



# TRIGUARD: ADVANCED MULTI-VERIFICATION SYSTEM FOR BANK LOCKER SECURITY

S. SHOBANA, M.E.,  
Assistant Professor,  
Dept. of ECE,  
PERI-IT

Vadlamani dinesh,  
Vidhya.S,  
Saravana kumar.A,  
Dept of ECE,  
PERI IT.

**Abstract:** - In today's world, ensuring the security of personal belongings is paramount. Traditional lock and key systems are no longer sufficient to meet the evolving challenges of theft and unauthorized access. In response, our innovative locker system offers a comprehensive solution that integrates advanced biometric technology with traditional security measures. Firstly, our system employs facial recognition technology to verify the identity of the user, ensuring that only authorized individuals gain access to the locker. Secondly, fingerprint scanning adds an extra layer of security by verifying the unique biometric signature of the user. Finally, a keypad with a secret code provides yet another level of authentication, akin to a digital password known only to the user. Together, these three layers of security create a robust and foolproof system that guarantees the safety of personal belongings. Our locker system not only provides unparalleled security but also offers convenience and peace of mind to users, knowing that their possessions are safely stored away from prying eyes.

## I. INTRODUCTION

In today's world, ensuring the security of personal belongings is paramount. Traditional lock and key systems are no longer sufficient to meet the evolving challenges of theft and unauthorized access. In response, our innovative locker system offers a comprehensive solution. Consumer electronics include MP3 players, mobile phones, video game consoles, digital cameras, GPS receivers, and printers. Household appliances, such as microwave ovens, washing machines and dishwashers, include embedded systems to provide flexibility, efficiency and features.

that integrates advanced biometric technology with traditional security measures. Firstly, our system employs facial recognition technology to verify the identity of the user, ensuring that only authorized individuals gain access to the locker. Secondly, fingerprint scanning adds an extra layer of security by verifying the unique biometric signature of the user. Finally, a keypad with a secret code provides yet another level of authentication, akin to a digital password known only to the user. Together, these three layers of security create a robust and foolproof system that guarantees the safety of personal belongings. Our locker system not only provides unparalleled security but also offers convenience and peace of mind to users, knowing that their possessions are safely stored away from prying eyes.

An embedded system is a controller programmed and controlled by a real-time operating system (RTOS) with a dedicated function within a larger mechanical or electrical system, often with real-time consumption of embedded systems computing constraints.

It is embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. Ninety-eight percent of all microprocessors are manufactured to serve as embedded system component.

Examples of properties of typical embedded computers when compared with general-purpose counterparts are low power consumption,

small size, rugged operating ranges, and low per-unit cost. This comes at the price of limited processing resources, which make them significantly more difficult to program and to interact with.

However, by building intelligence mechanisms on top of the hardware, taking advantage of possible existing sensors and the existence of a network of embedded units, one can both optimally manage available resources at the unit and network levels as well as provide augmented functions, well beyond those available. For example, intelligent techniques can be designed to manage power.

Advanced HVAC systems use networked thermostats to more accurately and efficiently control temperature that can change by time of day and season. Home automation uses wired- and wireless-networking that can be used to control lights, climate, security, audio/visual, surveillance, etc., all of which use embedded devices for sensing and controlling.

Like traffic lights, factory controllers, and largely complex systems like hybrid vehicles, MRI, and avionics Embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations. Complexity varies from low, with a single microcontroller .

Embedded systems in automobiles include motor control, cruise control, body safety, engine safety, robotics in an assembly line, car multimedia, car entertainment, E-com access, mobiles etc.

- Embedded systems in telecommunications include networking, mobile computing, and wireless communications, etc.
- Embedded system in smart cards include banking, telephone and security systems.
- Embedded Systems in satellites and missiles include defence, communication, and aerospace

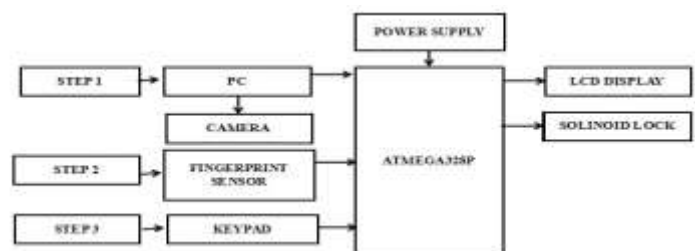


Fig: Block diagram



The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Revision 2 of the Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode. Revision 3 of the board has the following new features:

1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes. Stronger RESET circuit. Atmega 16U2 replace the 8U2. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

## II. WORKING PRINCIPLE

The principle behind the LCD's is that when an electrical current is applied to the liquid crystal molecule, the molecule tends to untwist. This causes the angle of light which is passing through the molecule of the polarized glass and also cause a change in the angle of the top polarizing filter. As a result, a little light is allowed to pass the polarized glass through a particular area of the LCD. Thus, that particular area will become dark compared to other. The LCD works on the principle of blocking light. While constructing the LCD's, a reflected mirror is arranged at the back. An electrode plane is made of indium-tin oxide which is kept on top and a polarized glass with a polarizing film is also added on the bottom of the device. The complete region of the LCD has to be enclosed by a common electrode and above it should be the liquid crystal matter.

Next comes to the second piece of glass with an electrode in the form of the rectangle on the bottom and, on top, another polarizing film. It must be considered that both the pieces are kept at right angles. When there is no current, the light passes through the front of the LCD it will be reflected by the mirror and bounced back. As the electrode is connected to a battery the current from it will cause the liquid crystals between the common-plane electrode and the electrode shaped like a rectangle to untwist. Thus, the light is blocked from passing through. That particular rectangular area appears blank.

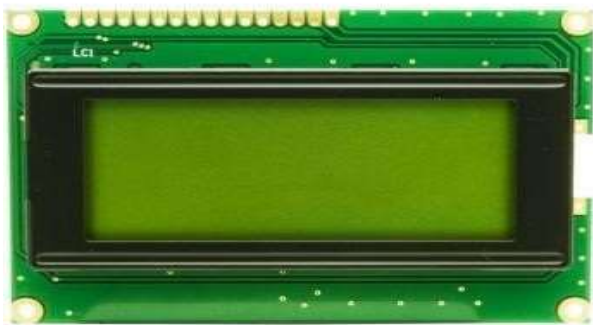
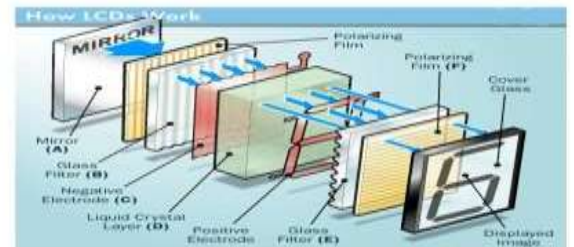


Fig LCD Display



- LCD consumes less amount of power compared to CRT and LED

Fig LCD layer Diagram

LCD are consisting of some microwatts for display in comparison to some mill watts for LED's

- LCD are of low cost.
- Provides excellent contrast.
- LCD are thinner and lighter when compared to cathode ray tube and LED.

## APPLICATIONS

- Liquid crystal technology has major applications in the field of science and engineering as well on [electronic devices](#).
- Liquid crystal thermometer
- Optical imaging
- The liquid crystal display technique is also applicable in visualization of the radio frequency waves in the waveguide
- Used in the medical applications

## ADVANTAGES

- LCD consumes less amount of power compared to CRT and LED
- LCD are consisting of some microwatts for display in comparison to some mill watts for LED's
- LCD are of low cost

- Provides excellent contrast
- LCD are thinner and lighter when compared to cathode ray tube and LED

### III. SOFTWARE PROCESS

Embedded C is most popular programming language in software field for developing electronic gadgets. Each processor used in electronic system is associated with embedded software.

Embedded C programming plays a key role in performing specific function by the processor. In day-to-day life we used many electronic devices such as mobile phone, washing machine, digital camera, etc. These all device working is based on microcontroller that are programmed by embedded C.

