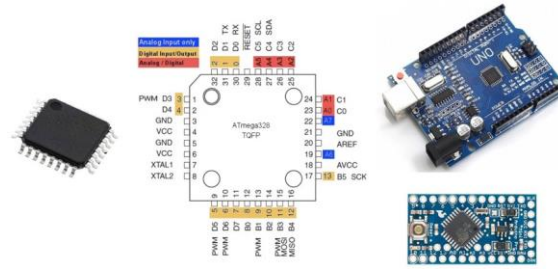


FIGURE 2. Linear Voltage Regulator

ARDUINO UNO

In contrast to microprocessors, microcontrollers often contain analog and digital pins that may be readily manipulated as input or output pins. Reading from a physical sensor is often realized as an input, whereas control or actuation is typically realized as an output. An analog and a digital pin are connected internally to an analog-digital converter (ADC), which has the capability of translating a range of voltages, such as 0-

3.3V, into a range of numerical values, such as 0-1023. In general, a digital pin can only have a LOW level (0V, for example) and a HIGH level (3.3V for instance). The popular ATmega328P 8-bit microcontroller used in the Arduino Uno, Nano, and ProMini boards is seen in the picture below.



From left to right, you can see the actual chip, the schematic with the pin arrangement, and finally the Arduino Uno and ProMini boards, which expose the microcontroller pins on header pins.

You must connect an analog physical sensor, such as an analog LM35DZ temperature sensor, to an analog pin. If you have a digital sensor, it indicates that the perceived value is represented by a digital coding of the value rather than a linear function of the voltage. Depending on the coding, you must drive (e.g. read) the digital pin to ascertain the numerical value. Nevertheless, this is commonly done using pre-written sensor or communication libraries, such as the OneWire library for digital sensors that use the OneWire protocol. If just the LOW and HIGH levels are utilized, a digital sensor can be linked to an analog pin. Nonetheless, unless otherwise indicated by the sensor or communication library, it is a good practice to utilize a digital pin for digital sensors. Anyone interested in a digital DHT22 sensor can examine the DHT.cpp file to discover how the DHT22 read function is implemented. To apply these kind of codes, one must first obtain the reference datasheet for the DHT22 sensor from the manufacturer.

NODEMCU



THE NODEMCU (NODE MICROCONTROLLER UNIT) IS AN OPEN-SOURCE SOFTWARE AND HARDWARE DEVELOPMENT ENVIRONMENT BASED ON THE ESP8266, A LOW-COST SYSTEM-ON-A-CHIP (SOC). THE ESP8266, CREATED AND BUILT BY ESPRESSIF SYSTEMS, HAS ALL OF THE ESSENTIAL COMPONENTS OF A COMPUTER: CPU, MEMORY, NETWORKING (WiFi), AND EVEN A CONTEMPORARY OPERATING SYSTEM AND SDK. AS A RESULT, IT IS A GOOD SOLUTION FOR INTERNET OF THINGS (IoT) PROJECTS. THE ESP8266 IS LIKEWISE DIFFICULT TO ACCESS AND USE. FOR THE SIMPLEST FUNCTIONS, LIKE AS TURNING IT ON OR SENDING A KEYSTROKE TO THE CHIP'S "COMPUTER," YOU MUST ATTACH WIRES WITH THE NECESSARY ANALOG VOLTAGE TO ITS PINS. YOU MUST ALSO PROGRAM IT IN LOW-LEVEL MACHINE INSTRUCTIONS THAT CAN BE UNDERSTOOD BY THE CHIP HARDWARE.

Using the ESP8266 as an embedded controller chip in mass-produced devices allows for this degree of integration. It is a significant burden for hobbyists, hackers, or students who wish to use it in their own IoT projects. For its adaptable IoT controller, the Arduino project produced an open-source hardware design and software SDK. The Arduino hardware, like NodeMCU, is a microcontroller board with a USB port, LED

lights, and standard data pins. It also specifies common interfaces for communicating with sensors or other boards. Nevertheless, unlike NodeMCU, the Arduino board may include a number of CPU chips (usually an ARM or Intel x86 chip), memory chips, and programming environments. With the ESP8266, there is an Arduino reference design.

