

IOT PRISION BREAK MONITORING AND ALTERING SYSTEM

Submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in Electronics and Communication Engineering

by

K.PRUDVI HARI (Reg.No.40130106)

K.SURYA KIRAN (Reg.No.40130095)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS**

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

CATEGORY-1 UNIVERSITY BY UGC

Accredited with Grade "A++" by NAAC | 12B Status by UGC| Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL - 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **K.PRUDVI HARI (40130106)** and **K.SURYA KIRAN (40130095)** who carried out the project entitled **"IOT BASED PRISON BREAK MONITORING AND ALERTING SYSTEM"** under our supervision from November 2023 to April 2024.

Internal Guide

Dr. S. LAKSHMI M.E, Ph.D,
Professor

Head of the Department

Dr. T. RAVI, M.E, Ph.D.,
Professor

Submitted for Viva voce Examination held on 17 April 2024

Internal Examiner

External Examiner

DECLARATION

I, PRUDHVI HARI.K (41030106), hereby declare that FINAL YEAR PROJECT REPORT entitled "IOT PRISON BREAK MONITORING AND ALTERING SYSTEM" done by me under the guidance of **Dr. S. Lakshmi M.E., Ph.D.**, Professor, is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Electronics and Communication Engineering.

DATE: 17-04-2024

PLACE: CHENNAI

K. Prudhvi Harik

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to The **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **DR. N. M. NANDHITHA, M.E., Ph.D., DEAN, SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING** and **DR. T. RAVI, M.E., Ph.D., HEAD OF THE DEPARTMENT, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING** for providing me necessary support during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.S.Lakshmi M.E, Ph.D, Professor, Dept. of Electronics and Communication Engineering**, for her valuable guidance, suggestions, and constant encouragement for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Electronics and Communication Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

We have surveillance systems for protection of public places such as banks, shopping malls, homes, etc. from robbers, and other negative people. People are well acquainted with current security systems of the Indian jails. There are some system like CCTVs, drones and guards are used to monitor the activities of the jail, But as these security systems are not sufficient to monitor all such criminal activity and surely ensure that there is no such chance of the escaping of these prisoners from the prison. There are also many problems associated with the modern security systems, Some of them which are detected issues with these CCTVs are that: not having proper clear images at night, unsaturated camera footage, disturbing videos, visible horizontal lines on videos, no video signal is available sometime, recording system is not their by DVR, starting some false alarms with not proper cause, bright spots on the monitor, etc. By These troubles there are the situation that can be created in the jails where prisoner can get a chance to flee as well as can cause any unexpected activities inside the jail, also deployment of these techniques is quite costlier. Many systems are introduced before have to fulfill this demand that generally use equipment such as lot , Bluetooth, GSM, GPS but these systems are not steady and can be affected by cyber-attacks, which will be the issue of the safety. Now we came up with this project with an idea to design an advanced and reliable , safe fix for this problem of this situation. Motive behind our device is to implement an safe and monitored environment in the prison that supervise the motion of the prisoners and the outsiders and overcome the problem present with the security modules available in the market previously.

CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
3	EXISTING METHOD	6
4	PROPOSED METHOD	7
	4.1 Hardware requirements	8
	4.2 Open problems in existing method	10
	4.3 Flow chart	11
	4.4 Implementation	12
	4.5 Aim and Scope	15
	4.6 Working	17
	4.7 Customization and Adaptability	18
	4.8 Limitations	22
5	RESULT AND DISCUSSION	35
6	CONCLUSION AND FUTURE SCOPE	38
	6.1 Conclusion	38
	6.2 Future Scope	38
	REFERENCES	40

LIST OF FIGURES

FIGURE NO	FIGURE NAME	PAGE NO
3	Block diagram of the existing method	6
4	Block diagram of the proposed method	8
4.3	Flow chart	11
4.4	Receiver section	14
5.1	Output 1	35
5.2	Output 2	35
5.3	Output 3	36
5.4	Output 4	36
5.5	Overall output	37

CHAPTER - 1

INTRODUCTION

Project's main aim is detect movement or status of behavior of prisoner's inside prison , whether they are in the premise area or not ,or their any unusual activity is affecting safety of prison or not . For this purpose, Geofencing has been done and to fail the idea of escaping, laser is used . This Project is based on Prison Security and Safety devices that are made by using Wi-Fi, Bluetooth for Internet as communication mode, GPS and GSM for SMS as communication mode for communication between higher authority and prison alert system. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. Further we have known the Project and proposes a new problem statement based on the overlook of the currently used systems and gives the future aspects of the give project. As we know The prison system in India is not as good as we are known by our cinema, our by diplomatic debate related to politics .In the era of everything digitally present in our country India, we are so orthodox about our safety, that prison system are not updated, also no concern is shown at present time also about related to safety upgradation of prison. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome

as we know we can rely more on machines for being perfectionist we should engage with this system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. The digital system to be used can be made reliable that it can't be under cyber attack, as there are people who want to deform the government authority, and some want to support prisoner for their particular motive. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with this system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized, by which it will be more safe and reliable system. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system. After knowing the currently available system it will clarify the points that should be examined to design an efficient setup, after which we will work on it. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease its efficiency. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly

populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. Correctional facilities play a crucial role in maintaining societal order by securely confining individuals who have been convicted of crimes. However, ensuring the security and safety of both inmates and staff within these facilities poses significant challenges. Prison breaks and unauthorized activities can have severe consequences, including threats to public safety and compromised justice systems.

In recent years, advancements in technology, particularly in the realm of the Internet of Things (IoT), have offered new opportunities to enhance prison security through continuous monitoring and real-time alerting systems. By leveraging IoT devices such as sensors, cameras, and communication networks, correctional facilities can establish proactive monitoring mechanisms to detect and respond swiftly to security breaches.

This report introduces an IoT-based Prison Break Monitoring and Alerting System designed to address the inherent security challenges faced by correctional facilities. The system aims to provide comprehensive monitoring of prison environments, early detection of security threats, and prompt alerting mechanisms to enable timely intervention by prison authorities.

In this report, we will delve into the architecture, functionality, benefits, and implementation of the IoT-based prison break monitoring and alerting system. Through an in-depth analysis of its components and capabilities, we aim to demonstrate how this innovative solution can significantly improve the security posture of correctional facilities and ensure the safety of inmates, staff, and the community at larger.

By harnessing the power of IoT technologies and proactive monitoring strategies, correctional facilities can strengthen their defenses against security breaches and uphold their mandate of maintaining secure and orderly environments conducive to rehabilitation and justice.

CHAPTER - 2

LITERATURE SURVEY

Below are the literature surveys we have done. Every project based on the different deep learning methods. Recently, deep learning-based methods based on iot prison break monitoring and altering system have attracted great interest and became a new research topic in the field of IOT.

