International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2125
***Article Received**: 30 November 2022 **Revised**: 10 January 2023 **Accepted**: 02 February 2023*

IOT based Security System for Auto Identifying Unlawful Activities using Biometric and Aadhar Card

Brijesh Nayyar[1], Dr. Vishal Goar[2]
PhD Scholar, Maharaja Ganga Singh University, Bikaner
(brijeshnayyar75@gmail.com)[1]
Assistant Professor, Engineering College Bikaner
(dr.vishalgoar@gmail.com)[2]

Abstract: In today's era, where thefts are consecutively increasing, especially in banks, jewelry shops, stores, ATMs, etc, there is a need to either develop a new system or to improve the existing system, due to which the security in these areas can be enhanced. However, the traditional methods (CCTV cameras, alarm buttons) to handle the security issues in these areas are still available, but they have lots of limitations and drawbacks. So, in order to handle the security issues, this paper describes how the biometric and IoT (Internet of Things) techniques can greatly improve the existing traditional security system. Our proposed system uses biometric authentication using the fingerprint and iris pattern with the strength of IoT sensors, microcontroller and UIDAI aadhar server to enhance the security model and to cut the need of keeping extra employees in monitoring the security system.

Keywords: Authentication, Biometric, aadhar, sensor, LED, Cloud database, Scanner.

I. Introduction:

Maintaining security in sensitive areas such as the banking system, ATM, military, jewelry shops, stores etc is a growing concern in our society. In such areas, any kind of misleading activity or robbery should be recorded, analyzed and reported to the concerned authority in order to track those unauthorized persons who had made the misleading activity. In our proposed system, the users first authenticate themselves using their aadhar card by providing the biometric data (fingerprint or the iris of the eye). After this, the user's biometric data will be sent to the cloud server as well as to the UIDAI aadhar server for storage and authentication respectively. If successful authentication happens, then the institution's door will be opened and the user is permitted to enter the institution, otherwise the door will remain closed. In case, if after successful authentication, any unlawful activity has been made by the user, then our system can track that user using his/her demographic and personal data, which can be extracted from the UIDAI aadhar server, based on user's stored biometric data and aadhar card number, which were provided by the user at the time of authentication process. So, in this manner, our proposed system can greatly improve the existing security system and also cuts the need to keep the extra employees in monitoring the security system.

II. Literature Survey:

Biometric-based security systems have become increasingly popular due to their high level of security and accuracy. Biometric authentication involves the use of unique physical characteristics such as fingerprints, iris scans, and facial recognition to verify the identity of a person. The use of biometrics in security systems ensures that only authorized persons are granted access to sensitive areas. IoT-based security systems are designed to monitor and protect assets and people by using connected devices. These devices collect and analyze data in real-time and can trigger alerts when suspicious activity is detected. The integration of biometric authentication and Aadhar card in IoT-based security systems provides an added layer of security and accuracy and it has gained significant popularity in recent years. With the advent of the Internet of Things (IoT), there has been an increasing interest in developing IoT-based security systems for automated identification of unlawful activities.

In this literature review, we will examine some of the existing research on the topic of IoT-based security systems for auto-identifying unlawful activities using biometric.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2125
***Article Received**: 30 November 2022 **Revised**: 10 January 2023 **Accepted**: 02 February 2023*