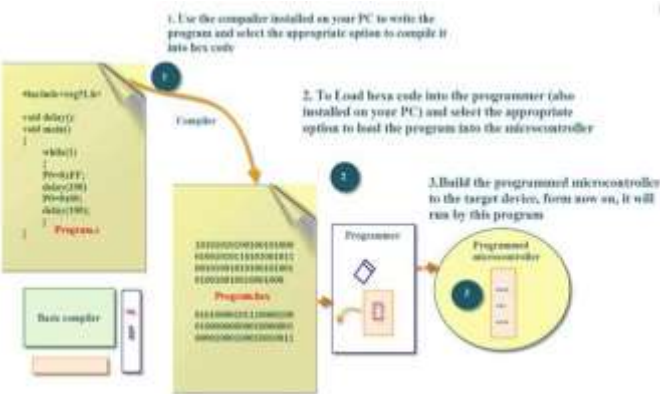


Fig 3.1 Block diagram of Embedded C

The Embedded C code written in above block diagram is used for blinking the LED connected with Port0 of microcontroller. In embedded system programming C code is preferred over other language. Due to the following reasons:

- Easy to understand
- High Reliability
- Portability
- Scalability

Function is a collection of statements that is used for performing a specific task and a collection of one or more functions is called a programming language.

Most consumers are familiar with [application software](#) that provide functionality on a computer. Embedded software however is often less visible, but no less complicated. Unlike application software, embedded software has fixed hardware requirements and capabilities, and addition of third-party hardware or software is strictly controlled.

Embedded software needs to include all needed [device drivers](#) at manufacturing time, and the device drivers are written for the specific hardware. The software is highly dependent on the CPU and specific chips chosen. Most embedded software engineers have at least a passing knowledge of reading [schematics](#), and reading data sheets for components to determine usage of registers and communication system. Conversion between [decimal](#), [hexadecimal](#) and [binary](#) is useful as well as using [bit manipulation](#).

Web applications are rarely used, although XML files and other output may be passed to a computer for display. File systems with folders are typically absent as are SQL databases.

The Arduino hardware and software were designed for artists, designers, hobbyists, hackers, newbies, and anyone interested in creating interactive objects or environments. Arduino can interact with buttons, LEDs, motors, speakers, GPS units, cameras, the internet, and even your smart-phone or your TV! This flexibility combined with the fact that the Arduino software is free, the hardware boards are pretty cheap, and both the software and hardware are easy to learn has led to a large community of users who have contributed code and released instructions for a **huge** variety of Arduino-based projects

There are many varieties of Arduino boards ([explained on the next page](#)) that can be used for different purposes. Some boards look a bit different from the one below, but most Arduinos have the majority of these components in common:



Fig 3.2 Arduino IDE Diagram

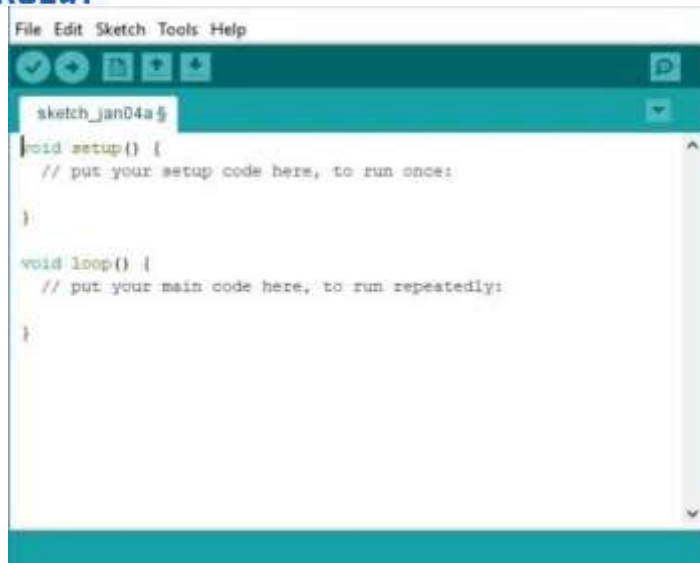


Fig3.3 .Arduino IDE Software diagram

The Arduino IDE supports the languages [C](#) and [C++](#) using special rules of code structuring. The Arduino IDE supplies a [software library](#) from the [Wiring](#) project, which provides many common input and output procedures.

User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub `main()` into an executable [cyclic executive](#) program with the [GNU toolchain](#), also included with the IDE distribution.