Arjun et al., (2019) This paper presents the problem statement of making a digitally sound and useful system to alert the authorities in case of prison break and to monitor the inmates using IOT. This device aims to monitor the activities of the inmates on regular basis and detect their location and also the change in location of the prisoners through radio frequency and send the alert signal to the concerned department of the police if there is any case of prison break. The device comprises of Arduino and a radio frequency (RF) module. The main portal of the officer is designed using IoTGecko. The RF module is installed on each inmate that continuously tracks their location. Once the inmate is out of his/her validated location an alert signal is sent on the portal of the officer and also throughout the jail aiming to alert about the jailbreak.

Jisha et al., (2018) propose a system for intruder detection which employs an object detection technique using Wireless sensor networks. PIR (Passive infrared) sensors are used which are further connected to MICAz sensor node. The proposed system is expected to detect and track the intruder and report its speed and direction of movement to a central base station for further processing

Singh and Khushwaha (2020) propose a mechanism for smart border surveillance and automatic combat. It makes use of features extracted from optical flow information of the scene. Once the automatic detection of intruder takes place, suitable action is taken depending upon the relative position of the intruder with respect to the border fence. If the intruder happens to be behind the fence, mere tracking is followed. If the intruder is

above the fence and trying to cross it, an alarm is raised. Auto-firing can be activated when the intruder has actually crossed the fence.

Jin et al., (2019) present a method for detecting and classifying a target by using seismic and PIR sensors. The target can be classified into one of the three classes of vehicle, animal or human. A wavelet method called symbolic dynamic filtering (SDF) is used for feature extraction from the sensor signals.

Zhang and Liang Ye et al., (2018) present a method to detect moving target via using the technique of background subtraction and shadow removal. The method is applied for RGB color space. Metrically trimmed mean and mean absolute deviation are the estimators used for background subtraction. The Chromacity difference and brightness difference are the estimators for shadow removal.

Zynthia et al., (2020) This paper proposes an IoT based inmate detection technique that works on two main approaches: i) Light source based approach using Laser and GSM module to detect the movement near the boundary wall, ii) Geo- fencing based approach in which each prisoner will be provided with a wearable and non- detachable device that consists of GPS,GSM and Microcontroller. Geo-fencing will be done on the coordinates of the Jail's perimeter wall so that if somebody tries to reach the wall an alert signal would be broadcasted through repeated phone calls. In-case the inmate runs away from the jail then the physical location of his/her is tracked with the help of latitude and longitude of the location. The main challenge of this device was the shortage of the battery life.

CHAPTER 3

EXISTING METHOD

In the current scenario, we can easily find surveillance systems to protect public places like banks, malls, houses, etc. from robbers. People are well aware of the current security systems of Indian prisons. Currently, CCTV, drones and guards are used to monitor the prison's activities. But these surveillance systems are not sufficient to keep an eye on such criminals and ensure that there is no chance of these prisoners escaping. Because there are many problems with modern security systems. Some of the problems found with these CCTVs are degraded image at night, noisy camera footage, flickering videos, horizontal lines appearing on videos, insufficient video signal, no DVR recording, triggering and annoying false alarms, bright spots on the monitor, etc. These problems can cause a lot of chaos in the prisons and the prisoner may get a chance to escape, as well as the deployment of these techniques is relatively more expensive. The drawbacks are:

- Sensitivity to Environmental Conditions
- Maintenance Challenges
- False Positives and Negatives

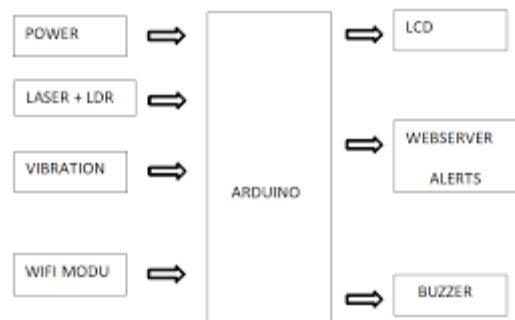


Fig:3.1: Block diagram of Existing method

As shown in the above figure there will be laser and LDR for the project but now in advance we are using vibration sensor. Because there are many problems with modern security systems. Some of the problems found with these CCTVs are degraded image at night, noisy camera footage, flickering videos, horizontal lines appearing on videos, insufficient video signal, no DVR recording, triggering and annoying false alarms, bright spots on the monitor, etc. These problems can cause a lot of chaos in the prisons and the prisoner may get a chance to escape, as well as the deployment of these techniques is relatively more expensive.

CHAPTER – 4

PROPOSED WORK

The prison break monitoring system is operated by giving a code for every prisoner using the RFID Technology which gives unique code to each prisoner. Things included the methodologies are RF Transmitters , Wi-fi Module and Microcontroller.

For detecting movement at any place we have two type of system , either we can put detecting system on moving object or to create an are and give signal to non moving object. Like this we have two type of Prison Break Prevention, Monitoring and Alerting Systems that are:

The module is mainly a type wearable device that is non-detachable and that can be installed anywhere on the prisoner's body or clothes, it is of type to put detecting system on moving object. In This device generally equipment used are a Microcontroller, RF Module, GSM and other detecting type of sensors based on motion, that will send the data to the receiver side to know the status of the prisoner, moving object. These sensors send information to the receiver in the form of Data signal . These sensors and modules are linked with the microcontroller. The microcontroller gathers the data fetched by the sensors which are on moving object, after that further analysis is done to extract information from the raw data got from prisoner. After this processing the information is transmitted to the receiver terminal, which will now status of prisoner .

The second module is basically a control room that consists of equipment like of a Microcontroller, Display unit (LCD), RF Module, Laser, Alarm, and Geo-fencing, that is based on second type which will create and will send information to non moving object. A breaking fence is formed to monitor the movement near the boundary of the

prison and LCD is used to display the information transmitted by the transmitter section. As shown in figure 4 the connections are connected and the output will display on the led display and blink app

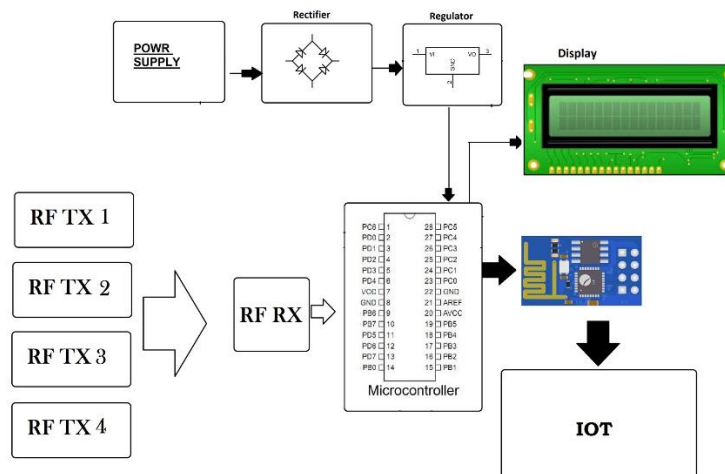


Fig: 4.1: Block diagram

We propose a system comprising wearable devices equipped with RF transmitters worn by prisoners, RF transceivers installed at strategic locations within the prison and a gateway for relaying data to the central monitoring system which is responsible for analyzing data and triggering alerts in case of security breaches. The central monitoring system analyzes data in realtime and sends notifications to concerned authorities via a secure protocol like IoT Gecko triggering alerts through buzzer's .Our entire system is grounded with a Microcontroller Circuit and a Unique Prisoner Code with a Transmitter Module is given for each prisoner. The Hybrid Transceivers are used for end-to-end Synchronization between Tx and Rx side where the Receiver module is fixed in the Central Monitoring System. Where loss of RF signals from the Transmitter part initializes the Central Monitoring System to trigger the alert/buzzer through IoT Gecko that had been interfaced with our proposed system. Finally the attempted Prisoner Identity will be displayed on the LCD screen.