Sr.	Authors	Year	Title of Paper	Methodology	Remarks
1	Sri Shimal Das, Smt. Jhunu Debbarma	2011	Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian E-Banking system	Security, ATM, Biometric (Fingerprint), Crime, Verification, E-Banking, UML	This paper focuses on vulnerabilities and increasing wave of criminal activities occurring at ATMs, where quick cash is prime target for criminals rather than at bank themselves.
2	Anil K. Jain, Karthik Nanda kumar	2012	Biometric Authentication: System Security and User Privacy	Biometrics, enrollment, feature extractor, template, metric matcher	This paper presents the vulnerabilities found in biometric system and the possible measures to rectify them.
3	Suman Sengupta, Tutu Sengupta	2013	IRIS texture analysis, finger printing and signature verification for automatic data retrieval system using biometric pattern recognition system	Biometric, eyeprint, IRIS, unique identification code, pattern recognition, finger print sensor, swipe machine, signature verification, digitizers, scanners	This paper proposed a new biometric based combined smart card IRIS feature extraction system, finger printing and signature verification system, which can be successfully implemented for retrieval of individual's data.
4	Ambika Arora, Alpana Singh, Bhumija Singh and Narendra Kumar	2014	Bank locker system with IRIS enrollment security	Locking system, Keyboard, Microcontroller, IRIS scanner, RFID	They proposed a microcontroller based efficient method of security in bank lockers, houses, treasuries etc. They incorporated IRIS biometric recognition method with the RFID (radio frequency identifier) card for implementing their security system.
5	Prof R. Srinivasan, T. Mettilda, D. Surendhran, K. Gopinath, P. Sathishkumar	2015	Advanced locker security system	RFID, GSM, Conveyer, Microcontroller, Heat sensor	They proposed a microcontroller based automated locker security system based on RFID, password, CONVEYER, heat sensor and GSM technologies
6	Narmatha. K, Abinaya R, Jai Kishen Singh. G, Balaje. R	2016	Security for ATM machine using aadhar card, IRIS scanner and IOT	Aadhar card, IRIS scanner, face detectors, Internet of Things, Biometric, Vibration detection sensors	Proposed system presents a method of securing ATM machine using biometrics (finger print, IRIS), aadhar card, vibration detection sensors and IOT.
7	Aravinth. J, Gokilaprabha. P, Haribhuvaneshwaran. T, Yogeshwaran. R, Mrs. Aiswarya. S	2016	Bank locker security system using IOT	Respberry pi-2 model B, Signal conditioning unit, Ethernet, SD-card, GSM, Smart phone	Proposed system provides a method for secure access only to authorized user via SMS and captured image by Raspberry Pi.
8	Dhvani Shah, Vinayak Bharadi	2016	IOT based biometric implementation on Raspberry Pi	IOT, Raspberry Pi (Rpi), Cloud, Biometrics, Biometric Security, Cryptography, AES-256 Encryption	This paper proposed that how biometrics can take benefit of cloud's boundless computational resources and its properties to reduce the cost of biometric system requirements while enhancing the performance of biometric system using Respberry Pi, act as a remote enrollment node.
9	Annies Joshy, Jalaja M.J.	2017	Design and Implementation of IOT based secure biometric authentication system	Authentication, IRIS recognition, IOT, blowfish, RSA, aadhar database, time and attendance system	Proposed system presents a method to provide a secure and reliable biometric authentication system based on IOT.
10	Sandip Dutta, Nitin Pandey, Sunil Kumar	2018	Microcontroller based bank locker security system using	IRIS Scanner, Vein Scanner, Locker, Microcontroller,	This paper proposed a microcontroller based system for user authentication by

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 9 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v9i1.2125
***Article Received**: 30 November 2022 **Revised**: 10 January 2023 **Accepted**: 02 February 2023*