LCD



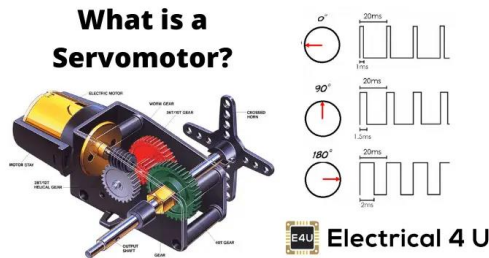
16 x 2 LCD is a type of electrical gadget that displays messages and data. LCD is an abbreviation for Liquid Crystal Display. The display is referred to as the 16 x 2 LCD since it has 16 columns and 2 rows. It can show (16 x 2=32) 32 characters in total, with each character made up of 5 x 8 Pixel Dots. These displays rely heavily on multi-segment light-emitting diodes. There are several display combinations available on the market, such as 8 x 1, 8 x 2, 10 x 2, 16 x 1, and so on, but the 16 x 2 LCD is the most commonly utilized. Because these LCD modules are inexpensive and easy to program, they are widely utilized in DIY circuits, gadgets, and embedded applications. These 16 x 2 LCD display modules have a fixed configuration of 16 columns and 2 rows. This module's initial row has a total of 16 columns numbered 0 to 15, and its position is 0. In addition, the second row comprises 16 columns numbered 0 to 15.

PIN CONFIGURATION

A register select (RS) pin that determines where in the LCD's memory data is written. You may choose between a data register, which stores what appears on the screen, and an instruction register, which is where the LCD's controller searches for instructions on what to do next. A Read/Write (R/W) pin that chooses either reading or writing mode. An enabling pin that allows writing to the registers 8 data pins (D0 - D7). When you write, the states of these pins (high or low) represent the bits you're sending to a register, or the values you're reading when you read. There is also a display contrast pin (Vo) and power supply pins (+5V and GND).

Backlight (Bklt+ and Bklt-) pins that may be used to power the LCD, alter the display contrast, and switch the LED backlight on and off.

SERVO MOTOR



A servo motor is a self-contained electrical device that rotates machine parts with high efficiency and precision. This motor's output shaft can be changed to a certain angle, location, and velocity that a standard motor cannot. The Servo Motor combines a standard motor with a sensor to provide positional feedback. The most significant component of the Servo Motor created and utilized exclusively for this purpose is the controller. The servo motor is a closed-loop system that uses location feedback to regulate rotational or linear speed and position. An electric signal, either analog or digital, controls the motor and defines the amount of movement that indicates the ultimate command position for the shaft.

Unlike traditional DC motors, servo motors are designed to rotate to a specific angle and maintain that position until a new command is given. Servo motors typically have a built-in feedback mechanism that allows them to adjust their position based on external factors such as load, temperature, or wear. This feedback can be achieved through various mechanisms such as potentiometers, encoders, or hall effect sensors. Servo motors are commonly used in robotics for tasks such as controlling arm movements, opening and closing grippers, and controlling the movement of wheeled robots. They are also used in many other applications such as CNC machines, cameras, and model airplanes.