4.1 Hardware and Software Components

- **ATmega Microcontroller:** The ATmega328P Microcontroller is the heart of the system, which controls all the operations and manages communication between the RF transmitters and the receivers based on the predefined programming logic. An AVR architecture of 32K 8-bit microcontroller is used. Most of the instructions are executed in a single clock cycle regulating a throughput of nearly 20 MIPS at 20MHz. The ATMEGA328-PU is a PDIP 28 pin package and is suitable for use in our 28 pin AVR Development Board.
- **RF Transmitters and Receivers:** ST-TX01-ASK is an ASK Hybrid transmitter module designed by the Saw Resonator, with an effective low cost, small size, and simple-to-use which is responsible for transmitting signals from the prisoner to the monitoring center within the range. The ST-RX02-ASK is an ASK Hybrid receiver module, an effective low cost solution for use at 315/433.92 MHZ that receives signals from the RF transmitters worn by the prisoners to detect any break in RF attempts.
- **Buzzer:** A buzzer is installed at the monitoring center to alert the security personnel in case of a prison break.
- **LCD :** We use a 16x2 LCD display as output which has a resolution of 160x32 pixels, with each character taking up 5x8 pixels. The display can be controlled using a microcontroller that sends commands and data to the LCD module which allows text or other information to be displayed on the screen like alphanumeric characters, symbols, and basic graphics. It can also be programmed to display custom characters and graphics. The module typically includes a backlight, which can be controlled to adjust the brightness of the display.
- **Power Supply:** Our system requires a power supply to run the various components. This may include batteries or a power supply unit.
- **Arduino Compiler:** It is a critical component in the development of our system, as it allows us to write, compile, and upload code to the microcontroller, enabling the creation of customized monitoring and system.

- **IoT Gecko:** This platform provides connectivity between RF transmitter and microcontroller, device management, data management, and cloud integration. The IoT Gecko interface can enable users to monitor the system in real-time and take proactive measures to prevent security breaches. Additional Components: The extra components being used are Resistors, Capacitors, Push Button, Crystal Oscillator, Cables, Connectors, Diode, PCB, LED's, Transformer, and Adapter.

4.2 OPEN PROBLEMS IN EXISTING METHOD

In existing methods of prison security, there are several open problems that persist despite technological advancements. Here are some key issues

- **False Alarms and Noise:** Current systems may suffer from false alarms triggered by environmental factors or system errors, leading to desensitization of security personnel and decreased responsiveness to genuine threats.
- **Limited Coverage and Blind Spots:** Despite advancements in surveillance technology, there may still be areas within the prison that lack adequate monitoring coverage, creating potential blind spots where security breaches could occur undetected.
- **Scalability Challenges:** Implementing comprehensive security systems in large-scale correctional facilities can be challenging due to the scalability limitations of existing technologies, leading to gaps in security coverage in certain areas.
- **Integration Complexity:** Integrating various security components such as sensors, cameras, and alerting systems into a cohesive and interoperable framework can be complex and costly, especially in older prison facilities with outdated infrastructure.
- **Response Time Optimization:** While current systems may provide timely alerts to security personnel, optimizing response times to security incidents remains a challenge, especially in large facilities where the sheer size and complexity can delay intervention.

- **Privacy Concerns:** The deployment of advanced surveillance technologies raises privacy concerns among inmates, staff, and civil liberties advocates, necessitating careful consideration of privacy regulations and ethical implications.
- **Maintenance and Reliability:** Ensuring the ongoing reliability and performance of security systems requires regular maintenance and updates, which can be resource-intensive and may lead to system downtime if not managed effectively.
- **Human Factors and Training:** Despite technological advancements, human factors such as human error, fatigue, and inadequate training of security personnel remain significant challenges in maintaining effective prison security. Addressing these open problems requires a multidisciplinary approach that integrates advancements in technology, policy development, and human factors considerations to create comprehensive and adaptive prison security solutions

4.3 FLOW CHART

Certainly! Here's a detailed explanation of the figure shown below of the IoT-based Prison Break Monitoring and Alerting System.

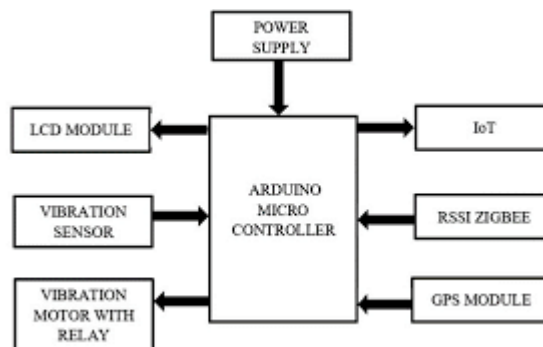


Fig: 4.3: Flow chart

Sensors are the foundational components of the system and are strategically placed throughout the prison facility. They are responsible for detecting various parameters such as motion, sound, vibration, and other environmental factors that could indicate a security breach or attempted prison break. Overall, the block diagram illustrates how the various components of the IoT-based Prison Break Monitoring and

Alerting System work together seamlessly to enhance security within correctional facilities by providing proactive monitoring, real-time detection, and prompt response to security incidents.

4.4 IMPLEMENTATION

Well it is a quite shocking fact but prison escapes are not very uncommon occurrences. There is no exact data count but we have all heard and still keep hearing of a variety of prison escapes happening globally. The fact that such number of inmates may still be roaming among us is itself scary. Well so here we propose a prisoner tracking system that helps detect prison breaks and instantly alert authorities using IOT. The system makes use of a microcontroller based circuit to achieve the task using rf technology. We make use of RF trackers on each inmate to detect their presence in the premises. The 2 central monitoring units are used to scan through all inmates as per data fed to it and constantly keep track of each prisoner. Each prisoner is mounted with a rf tracker transmitting a unique prisoner code wirelessly. Whenever a prisoner exits the facility the centralized system is unable to receive his/her code. At that time the receiver circuitry instructs the controller to tack action against particular prisoner. The System now transmits the prisoner details over to the officers alerting portal to send out instant alert and catch the prisoner before he runs even 50 meters away from the facility. Here we use IOTGecko to develop the online alerting portal system to receive input from monitoring device and display alert and sound alarm through internet.