Sr.	Authors	Year	Title of Paper	Methodology	Remarks
	Khatri		IRIS scanner and Vein scanner	Biometrics, Wireless motion sensor (PIR sensor), Digital lock, Unique identification number	means of IRIS scanner, Vein scanner, Digital lock and unique identification number (aadhar card, driving license, voter Id card, etc) for bank locker. The proposed system also detects any human movement and subsequently raise an alarm, while the bank is closed.
11	Satvik Gogineni, K Marimuthu, Syed Amma Sheik	2018	IOT based centralized bank security system for monitoring and auto arresting	Microcontroller, Alarm, Sensors (PIR, IR, Smoke, Fire, Gas sensors), ATM, Web monitoring system, LAN	This paper proposed an IOT based system for alerting theft and to auto arrest the thief in bank or ATM itself from centralized monitoring unit.
12	J.S. Vimali, Senduru Srinivasulu, Gowri. S	2019	IOT based bank security system	Fire & smoke sensor, camera, PIR Sensor, wireless transmitter, GSM	Proposed system uses microcontroller with different sensors (PIR, smoke or fire) to recognize or perceive unauthorized activities inside the bank or ATM.
13	Wencheng Yang, Song Wang, Guanglou Zheng, Jucheng Yang, Craig Valli	2019	A privacy preserving lightweight biometric system for internet of things security	Biometric, fingerprint biometric authentication, MCC algorithm of authentication, block based XOR operation	This paper proposed a privacy preserving lightweight biometric system, for resource limited IOT devices to save memory and computational cost.
14	Gaurav Meena and Sarika Choudhary	2019	Biometric authentication in internet of things: A conceptual view	IOT, IRIS recognition, biometric authentication, SIFT, HCT, BFO, FAR, FRR accuracy matrices, neural network	This paper presents the conceptual idea of securing internet of things network using biometric authentication with IRIS recognition.
15	J. Thirumalai, Gokul R.,Ganasekaran P, Manlellore Murli M, Jackson Jublience Joseph L	2020	An IOT based bank locker security system	Internet of Things, sensors, security, GSM, fingerprint, Arduino UNO, RFID	Proposed system presents a method automated safety vault with double layered defense mechanism in order to prevent any unauthorized access to the vault.
16	Dnyaneshwari P. Wagh, H.S. Fadewar and G.N. Shinde	2020	Biometric finger vein recognition methods for authentication	Biometrics, Security, Light reflection method, Light transmission method	This paper compares various techniques of biometric authentication methods with main emphasis on finger vein identification or authentication.
17	Arvasu Chikara, Pallavi Choudekar, Ruchira and Divya Asija	2020	Smart bank locker using fingerprint scanning and image processing	Face recognition, Fingerprint Scanning, Security, Atmega32, WebCam, LCD	They proposed a microcontroller (Arduino) based automated system to improve the safety of lockers in the banking sector as bank safety is an important concern at present.
18	Shweta Agrawal, Subhashis Banerjee, Subodh Sharma	2020	Privacy and Security of Aadhar: A Computer Science Perspective	Privacy, Security, Cryptography, Authentication, Identification	This paper does in depth analysis of the aadhar system, used in biometric authentication. This paper discusses Privacy and security requirements, vulnerabilities in aadhar system, functional architecture of aadhar system, various entities involved in aadhar system and many other things what we need to know about the complete functioning of aadhar system.

Existing Security System: Traditional security systems are under the surveillance of CCTV cameras, alarm and emergency buttons etc and to capture any unlawful activities in these sensitive regions, CCTV cameras are mainly used. In such systems however, we have CCTV cameras for recording videos of all unlawful activities, but it will become very difficult to track the invaders as we don't have any kind of concrete record such as name, address, age, etc of them. Also, CCTV cameras need to be watched continuously regardless of day and night by some individual, which is time consuming and troublesome work especially in night times or off banking hours. In addition, the alert emergency button needs to be pressed manually. Therefore, a very rigid and vigilant human intervention for 24*7 is a very cumbersome task.

Proposed Security System: To overcome the problems associated with traditional authentication methods, we can use biometric authentication methods for implementing security. There are various kinds of biometric authentication methods such as fingerprint, finger vein, face, IRIS, palm, etc but in our proposed system we have used the fingerprint and IRIS recognition biometric methods for the authentication of an individual. So, if we bound an individual to first authenticate using his/her biometric data, before entering in an area where security is a prime concern and subsequently record that individual's biometric data in some cloud or local database then it will definitely enhance the security of our system because if we have the individual's biometric data then we can extract that individual's demographic and personal data from the CIDR (Central Identities Data Repository) - A centralized database of aadhar, managed by UIDAI (Unique Identification Authority of India), where biometric and demographic data is stored of every registered citizen of India. Keeping in mind the idea of authenticating the individual and maintaining the individual's biometric data, so that the individual can be tracked using his/her demographic and personal data extracted from the CIDR server, we developed our proposed system.