#### IV.EXPERIMENTAL RESULTS

**Facial Recognition:** Use a facial recognition library like OpenCV to detect and recognize faces.

**Fingerprint Scanner:** Utilize a fingerprint scanning library or hardware API to capture and verify fingerprints.

**Keypad Input:** Read input from a keypad and validate it against a pre-set secret code.

**Integration:** Integrate the three components to work together, ensuring they collectively authenticate the user.

**Access Control:** If all three authentication methods pass, unlock the locker; otherwise, deny access

- ★ The project aims to create a locker system that uses your face, fingerprint, and a secret code to make sure only you can access it. This provides extra layers of security to keep your belongings safe.
- ★ By using your face and fingerprint, the locker system offers a convenient and personalized way to access your belongings. You don't need to worry about forgetting keys or combinations, making it easy to use daily.
- ★ If someone unfamiliar tries to access your locker, the system automatically takes their picture and sends it to your email. This feature adds an additional level of security by keeping you informed about any unauthorized attempts to access your locker.

A face analyzer is software that identifies or confirms a person's identity using their face. It works by identifying and measuring facial

features in an image. Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images. Biometric security systems use facial recognition to uniquely identify individuals during user onboarding or logins as well as strengthen user authentication activity. Mobile and personal devices also commonly use face analyzer technology for device security.

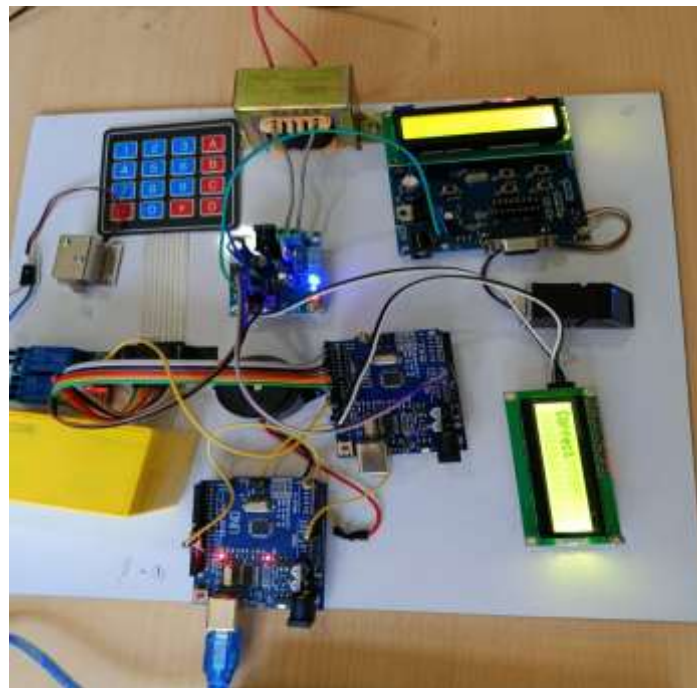


Fig 4.1 working of bank locker system

#### V.FUTURE WORK

1. **\*Biometric Authentication\*:** Enhancing TRIGUARD with biometric authentication such as fingerprint, iris, or facial recognition adds an extra layer of security, ensuring that only authorized individuals can access the bank locker.
2. **\*AI-based Anomaly Detection\*:** Utilizing artificial intelligence algorithms, TRIGUARD can learn and detect unusual patterns or behaviors associated with accessing the bank locker. This could include detecting unauthorized access attempts, abnormal frequency of access, or unusual opening times.
3. **\*Blockchain Technology\*:** Implementing blockchain technology can provide a tamper-proof and transparent audit trail for all access and transactions related to the bank locker. Each access attempt or transaction can be securely recorded on the blockchain, ensuring immutability and accountability.
4. **\*IoT Sensors\*:** Integrating IoT sensors within the bank locker system enables real-time monitoring of environmental conditions such as temperature, humidity, and tamper detection. This ensures that the contents of the bank locker remain safe and secure at all times, with alerts sent for any anomalies.
5. **\*Remote Access Management\*:** Offering remote access management



capabilities allows authorized users to securely access their bank locker from anywhere, using their mobile devices or computers. This enhances convenience for customers while maintaining robust security protocols.