IOT Prison Break Monitoring & Alerting System (Receiver section)

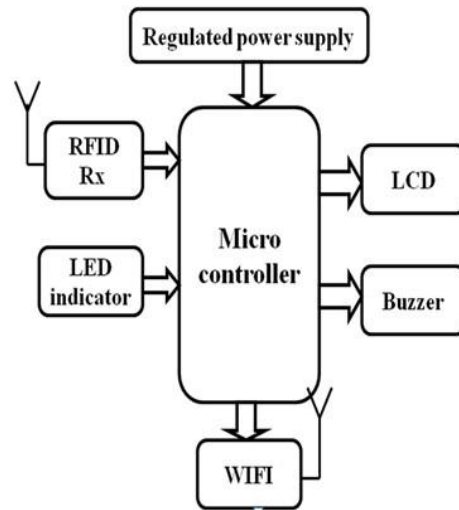


Fig: 4.4: Reciever Section

Discussion on Results of Light Source Approach In this configuration, the perimeter wall of the prison can be divided into numerous zones, each of which has a Laser module installed on one side and an LDR to detect laser beams on the other wall. The laser beam would be broken if the prisoner tried to approach the wall, raising an alert by activating the siren and sending brief signals to the authorities. The circuit connection for connecting a laser sensor, LDR, and an Arduino Uno board is shown in Fig.4.4 . This circuit enables an alarm system (Siren/Buzzer) and processes the signals supplied by the light source module. It is assumed that the perimeter walls around the jail have numerous levels and are off-limits to any inmates. A 10 m gap separates the LDR positioned on one side of the wall from where the laser sensor is deployed at one end of the wall. The IOT platform will alert the jail guards if someone breaks through this wall to flee.

Implementing an IoT-based prison break monitoring and alerting system involves several steps, including hardware setup, software development, integration, testing, and deployment. Here's a general outline of the implementation process:

- Requirement Analysis.

- Define the requirements and objectives of the system based on the specific needs of the correctional facility. Identify key functionalities, such as sensor types, communication protocols, alerting mechanisms, and user interfaces.
- Hardware Selection and Setup.
- Choose appropriate sensors, cameras, gateway devices, and communication infrastructure based on the requirements. Install and configure hardware components throughout the prison facility, ensuring optimal coverage and connectivity.
- **Software Development:** Develop the software components of the system, including: Firmware for sensors and gateway devices to collect and transmit data. Backend server software for data processing, analysis, and alert generation.
- User interfaces for administrators and security personnel to monitor alerts and manage system settings.
- Mobile applications or web interfaces for remote access to surveillance footage and alert notifications.
- **Integration:** Integrate hardware and software components to establish communication between sensors, cameras, gateway devices, and the central monitoring system. Implement protocols for data transmission, storage, and analysis, ensuring compatibility and interoperability between different components.
- Testing: Conduct comprehensive testing of the system to validate its functionality, reliability, and performance. Test individual components as well as the integrated system in simulated and real-world environments. Perform unit tests, integration tests, and end-to-end tests to identify and address any issues or bugs.
- **Deployment:** Deploy the IoT-based monitoring and alerting system in the correctional facility according to the planned implementation strategy. Install hardware components, configure software settings, and conduct final checks to ensure proper functionality before deployment.

- **Training and Documentation:** Provide training to prison staff and administrators on how to use the system effectively. Develop user manuals, guides, and documentation to support ongoing maintenance and operation of the system.
- **Monitoring and Maintenance:** Monitor the system regularly to ensure optimal performance and reliability. Implement maintenance procedures for hardware and software components, including software updates, firmware upgrades, and hardware replacements as needed.
- **Continuous Improvement:** Gather feedback from users and stakeholders to identify areas for improvement and optimization. Use data analytics to analyze system performance, identify trends, and enhance security protocols based on insights gained from real-world usage.

By following these steps, correctional facilities can successfully implement an IoT-based prison break monitoring and alerting system to enhance security and ensure the safety of inmates and staff. Collaboration with experts in IoT, security, and software development can further streamline the implementation process and maximize the effectiveness of the system.

4.5 AIM AND SCOPE

Aim is detect movement or status of behavior of prisoner's inside prison , whether they are in the premise area or not ,or their any unusual activity is affecting safety of prison or not . For this purpose, Geofencing has been done and to fail the idea of escaping , laser is used . This Project is based on Prison Security and Safety devices that are made by using Wi-Fi, Bluetooth for Internet as communication mode, GPS and GSM for SMS as communication mode for communication between higher authority and prison alert system. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market.

And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. Further we have known the Project and proposes a new problem statement based on the overlook of the currently used systems and gives the future aspects of the give project. As we know The prison system in India is not as good as we are known by our cinema, our by diplomatic debate related to politics

.In the era of everything digitally present in our country India, we are so orthodox about our safety, that prison system are not updated, also no concern is shown at present time also about related to safety upgradation of prison . Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too.

For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. The digital system to be used can be made reliable that it can't be under cyber attack, as there are people who want to deform the government authority, and some want to support prisoner for there particular motive. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have

human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system.

Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency.

4.6 WORKING

The system maintains logs of all detected incidents, responses, and outcomes for future analysis and reporting purposes. This data can be invaluable for improving security protocols and identifying vulnerabilities in the facility.

- **Enhanced Security:** Provides proactive monitoring and rapid response capabilities to prevent escapes and maintain order within the facility.
- **Efficiency:** Automates many aspects of security monitoring, reducing the workload on human personnel and minimizing the risk of human error.

- **Scalability:** Can be scaled to accommodate facilities of various sizes and configurations.
- **Data Insights:** Generates valuable insights into inmate behavior patterns and security risks, aiding in long-term security planning and decision-making.
- Challenges are
- **False Alarms:** Ensuring the system can distinguish between genuine threats and false alarms to prevent unnecessary disruptions.
- **Integration:** Seamless integration with existing security infrastructure and protocols can be complex and require careful planning.
- **Privacy Concerns:** Balancing the need for security with the rights and privacy of inmates and staff members.
- **Maintenance:** Regular maintenance and updates are necessary to ensure the system remains effective and up-to-date with evolving security threats.

An IoT-based prison break monitoring and alerting system represents a significant advancement in prison security, leveraging technology to create safer and more secure environments for both inmates and staff.

Redundant Communication Channels: Employing multiple communication channels (e.g., cellular, satellite) ensures that the system remains operational even if one channel fails, guaranteeing reliable transmission of alerts to security personnel.

4.7 CUSTOMIZATION AND ADAPTABILITY:

Tailored Security Protocols: The system should allow for customization of security protocols based on the specific needs and risk profiles of each correctional facility, enabling administrators to configure alerts and responses according to their requirements.