Components employed in our proposed security system: In our proposed system, we are employing the following components or modules to prevent and to record any kind of unlawful activities which may possibly happen in the institution.

1. Arduino microcontroller
2. Biometric scanners (eye IRIS and Fingerprint): For simplicity we call the scanner which is situated inside the institution as "inside scanner" and the scanner which is situated outside the institution, in front of the door, as "outside scanner".
3. Automatic open/close mechanism based door
4. IR Sensor
5. Cloud Database
6. RFID (Radio frequency identification) reader
7. LED (display console)
8. Keypad
9. Alarm or Buzzer
10. GSM module
11. AUA (authentication user agency) module.

Description of components employed in our proposed security system: In our proposed system, we are using the Arduino microcontroller. Arduino microcontroller is a low-cost, flexible, and easy-to-use programmable open-source microcontroller board that can be integrated into a variety of electronic projects. This board can be interfaced with other Arduino boards, Arduino shields, Raspberry Pi boards and can control relays, LEDs, servos, and motors as an output. Programs can be loaded onto it from the easy-to-use Arduino IDE.

Two biometric scanners (one is placed outside the institution and other is placed inside the institution) are equipped with the keypad which are used to read the biometric data of a user and to read his/her respective aadhar card number, entered by that user using the keypad of the scanner. These scanners are able to read the biometric traits of the user using a fingerprint scanner as well as using IRIS scanner (if the fingerprint of some user is not recognized properly).

There is an automatic open/close mechanism based door in our proposed system, which is very much similar to the door employed in the elevator of a building or the door of a metro train, but in our proposed system it must be controlled by commands from the microcontroller.

The IR sensor equipped with the gate is used to count the number of persons passed through the gate from outside to inside the institution or bank.

Log records are also maintained in our cloud database to keep track of all those individuals who entered the institution. This cloud database will store the aadhar card number of all authenticated individuals who had entered the institution at a particular date and time. In case, any unlawful activity happens in the institution, the stored information can be used to track the intended individual. Here, we store the individual's information in a cloud database rather than in the local database as there may be more chance that information stored in the local database can be lost due to some kind of catastrophic failures.

For those individuals who are illiterate or are physically handicapped and therefore can't type their aadhar card number using the keypad every time they enter in the institution, there exists a provision for them in our proposed system that they can use their RFID tag in which their aadhar card number is stored electronically. This RFID tag is read by the RFID scanner which is equipped with the scanner.

A display console is also used in our proposed system to show the entered aadhar card number by the individual and also to show the status of whether the authentication of the individual is successful or not.

For entering the information from the individual a keypad is also employed in our proposed system.

A buzzer component will raise an alarm in case any misleading activity happens or possible to happen.

Using the GSM module, a signal or SMS is sent to the concerned authority of the institution as well as to the nearby police station in order to inform about any unlawful activity.

An AUA module to send the biometric data and aadhar card number of an individual to UIDAI (Unique Identification Authority of India) database server known as CIDR (Central Identities Data Repository), where the aadhar card number and biometric as well as demographic data of each individual is stored. The UIDAI manages the CIDR and provides identification and authentication services with yes/no answers to the requesting AUA. An AUA is required to enter into a formal contract with UIDAI to be able to use aadhar authentication services. Examples of AUAs are banks, various state and central government ministries providing services such as the Public Distribution System (PDS), the Natural Rural Employment Guarantee Act (NREGA), and even private agencies like mobile phone operators.