6. \*Partnerships with Fintech Companies\*: Collaborating with fintech companies specializing in cybersecurity or emerging technologies like quantum encryption can provide access to cutting-edge solutions to further strengthen TRIGUARD's security features.

## VI.CONCLUSION

Our locker system embodies the pinnacle of security, combining cutting-edge technology with user-friendly access control measures. By integrating facial recognition, fingerprint scanning, and keypad authentication, we ensure that only authorized individuals gain access to their belongings. This multi-layered approach not only provides robust protection against unauthorized entry but also offers peace of mind to users, knowing that their valuables are safeguarded by a system that leaves no room for compromise. With our locker system, security isn't just a feature—it's a guarantee.

The implementation of a TriGuard Advanced and Multi-Verification System for bank locker security represents a significant step forward in ensuring the protection of valuable assets and sensitive information stored within bank lockers. By integrating multiple authentication methods such as biometrics, passwords, and tokens, the system offers a robust and multi-layered approach to security, significantly reducing the risk of unauthorized access.

Furthermore, the system's emphasis on user experience ensures that security measures are implemented without compromising convenience or efficiency for customers. Real-time monitoring and alerts, coupled with detailed audit trails, enable proactive threat detection and promote accountability and transparency within the bank locker system.

Compliance with regulatory requirements is ensured, bolstering the bank's reputation and credibility while mitigating legal risks. The system's adaptability to emerging threats, facilitated by machine learning algorithms, ensures continuous improvement and resilience against evolving security risks.

Overall, the TriGuard Advanced and Multi-Verification System delivers a comprehensive and effective solution that enhances security, improves user experience, ensures regulatory compliance, enables real-time monitoring and alerts, promotes accountability and transparency, adapts to emerging threats, and maintains resilience to failures. As such, it represents a valuable investment for financial institutions seeking to safeguard customer assets and uphold trust and confidence in their banking services.

## VII.REFERENCES

[1] Manohar, V.J., Paul, B. and Pranathi, M.S., 2023, May. A Novel Two Level Bank Security System using IoT based Controller. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 12821287). IEEE.

[2] Umadi, K.R., Aishwarya, A., Narendramath, J.E., Inchara, S.M. and

Dharishini, P.P.P., 2023, January. Smart E-Locker System using IoT. In *2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)* (pp. 41-45). IEEE.

[3] Yadav, A., Rana, F.K., Raj, G., Yadav, A., Sachan, A. and Bhardwaj, P.,

2022, April. Smart Door Locking System Using LoRa Technology. In *2022*

*10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22)* (pp. 1-5). IEEE.

[4] Venkatraman, S., Varshaa, R.R. and Vigneshwary, P., 2021, March. IoT based Door open or close monitoring for home security with emergency notification system using LoRa Technology. In *2021 7th International Conference on Advanced Computing and*

*Communication Systems*

(ICACCS) (Vol. 1, pp. 173-178). IEEE.

[5] Kshirsagar, A. and Patil, N., 2021, July. IoT based smart lock with predictive maintenance. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE. [6] Saritha, B., Bharadwaja, C.S., Nikhitha, M., Nethra Reddy, C.H., Arun, K. and Ahmed, S.M., 2022. An Intelligent Anti-Theft Vehicle Locking System Using IoT. In *ICDSMLA 2020: Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications* (pp. 15891595). Springer Singapore.

[7] Narkhede, A., Mapari, V. and Karande, A., 2021. Iot smart locker. In *Cybernetics, Cognition and Machine Learning Applications: Proceedings of ICCMCLA 2020* (pp. 1-7). Springer Singapore.

[8] Bhattacharya, S., Basak, S., Chakraborty, R., Dey, U., Chowdhury, N. and Hegde, R., 2022, February. Smart Lock Using IoT. In *2022 Interdisciplinary Research in Technology and Management (IRTM)* (pp. 1-4). IEEE.

[9] Dansana, D., Mishra, B.K., Sindhuja, K. and Sahoo, S., 2021. IoT-Based Smart Security System on a Door Lock Application. In *Next Generation of Internet of Things: Proceedings of ICNGIoT 2021* (pp. 695-703). Springer Singapore.

[10] Shanthini, M., Vidya, G. and Arun, R., 2020, August. IoT enhanced smart door locking system. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 92-96). IEEE.