- **Integration with Existing Systems:** Seamless integration with existing prison management systems, access control systems, and emergency response protocols ensures smooth interoperability and minimizes disruptions during system implementation.

For this purpose, Geofencing has been done and to fail the idea of escaping , laser is used . This Project is based on Prison Security and Safety devices that are made by using Wi-Fi, Bluetooth for Internet as communication mode, GPS and GSM for SMS as communication mode for communication between higher authority and prison alert system. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system .

After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. Further we have known the Project and proposes a new problem statement based on the overlook of the currently used systems and gives the future aspects of the give project. As we know The prison system in India is not as good as we are known by our cinema, our by diplomatic debate related to politics .In the era of everything digitally present in our country India, we are so orthodox about our safety, that prison system are not updated, also no concern is shown at present time also about related to safety upgradation of prison . Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era.

No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. The digital system to be used can be made reliable that it can't be under cyber attack, as there are people who want to deform the government

authority, and some want to support prisoner for there particular motive. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have human power present .

So The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other.

Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency.

1. Continuous Improvement and Evaluation:

- **Regular Training and Drills:** Conducting regular training sessions and drills for security personnel ensures that they are proficient in using the system and can respond effectively to security threats in real-world scenarios.
- **Periodic Audits and Reviews:** Regular audits and reviews of system performance, conducted by both internal teams and external security experts, help identify areas for improvement and ensure that the system remains effective in mitigating security risks.

2. Legal and Ethical Considerations:

- **Compliance with Regulations:** Adhering to relevant laws, regulations, and industry standards governing the use of surveillance technology and data privacy is essential to prevent legal and ethical complications.
- **Transparency and Accountability:** Maintaining transparency about the use of the system and ensuring accountability for its operation and data handling practices fosters trust among inmates, staff, and the public.

By addressing these additional aspects, an IoT-based prison break monitoring and alerting system can be further strengthened to meet the complex security challenges faced by correctional facilities while upholding principles of safety, fairness, and accountability. As we know The prison system in India is not as good as we are known by our cinema, our by diplomatic debate related to politics .In the era of everything digitally present in our country India, we are so orthodox about our safety, that prison system are not updated, also no concern is shown at present time also about related to safety upgradation of prison . Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too.

For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be

more safe and reliable system. The digital system to be used can be made reliable that it can't be under cyber attack, as there are people who want to deform the government authority, and some want to support prisoner for there particular motive. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with ths system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market.

And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe.

4.8 LIMITATIONS

1) Implementation of Advanced Technologies:

- **Biometric Authentication:** Utilizing biometric scanners for inmate identification adds an extra layer of security, ensuring that only authorized individuals can access certain areas or perform specific actions within the facility.

- **Video Surveillance:** Integrating video cameras with the IoT system allows for visual verification of security breaches, providing real-time footage to security personnel for better situational awareness and response.
- **Machine Learning and AI:** Implementing machine learning algorithms can enhance the system's ability to detect abnormal behavior patterns by continuously analyzing sensor data and adapting to evolving threats over time.

2) Redundancy and Fail-Safe Mechanisms:

- **Backup Power Supply:** To ensure uninterrupted operation, the system should have backup power sources such as generators or batteries in case of power outages.

While an IoT-based prison break monitoring and alerting system offers significant benefits in enhancing security within correctional facilities, it also has several limitations that need to be considered:

- **Cost:** Implementing and maintaining a comprehensive IoT system can be expensive, requiring significant upfront investment in sensors, communication infrastructure, software development, and ongoing maintenance.
- **Complexity:** Integrating various sensors, communication protocols, and software components into a cohesive system requires careful planning and technical expertise. Complex systems are prone to issues such as interoperability problems, software bugs, and hardware failures.
- **False Alarms:** The system may generate false alarms due to environmental factors (e.g., fluctuations in sensor readings), technical glitches, or misinterpretation of data. False alarms can lead to unnecessary disruptions, erode trust in the system, and divert resources away from genuine security threats.

- **Privacy Concerns:** Collecting and analyzing sensitive data about inmates' movements and behavior raises privacy concerns. Striking the right balance between security needs and individual privacy rights is challenging and requires clear policies, safeguards, and oversight mechanisms.
- **Security Vulnerabilities:** IoT systems are vulnerable to cyberattacks, including unauthorized access, data breaches, and sabotage. Protecting against cybersecurity threats requires robust encryption, access controls, regular security audits, and prompt patching of software vulnerabilities.
- **Dependency on Technology:** Over-reliance on technology may lead to complacency among security personnel, who may become less vigilant or proactive in monitoring the facility manually. Maintaining a balance between technology-driven surveillance and human oversight is crucial for effective security management.
- **Limited Coverage:** While IoT sensors can be deployed in key areas of the facility, they may not provide comprehensive coverage of all potential escape routes or blind spots. Ensuring adequate sensor placement and coverage requires careful planning and periodic reassessment of security needs.
- **Regulatory Compliance:** Adhering to regulatory requirements and obtaining necessary approvals for deploying surveillance technology in correctional facilities can be a complex and time-consuming process. Compliance with laws related to data privacy, surveillance, and inmate rights adds another layer of complexity to system implementation.
- **Environmental Challenges:** Correctional facilities often present harsh environmental conditions, such as extreme temperatures, humidity, and physical wear and tear. Ensuring the durability and reliability of IoT hardware in such environments is essential to maintain system integrity.

Addressing these limitations requires a holistic approach that encompasses technological, organizational, legal, and ethical considerations. By carefully evaluating the trade-offs and mitigating risks, correctional facilities can maximize the effectiveness of IoT-based security systems while minimizing potential drawbacks.

No such count documentation is present but prison escapes keep happen, either at large scale or in smaller scale, and no such is hyped in the era. This thought us is itself very scary, the prisoners are roaming about our society, it is dangerous too. For this status to overcome as we know we can rely more on machines for being perfectionist we should engage with this system of safety both human and digital system, so as we have human power present so The changes required in the today's prison system is that, that the system should be a bit digitalized , by which it will be more safe and reliable system. Organization of the Project: While working on Project is the literature survey has been done to know about their pros and cons in the market. And further we have seen the functioning of these currently available system . After knowing the currently available system it will clarifies the points that should be examined to design an efficient setup, after which we will work on it. They have particular restriction on each of them. Wi-Fi and Bluetooth devices have a limited to transmit signal and communicate with each other. Also prison's are present at different -different location, like that of village area, or highly populated dense area, having multistory building that causes Poor internet connectivity which will decrease it's efficiency. There are some more aspects that can be used to make this system more reliable against cyber attack, which can be used to make it safe. Because of this scenario of orthodox system, the jail breaks are very common and most usual thing to happen in present era. They have particular restriction on each of them.