III. Methodology:

We will develop a security system to address the identified research gaps. The sequences of steps that will be followed to build our proposed security system are as follows:

- ➢ An individual will first scan his/her biometric data (either fingerprint or IRIS)
- ➢ After this, the individual enters his/her aadhar card number.
- ➢ The individual's biometric data will then be stored in the local/cloud database and a request will also be sent to the UIDAI server for matching the individual's biometric data with his/her aadhar card number.
- ➢ If individual's authentication is successful from the UIDAI server, then he/she will be allowed to enter in the institution otherwise he/she will be denied to enter in the institution.
- ➢ If there is a case that some unlawful activity has been made by some authenticated individual then his/her biometric data, stored in our cloud database can be used to track his/her demographic and personal data extracted from CIDR server.
- ➢ Also, at every stage of entry and exit point in our proposed system we will use different kinds of sensors to record every possible activity which may indicate any misleading activity possibly happened to occur.
- ➢ These sensors will sense the data and send it to the microprocessor. The microprocessor will then act accordingly and direct our system for performing certain actions e.g. alert the concerning authority about the unlawful activity in the institution.

Working of our proposed system: In our proposed system, we have used an Arduino microcontroller as a central control unit which gives commands to different components employed in our proposed security system and hence controls the entire working of our proposed security system. When some individual wants to enter the institution or in the bank, then first he/she is required to authenticate himself/herself using the biometric scanner placed outside the institution. For this, the individual first scans his/her biometric trait which may be either fingerprint or the IRIS and then the individual enters his/her aadhar card number using the keypad or scans his/her RFID tag in which the individual's aadhar card number is stored. After this, an authentication request is sent using the AUA (authentication user agency) module to UIDAI (unique identification authority of India) server to match the details provided by the individual with the details already stored on the UIDAI server for verifying the authenticity of the individual. Once the individual has been authenticated successfully from the UIDAI server, the institution's door will be opened and the individual can go inside the institution.

In our proposed system, we have also provided a provision to enter more than one individual at once in the group, through the opened gate (especially in cases where some old man or some handicapped person needs assistance from his/her friend/relative). To achieve this functionality, the outside scanner which is equipped with the console, first asks the number of individuals which needs to be authenticated from the UIDAI server. Once the individual provides this information, the outside scanner equipped with RFID card reader and keypad is ready to scan and read the biometric data and aadhar card number respectively from each individual one by one. When all individuals are authenticated successfully, the door of the institution will be opened and they can go inside the institution.

As individuals are passing through the opened gate in the institution, the IR sensor counts them. This count is read by the scanner which is placed inside the institution. This scanner is similar in terms of design and working to the scanner placed outside the institution. The inside scanner will now wait up to the specified time limit for all those same individuals who recently came inside the institution by the process of authentication through the outside scanner or counted by the IR sensor in order to re-authenticate those same individuals using their biometric traits.

As long as the door remains open the inside scanner will be disabled and will not react to any kind of external events, i.e. the inside scanner is not able to recognize the biometric trait of individuals, but its countdown timer will keep running in the background. Also, the outside scanner will not read the biometric data of individuals until the inside scanner has completed all its pending authentication, so in this manner no one can open the closed door by authenticating himself/herself from the outside scanner.

Once the door is closed, the inside scanner becomes active and is ready to scan the biometric of individuals who have recently entered the institution. Also, once the inside scanner has been successfully authenticated all those same individuals, within a certain time interval, who recently came inside the institution by the process of authentication through the outside scanner or counted by the IR sensor, the outside scanner can react to user's input i.e. can read the biometric trait and aadhar card number of individual.

After expiration of the background timer of the inside scanner, the buzzer component will raise an alarm automatically, in order to alert the concerning authority of the institution about the event that there may be a chance of happening some misleading activity, which might be possible due to the fact that either the gate is still open, because someone is deliberately standing between the gate and don't want that the door be closed or there may be a situation that the door is closed but someone's authentication has remain pending by the inside scanner.