CONCLUSION

User authentication is an important aspect of securing smart home environments. A secure and anonymous authentication scheme for smart home environmental conclusion should ensure that only authorized users can access the smart home environment and their identity is kept private. One approach to achieving this goal is through the use of anonymous authentication protocols that allow users to authenticate without revealing their identity. One such protocol is the zero-knowledge proof protocol, which enables a user to prove knowledge of a secret without revealing the secret itself. Another approach is the use of biometric authentication, such as fingerprint or facial recognition, which can provide a secure and convenient way for users to authenticate without having to remember passwords or carry authentication tokens. To enhance the security of the authentication process, multi-factor authentication can be employed, which requires users to provide multiple forms of identification such as a password and a biometric identifier. Additionally, the use of strong encryption protocols and secure communication channels can further ensure the confidentiality and integrity of the authentication process and protect against eavesdropping and data interception. Overall, a secure and anonymous user authentication scheme for smart home environmental conclusion should incorporate a combination of these approaches to provide a robust

and reliable authentication system that protects users' privacy and secures their access to the smart home environment.

ADVANTAGES

- YOLO is extremely fast
- Accuracy high
- Implement to any processor with its dependencies
- Low cost

DRAWBACKS

- Security camera is not operating correctly.
- Still the surveillance camera and watchman are only watching people inside the Bank locker room.
- If there is an issue or a crime within the ATM, they will be able to view the entire video and then decide on a remedy. Processing time is lengthy.

APPLICATION

- Indoor ,outdoor monitoring
- Person identification
- Animal monitoring
- Security systems

FUTURE WORKS

Zero-knowledge proof (ZKP):

In this scheme, the user can prove their identity to the system without revealing their identity information. The user generates a public key, and the system generates a challenge based on this key. The user responds with a proof that they have the private key corresponding to the public key. This way, the system can verify the user's identity without knowing any personal information.

Biometric authentication:

Biometric authentication uses unique physical characteristics of an individual to authenticate their identity. This scheme is secure and anonymous as the system only verifies the biometric information without knowing the individual's personal information.

Blockchain-based authentication:

Blockchain technology offers a secure and decentralized platform for user authentication. The system can create a blockchain-based identity for the user, and the user can authenticate themselves using their private key. This scheme ensures security and anonymity as the user's personal information is stored securely on the blockchain.

Pass wordless authentication:

Pass wordless authentication uses other factors like biometric information or device identity to authenticate the user. This scheme eliminates the need for passwords and ensures a secure and anonymous authentication process.

REFERENCES

- 1) Bhattacharjya, X. Zhong, J. Wang, and X. Li, "Present scenarios of iot projects with security aspects focused," in *Digital Twin Technologies and Smart Cities*. Springer, 2020, pp. 95–122.
- 2) K. Gopalakrishnan et al., "Security vulnerabilities and issues of traditional wireless sensors networks in iot," in *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Springer, 2020, pp. 519–549.
- 3) M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Computers & Security*, 2019.
- 4) B. Yu and H. Li, "Anonymous authentication key agreement scheme with pairingbased cryptography for home-based multi-sensor internet of things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.
- 5) Y. Lu and L. Da Xu, "Internet of things (iot) cybersecurity research: a review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.
- 6) V. Tsakanikas and T. Dagiuklas, "Video surveillance systems-current status and future trends," *Comput. Electr. Eng.*, Aug. 2018.
- 7) L. Patino, T. Nawaz, T. Cane, and J. Ferryman, "PETS 2017: Dataset and challenge," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Honolulu, HI, USA, Jul. 2017
- 8) G. Awad, A. Butt, J. Fiscus, D. Joy, A. Delgado, M. Michel, A. F. Smeaton, Y. Graham, W. Kraaij, G. Quénot, M. Eskevich, R. Ordelman, G. J. F. Jones, and B. Huet. (2018). *TRECVID 2017: Evaluating Ad-Hoc and Instance Video Search, Events Detection, Video Captioning, and Hyperlinking*.
- 9) V. Kumar, S. Jangirala, and M. Ahmad, "An efficient mutual authentication framework for healthcare system in cloud computing," *Journal of medical systems*, vol. 42, no. 8, p. 142, 2018.
- 10) M. Karthigaiveni and B. Indrani, "An efficient two-factor authentication scheme with key agreement for iot based e-health care application using smart card," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–12, 2019.