An IoT-based prison break monitoring and alerting system is a sophisticated solution designed to enhance the security of correctional facilities. Here's an overview of how such a system might work:

Components of the System:

- **Sensors and Detectors:**

Motion sensors, pressure sensors on doors, windows, and other critical points.
Biometric scanners (like fingerprint or iris scanners) for authentication. RFID tags or GPS trackers for monitoring prisoner movement within the facility.

Communication Infrastructure: Wireless communication protocols like Wi-Fi, Bluetooth, or Zigbee for connecting sensors to the central monitoring system.

Possibly a cellular network connection for remote monitoring and alerts.

- **Central Monitoring System:** A central server or cloud-based platform to aggregate data from all sensors. Real-time monitoring and analysis of sensor data to detect any unusual activity or breaches. Database management for storing prisoner profiles, authorized movements, and historical data.
- **Alerting Mechanism:**
Integration with alarm systems, such as sirens, lights, or automated lockdown procedures. Notifications sent to security personnel via mobile apps, SMS, email, or dedicated monitoring consoles.

Working Process:

- **Continuous Monitoring:**
Sensors are deployed throughout the prison facility, including cell doors, corridors, perimeter fences, etc. These sensors continuously monitor for any suspicious activities or breaches.
- **Data Analysis:**
Sensor data is collected and analyzed in real-time by the central monitoring system. Algorithms are applied to detect patterns indicative of potential escape attempts or security breaches.
- **Alert Generation:**
If any abnormal activity is detected, the system triggers an alert.
Alerts can vary in severity based on the perceived threat level, triggering different response protocols.
- **Response and Intervention:** Security personnel receive immediate notifications on their devices or through central monitoring consoles.
They can assess the situation and take appropriate actions, such as investigating the area, dispatching response teams, or initiating lockdown procedures.

- **Documentation and Reporting:** Certainly, let's delve deeper into some additional aspects of an IoT-based prison break monitoring and alerting system:
- **Scalability Issues:** Scaling the system to accommodate larger facilities or sudden increases in inmate population can be challenging. Adding new sensors, expanding communication infrastructure, and upgrading software to support increased capacity may require substantial resources and careful planning.
- **Maintenance and Upkeep:** Ensuring the continued functionality and reliability of IoT components over time necessitates regular maintenance, calibration, and replacement of hardware. Failure to maintain the system adequately can result in degraded performance, false alarms, and security vulnerabilities.
- **Interference and Signal Degradation:** Environmental factors such as electromagnetic interference, signal attenuation, and obstructions (e.g., concrete walls) can degrade the performance of wireless communication between IoT devices and the central monitoring system. Mitigating signal interference requires careful placement of sensors and use of signal amplification techniques.
- **Limited Predictive Capabilities:** While IoT systems can detect ongoing security breaches in real-time, their ability to predict and prevent future incidents is limited. Predictive analytics techniques may help forecast potential security threats based on historical data, but they are subject to uncertainties and false positives.
- **Human Factors:** Human error, negligence, or intentional misuse can undermine the effectiveness of the system. Security personnel may ignore or misinterpret alerts, fail to respond promptly to security breaches, or bypass security protocols, compromising overall security posture.
- **Legal and Ethical Challenges:** Balancing security imperatives with ethical considerations and legal constraints poses significant challenges. Surveillance technologies raise concerns about civil liberties, inmate rights, and the potential for abuse or misuse of power. Ensuring transparency, accountability, and adherence to due process is essential to address these concerns.

- **Cultural Resistance:** Introducing advanced surveillance technology into correctional facilities may face resistance from staff members, inmates, and advocacy groups who perceive it as invasive or dehumanizing. Overcoming cultural resistance requires effective communication, stakeholder engagement, and demonstrating the benefits of the system in improving safety and security.
- **Integration with Legacy Systems:** Legacy infrastructure and outdated systems within correctional facilities may pose compatibility issues when integrating IoT solutions. Retrofitting existing facilities with modern technology while ensuring seamless integration and minimal disruption to operations requires careful planning and coordination.

By acknowledging and addressing these additional limitations and challenges, correctional facilities can better navigate the complexities of implementing and maintaining an IoT-based prison break monitoring and alerting system, ultimately enhancing security and safety within their premises.

In recent years, advancements in technology have revolutionized various aspects of our lives, including the way we approach security challenges. One area where technology has made significant strides is in the realm of prison security. Traditional methods of monitoring and securing correctional facilities have often been labor-intensive, prone to human error, and limited in their effectiveness. However, the emergence of Internet of Things (IoT) technology has paved the way for a new era of prison security systems that are intelligent, proactive, and highly responsive to threats. Among these innovations, IoT-based prison break monitoring and alerting systems stand out as a promising solution to enhance security and safety within correctional facilities.

At the heart of an IoT-based prison break monitoring and alerting system lies a network of interconnected sensors, detectors, and communication devices strategically deployed throughout the facility. These sensors are capable of monitoring various parameters such as motion, pressure, sound, and environmental conditions in real-time. By continuously collecting and analyzing data from these sensors, the system can

detect anomalies, unauthorized activities, or potential security breaches with a high degree of accuracy.

One of the key advantages of IoT-based prison security systems is their ability to provide proactive alerts and timely responses to security threats. When the system detects suspicious activity, it triggers instant alerts, notifying security personnel through multiple channels such as mobile devices, email, or centralized monitoring consoles. This rapid response capability allows security teams to intervene swiftly, investigate the situation, and take appropriate action to mitigate the threat, thereby preventing potential escapes or incidents of violence.

Moreover, IoT-based prison security systems offer unparalleled levels of customization and scalability to meet the unique needs and challenges of each correctional facility. Administrators can configure the system to define access control policies, set up geo-fencing boundaries, and establish personalized alert thresholds based on specific security requirements. Furthermore, these systems can be seamlessly integrated with existing security infrastructure and management systems, ensuring compatibility and interoperability across different platforms.

Another significant benefit of IoT-based prison security systems is their ability to generate valuable insights and actionable intelligence to enhance decision-making and security planning. By analyzing historical data and trends, administrators can identify patterns of inmate behavior, assess security risks, and implement targeted interventions to prevent security breaches proactively. Additionally, these systems facilitate compliance with regulatory requirements and standards governing prison security and inmate safety, thereby reducing the risk of legal liabilities and penalties.

Despite their many advantages, IoT-based prison break monitoring and alerting systems also pose certain challenges and considerations that need to be addressed. Privacy concerns, cybersecurity risks, and the potential for false alarms are among the key challenges that must be carefully managed to ensure the responsible and effective deployment of these systems. Moreover, ongoing training, maintenance, and regular audits are essential to ensure the reliability, accuracy, and integrity of IoT-based security systems over time.

In conclusion, IoT-based prison break monitoring and alerting systems represent a significant leap forward in the realm of prison security, offering unprecedented levels of intelligence, responsiveness, and adaptability to address the complex and evolving security threats faced by correctional facilities. By harnessing the power of IoT technology, we can create safer and more secure environments for inmates, staff, and the community at large, ultimately advancing the cause of justice, rehabilitation, and public safety in society.