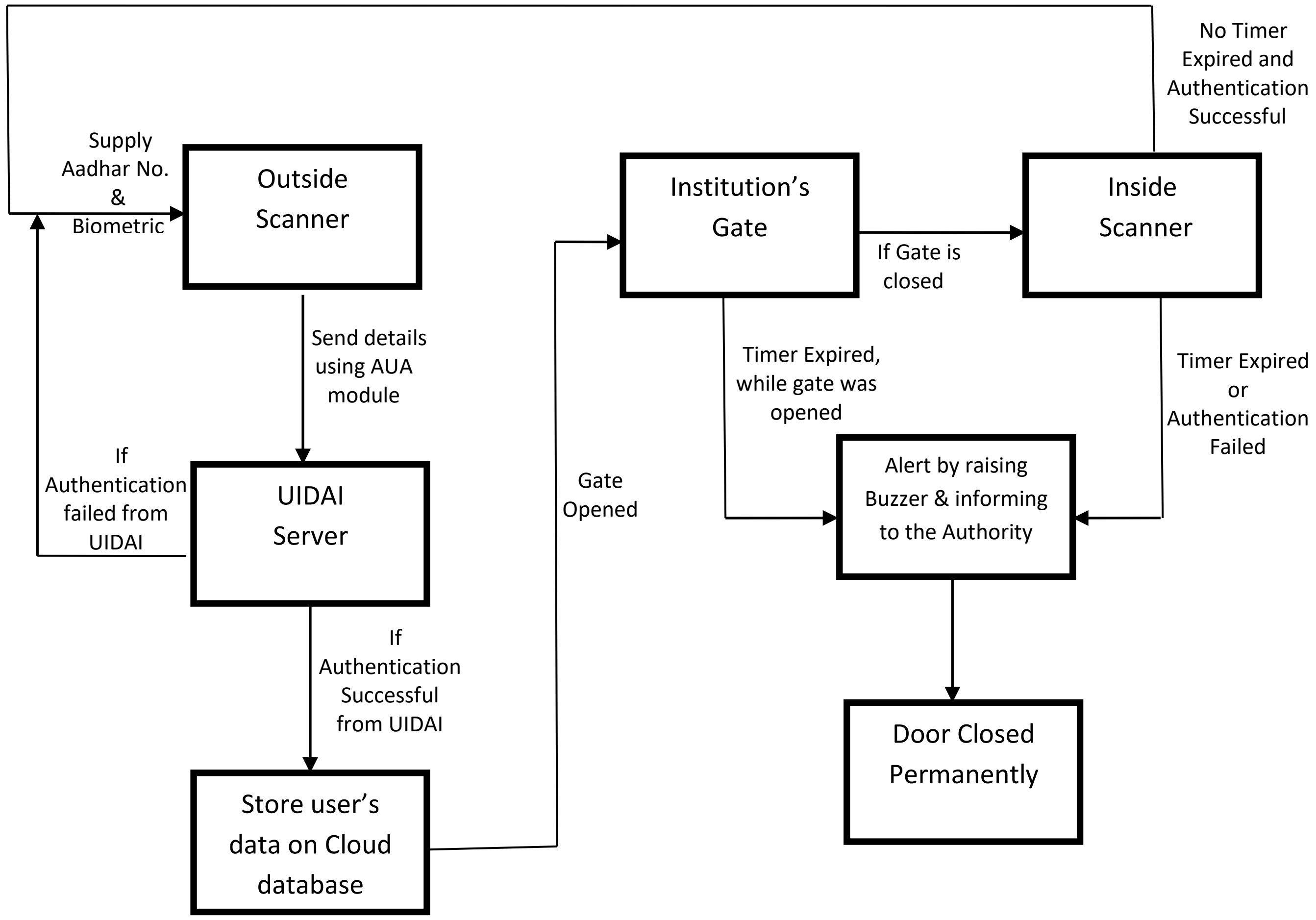
In this manner, if some unlawful activity has been happened in the institution by some intruder or unauthenticated individual, then his/her authentication will remain pending from the inside scanner thereby after a certain time limit the buzzer will raise an alarm, the door is locked permanently and an alert message will be sent to the concerned authority as well as to the nearby police station using the GSM technology.

Moreover, if the unlawful activity is getting performed by some authenticated person, then the individual's aadhar card information such as name, address, etc can be extracted from his/her aadhar card number which was stored in the cloud database of the institution, during the process of authentication. So later on, that individual can be tracked easily from his/her demographic and personal data extracted from the CIDR server using his/her stored aadhar card data. Thereby enhancing the security of our proposed system.

If there is a case that while the gate was opened for the entry of an authenticated individual, but some unauthenticated individual has also entered the institution with that authenticated individual through the opened gate, then our proposed system's IR sensor which keeps on monitoring the number of individuals passing through the opened gate in the institution will pass a value which denotes the count of individuals entered through the open gate at a particular moment, to the inside scanner. As a result of this, the inside scanner will now wait up to the specified time limit for all those same individuals who recently came inside the institution by the process of authentication through the outside scanner or counted by the IR sensor in order to re-authenticate those same individuals using their biometric traits. But for the unauthenticated individual who had entered the institution the inside scanner's timer will expire and ultimately the buzzer will raise an alert signal and at the same time a notification will also be sent to the concerned authority as well as to the nearby police station. The door is locked permanently and our system is in safe state.

In order to take the exit from the institution, the individual has to manually press the button which is equipped with the institution's gate. The exit button of the gate can only be pressed from inside and also only when our proposed system is running normally. On the other hand, if somehow our proposed system detects and reports any unlawful activity, then the exit button of the gate will not work in any manner unless the system gets a signal to open the gate from the concerned authority.

The **flow diagram** to represent the overall working of our proposed system is shown as under:


Supply Aadhar No. & Biometric
Outside Scanner
Send details using AUA module
If Authentication failed from UIDAI
UIDAI Server
If Authentication Successful from UIDAI
Store user's data on Cloud database
Gate Opened
Institution's Gate
If Gate is closed
Inside Scanner
No Timer Expired and Authentication Successful
Timer Expired, while gate was opened
Timer Expired or Authentication Failed
Alert by raising Buzzer & informing to the Authority
Door Closed Permanently

Future Scope: The future scope of an IoT-based security system for auto-identifying unlawful activities using biometric and aadhar card authentication is immense. As technology continues to advance, the system can be further enhanced to provide even more robust security measures. Here are some potential future advancements that can be made in this area:

1. Integration with Machine Learning: The integration of artificial intelligence (AI) and machine learning (ML) algorithms into the system would enable the system to learn and adapt to new threats and suspicious activities, making it even more effective in identifying potential threats.
2. Blockchain Integration: Another future scope could be the integration of blockchain technology to enhance the system's security and data privacy. Blockchain technology could help to create a tamper-proof record of all authentication and identification transactions, ensuring that any attempt to tamper with the system is immediately detected.
3. Global Implementation: The use of Aadhar card authentication can be extended globally, with each country having its own unique identification system.
4. Furthermore, the IoT-based security system can be integrated with various smart devices such as

smartphones, wearables, and smart homes to create a comprehensive security network. This would enable individuals to have complete control over their security and would allow them to monitor and control access to their personal spaces in real-time.

5. Multimodal Biometrics: Combining multiple biometric modalities such as facial recognition, voice recognition, and fingerprint scanning can make the identification process more reliable and efficient.
6. Use in Other Fields: The application of this system can be extended to various industries, such as healthcare, transportation, and hospitality, to enhance security and prevent unlawful activities.