Advantages:

- **Enhanced Security:** IoT-based systems offer real-time monitoring and rapid response capabilities, enabling prompt detection and intervention in the event of security breaches or escape attempts, thus bolstering overall security within correctional facilities.
- **Proactive Alerts:** These systems generate immediate alerts to security personnel upon detecting suspicious activities or anomalies, enabling swift action to mitigate potential threats and prevent security lapses.
- **Customization and Scalability:** Administrators can tailor the system to meet the specific security requirements of each facility, configuring access control policies, alert thresholds, and response protocols according to their needs. Additionally, IoT systems can be scaled to accommodate facilities of varying sizes and complexities.
- **Data-Driven Insights:** IoT-based systems provide valuable insights into inmate behavior patterns, security risks, and operational efficiencies through data analysis and trend identification, empowering administrators to make informed decisions and optimize security protocols.
- **Integration with Existing Infrastructure:** These systems can seamlessly integrate with existing security infrastructure and management systems, ensuring compatibility and interoperability while minimizing disruption during deployment and operation.

- **Compliance and Accountability:** By facilitating adherence to regulatory standards and best practices governing prison security and inmate welfare, IoT-based systems help mitigate legal risks and liabilities while promoting transparency and accountability in security operations.

Disadvantages:

- **Cost:** Implementing and maintaining IoT-based systems can incur significant upfront costs, including investment in hardware, software, infrastructure, and ongoing maintenance, which may pose financial challenges for some correctional facilities.
- **Complexity:** The complexity of IoT systems, involving a network of interconnected sensors, communication devices, and software components, may introduce technical challenges such as interoperability issues, software bugs, and configuration complexities, requiring specialized expertise for deployment and management.
- **Privacy Concerns:** Extensive surveillance capabilities inherent in IoT systems raise privacy concerns among inmates, staff, and advocacy groups, necessitating robust safeguards and adherence to privacy regulations to mitigate potential infringements and maintain public trust.
- **Cybersecurity Risks:** IoT devices are susceptible to cybersecurity threats such as hacking, data breaches, and denial-of-service attacks, posing risks to the integrity, confidentiality, and availability of sensitive information and compromising overall system security.
- **False Alarms:** IoT-based systems may generate false alarms due to environmental factors, technical glitches, or misinterpretation of sensor data, leading to unnecessary disruptions, resource wastage, and erosion of trust in the system's reliability and effectiveness.
- **Dependency on Technology:** Over-reliance on IoT technology may lead to complacency among security personnel, diminishing their vigilance and readiness to respond to security threats manually, thereby undermining the effectiveness of the system as a supplementary security measure.

In summary, while IoT-based prison break monitoring and alerting systems offer numerous advantages in enhancing security and operational efficiency within correctional facilities, they also present certain challenges and considerations that require careful planning, implementation, and management to maximize their benefits while mitigating potential drawbacks.

In the realm of correctional facility management, ensuring the security and safety of inmates, staff, and the public is paramount. Traditional methods of prison security often rely on manual surveillance and reactive measures, which may be prone to human error and inefficiencies. However, the emergence of Internet of Things (IoT) technology has revolutionized the landscape of prison security by introducing intelligent monitoring and alerting systems designed to proactively detect and respond to security threats.

An IoT-based prison break monitoring and alerting system comprises a network of interconnected sensors, detectors, and communication devices strategically deployed throughout the facility. These sensors are capable of monitoring various parameters such as motion, sound, temperature, and access points in real-time. Through continuous data collection and analysis, the system can swiftly identify anomalies, unauthorized activities, or potential escape attempts, thereby serving as a vigilant sentinel against security breaches.

One of the defining features of IoT-based prison security systems is their proactive alerting mechanism, which enables rapid response to emergent threats. Upon detecting any suspicious activity, the system promptly triggers alerts, disseminating notifications to security personnel via multiple channels including mobile devices, email, and centralized monitoring consoles. This instantaneous notification empowers security teams to swiftly assess the situation, initiate appropriate interventions, and avert potential security lapses, thus bolstering the overall resilience of the facility.

Moreover, IoT-based prison security systems offer unparalleled levels of customization and scalability to meet the unique needs and challenges of each correctional environment. Administrators can configure these systems to define access protocols, establish geo-fencing perimeters, and set personalized alert thresholds

tailored to the specific security requirements of their facility. Furthermore, seamless integration with existing security infrastructure and management systems ensures compatibility and interoperability, facilitating smooth deployment and operation.

In addition to their real-time monitoring and response capabilities, IoT-based prison security systems provide valuable insights and actionable intelligence to inform strategic decision-making and security planning. By leveraging historical data and trend analysis, administrators can discern patterns of inmate behavior, assess security vulnerabilities, and implement targeted interventions to forestall potential security breaches proactively. Furthermore, these systems foster compliance with regulatory standards governing prison security and inmate welfare, mitigating legal risks and liabilities.

While IoT-based prison break monitoring and alerting systems offer numerous advantages in enhancing security and operational efficiency within correctional facilities, they also present certain challenges and considerations that require careful planning, implementation, and management. Addressing privacy concerns, cybersecurity risks, cost implications, and the potential for false alarms is essential to ensure the responsible and effective deployment of these systems. By embracing innovation in prison security and harnessing the transformative potential of IoT technology, correctional facilities can create safer and more secure environments for inmates, staff, and the broader community, thus advancing the cause of justice, rehabilitation, and public safety in society.

CHAPTER - 5

RESULTS AND DISCUSSION

If there is no movements and vibrations then the output is shown as below figure 5.1. it's shows everything is ok.

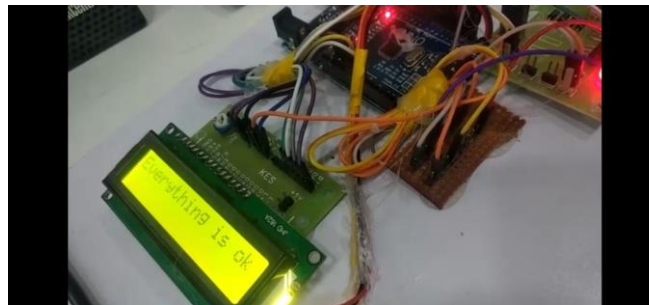


Fig :5.1: output 1

The system is made of Arduino module and a radio frequency (RF) module which helps us to achieve the desired results. The officer's main portal is made with the help of IOTGecko. The RF module is placed of each inmate, continuously tracking their location. Once the prisoner is out of his/her authenticated location an alert signal is passed on to the officer's portal and throughout the prison alerting about the escape. when their trying to escape from the jail. then immediately we will get messages. As shown in below figure 5.2 we will get messages to our registered mobile number.