Overall, the future scope of an IoT-based security system for auto-identifying unlawful activities using biometric and Aadhar card authentication is promising. It has the potential to transform security measures across various industries and enhance the accuracy and reliability of identifying unlawful activities.

IV. Conclusion:

In conclusion, the development of an IoT-based security system for auto-identifying unlawful activities using biometric and Aadhar card is a promising approach to improving security measures. Therefore, an IoT-based security system that employs biometric technology and Aadhar card authentication has the potential to revolutionize security measures in various fields, including law enforcement, banking, and other high-security areas. This system would enable quick and accurate identification of individuals, reducing the risk of unauthorized access and unlawful activities. By integrating biometric data and Aadhar card details with the IoT system, it becomes possible to identify and track any unauthorized or suspicious activity, such as burglaries, thefts, or unauthorized access attempts, in real-time.So, the Aadhar card authentication would enhance the system's reliability, ensuring that only authorized individuals have access to sensitive information or areas. Overall, the use of an IoT-based security system for auto-identifying unlawful activities using biometric and Aadhar card authentication has the potential to improve security and reduce crime rates.

References

[1] Sri Shimal Das, S. J. (2011). Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. *International Journal of Information and Communication Technology Research*.

[2] Anil K. Jain, K. N. (2012). Biometric Authentication: System Security and User Privacy. Identity Science (IEEE).

[3] Suman Sengupta, T. S. (2013). IRIS Texture Analysis, Finger Printing and Signature Verification for Automatic Data Retrieval System using Biometric Pattern Recognition System. International Journal of Advances in Computing and Management.

[4] Ambika Arora, A. S. (2014). Bank Locker System with IRIS Enrollment Security. International Journal of Engineering & Scientific Research (IJESR).

[5] Prof. R. Srinivasan, T. M. (2015). Advanced Locker Security System. International Conference on Information Engineering, Management and Security (ICIEMS).

[6] Narmatha. K, A. R. (2016). Security for ATM Machine using Aadhar Card, IRIS Scanner and IOT. International Journal of Engineering Science Invention Research & Development.

[7] Aravinth. J, G. P. (2016). Bank Locker Security System using IOT. IOSR Journal of Computer Engineering (IOSR-JCE) .

[8] Dhvani Shah, V. B. (2016). IOT Based Biometric Implementation on Raspberry Pi. ScienceDirect (Elsewire).

[9] Annies Joshy, J. M. (2017). Design and Implementation of IOT based Secure Biometric Authentication System. IEEE Spices.

[10] Sandip Dutta, N. P. (2018). Microcontroller based Bank Locker Security System using IRIS Scanner and Vein Scanner. Proceedings of International Conference on Inventive Research in Computing Applications (ICIRCA).

[11] Satvik Gogineni, K. M. (2018). IOT based Centralized Bank Security System for Monitoring and Auto Arresting. Research India Publications.

[12] J.S. Vimali, S. S. (2019). IOT based Bank Security System. International Journal of Recent Technology and Engineering (IJRTE).

[13] Wencheng Yang, S. W. (2019). A Privacy Preserving Lightweight Biometric System for Internet of Things Security. IEEE Communication Magazine.

[14] Choudhary, G. M. (2019). Biometric Authentication in Internet of Things: A Conceptual View. Journal of Statistics and Management Systems.

[15] J. Thirumalai, G. R. (2020). An IOT based bank locker security sytem. Journal of Engineering Research and Technology (IJERT).

[16] Dnyaneshwari P. Wagh, H. F. (2020). Biometric Finger Vein Recognition Methods for Authentication. Springler Nature Singapore Pte Ltd.

[17] Arvasu Chikara, P. C. (2020). Smart Bank Locker using Fingerprint Scanning and Image Processing. International Conference on Advanced Computing & Communication System (ICACCS).

[18] Shweta Agrawal, S. B. (n.d.). Privacy and Security of Aadhar: A Computer Science Perspective.