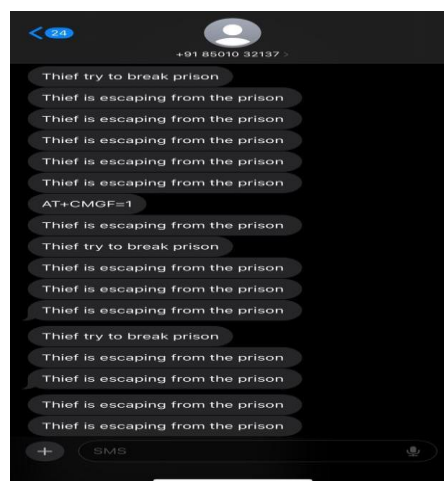


Fig: 5.2: Output 2

If the thief is moving and making the noises then the output will also display in the LCD display and as well as the messages and it rings the buzzer. When the thief is making any attempt to break prison then it shows on led display. When the receiver receives any vibrations from the vibration sensor then the display changes as shown in the figure 5.3.



Fig: 5.3: OUTPUT 3

And the last output is shown in the blynk software and when the receiver receives any vibrations then the value in the blynk app will change and it's shown as below figure 5.4.

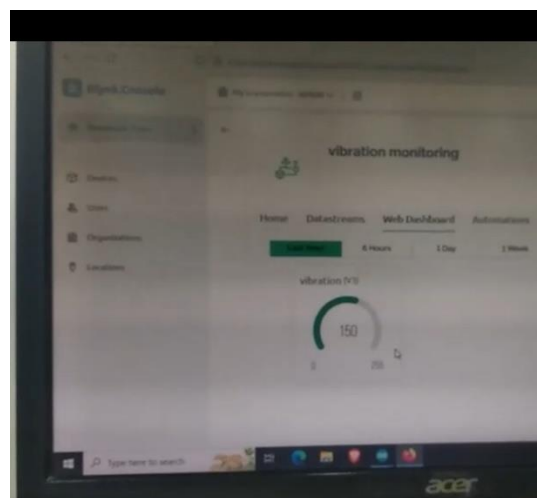


Fig :5.4: Output 4

The overall project output is displayed in three outputs .the first one is receiving messages and the second one is ringing buzzer and the third one is shown in blynk software. And the below figure 5.4 is the overall output shown in the project.

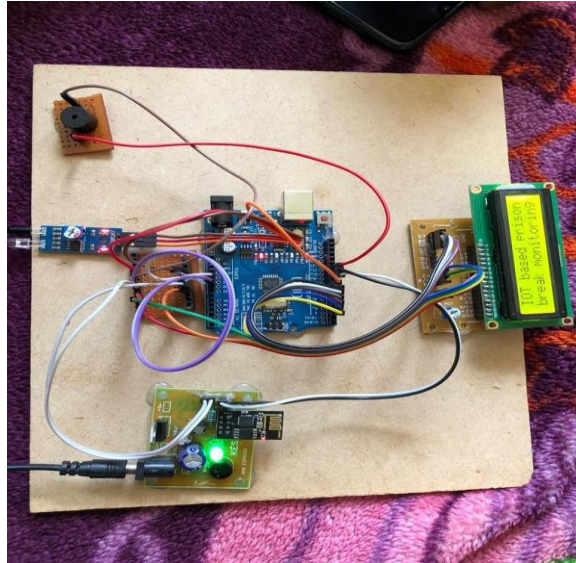


Fig: 5.5: overall project output

As shown in the above figure 5.5 the LCD displays as the thief trying to escape and the jail guard receives the meassages and buzzers starts ringing.

CHAPTER-6

CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSIONS

Basically The conclusion of the project is that if this system is implemented in our prison system it would add a new level to the security rules of our country, by which monitoring of the system will be ease. This system will bring major difference in the number of jail breaks happening per year, which are not in record. This iot based system explains the varied systems available for prison safety and security which constitutes of a RF Transmitter and Microcontroller. Transmitter and receiver helps us to reduce the time taken by the system to get and take data. From distance too it will be easy to monitor , all time monitor is not necessary. This will make a safe environment for common people, also a relaxed way to duty by authorities to know the information about prisoners

6.2 FUTURE SCOPE

If any time in future this system is implemented it can be made using nanotechnology reducing the size of the transmitter into a small chip. This chip can be planted anywhere on the inmates clothes without giving the inmate any clue of it. Even GPS system can be added on the chip making it easier to be tracked.

REFERENCES

- [1] Abraar.j, S. Banuselvi, and B. Kowsalya; "Prison Monitoring IBEACON and Arduino Microcontroller"; IJSDR1803026 International Journal of Scientific Development and Research (IJSDR); ISSN: 2455-2631; March 2018 IJSDR | Volume 3, Issue-3
- [2] Ashish Baghel, Rushin Deshmukh, and Vivek Kausadikar, "GPS based Hadcuffs System(using PIC 18f4550 and GSM)"; International Journal for Scientific Research & Development (IJSRD); ISSN:2321-0613 | Volume 5, Issue-4, 2017
- [3] Anu PS, Shibu V, Jabir K V T, and Preetha Mathew, "A High Security Prison Management SystemImplementation Using RFID CARD"; Anu PS et al, Int.J. Computer Technology &Applications(IJCTA); ISSN: 2229-6093 | Volume 6(1), 89-92
- [4] Badri Nath, Franklin Reynolds, and Roy Want,"RFID Technology and Applications," IEEE CS and IEEE ComSoc, Vol. 5, No. 1, 2006, pp. 22-24.
- [5] Cynthia, C.Bharathi Priya, Dr. Nageswara Guptha M; "IoT based Prisoner Escape Alert and Prevention System"; International Journal of Pure and Applied Mathematics; ISSN: 1314-3395; |Volume 120 No.6 2018, 11543-11554
- [6] El-Medany, Al- Omary, and Al-Hakim, "A cost Effective Real Time Tracking System Prototype Using integrated GPS/GSM Module", Wireless and mobile Communications (ICWMC),2010 , 6th International conference .Sept 10. International Journal of Computer science, Engineering and Application (IJCSEA) vol.3, no. 3, June2013.
- [7] Pasalram, N. Gunasekaran, and S. Rama Reddy, "Bluetooth in Wireless Communication"; IEEE Communications Magazine, June 2002, pp. 90-96.
- [8] Pooja, Sneha , and Neha, "Monitoring System for Prisoner with GPS using Wireless Sensor Network n(WSN)", IJCA; | Volume 91 No.13, April 2014.
- [9] Pankaj Verma, and J. S. Bhatia, "Design and Development of GPS-GSM Based Tracking System with Google Map Based Monitoring" International

Journal of Computer Science, Engineering and Applications (IJCSEA) Vol. 3, No. 03, June 2013.

- [10] Vaishali Rane, Harshada Vijay Gawde, Himanshu Sudhakar Kushwaha, Niragi Mahesh Masalia, TwinkleRajesh Panchal, "IOT Prison Break Alerting and Monitoring System (PBAS)"; Pramana Research Journal; ISSN: 2249 2976;|Volume-9 Issue-2 2019