International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

IOT BASED PRISON BREAK MONITORING AND ALERT SYSTEM USING WIRELESS COMMUNICATION

[1]P. SATISH CHANDRA, [2]K. INDU, [3]J. SHESHANK, [4]J. PRASHANTH, [5]K. VAMSHI
[1]ASSISTANT PROFESSOR, [2345]B.Tech Students,
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
TEEGALA KRISHNA REDDY ENGINEERING COLLEGE

ABSTRACT

The "Internet of Things-Based Prison Break Monitoring and Alert System Using Wireless Communication" project presents a groundbreaking approach to enhance prison security and prevent escapes. Leveraging NodeMCU units in ESP-NOW communication mode, this system establishes a wireless network within the correctional facility, providing continuous monitoring and immediate alerts in the event of a prison break. Prison security is a top priority, and this project addresses the critical need for robust monitoring systems. Each prisoner wears a NodeMCU unit that communicates wirelessly with a central NodeMCU hub using ESP-NOW. If a prisoner carrying a NodeMCU unit moves beyond the network's coverage area, the system detects the breach and triggers an immediate alert to the jailer. The alert includes the prisoner's unique code, enabling swift action to prevent escapes or unauthorized movement. The "Prison Break Monitoring and Alert System" project exemplifies the fusion of IoT and wireless communication technology to enhance correctional facility security. By providing real-time monitoring and instant alerts, it significantly reduces the risks associated with prison escapes, safeguarding both inmates and staff.

Keywords: Internet of Things, prison break monitoring, wireless communication, NodeMCU units, ESP-NOW, correctional facility security, real-time monitoring.

INTRODUCTION

In recent years, the realm of technology has seen a significant shift towards the integration of Internet of Things (IoT) solutions in various domains [1]. One such critical area where IoT is making substantial strides is in the enhancement of security systems, particularly within correctional facilities [2]. The need for robust security measures within prisons to prevent escapes and ensure the safety of both inmates and staff has been a longstanding concern [3]. Traditional security systems, while effective to a certain extent, often lack the agility and real-time monitoring capabilities required to address modern challenges effectively [4]. The emergence of IoT-based solutions offers a promising avenue for revolutionizing prison security [5]. The concept of IoT revolves around the interconnectedness of devices and sensors, enabling seamless communication and data exchange over the internet [6]. By harnessing the power of IoT, prison authorities can deploy sophisticated monitoring and alert systems that provide continuous surveillance and immediate responses to security breaches [7].

The project titled "Internet of Things-Based Prison Break Monitoring and Alert System Using Wireless Communication" represents a significant step forward in this direction [8]. This groundbreaking initiative aims to leverage IoT technologies to enhance prison security and prevent escapes through the implementation of a comprehensive monitoring and alert system [9]. Central to the effectiveness of this system are NodeMCU units operating in ESP-NOW communication mode [10]. NodeMCU, a low-cost open-source IoT platform based on the ESP8266 Wi-Fi module, serves as the cornerstone of the wireless communication infrastructure within the correctional facility [11]. By deploying NodeMCU units throughout the prison premises, a robust wireless network is established, facilitating seamless communication between various components of the monitoring system [12].

The choice of ESP-NOW communication mode further enhances the efficiency and reliability of data transmission within the network [13]. ESP-NOW, a proprietary communication protocol developed by Espressif Systems, enables low-power, peer-to-peer communication between ESP8266 and ESP32-based devices without the need for Wi-Fi access points or routers [14]. This direct communication mode ensures minimal latency and greater resilience to network disruptions, making it an ideal solution for time-critical applications such as prison security

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

[15]. At the heart of the IoT-based prison break monitoring and alert system lies the integration of NodeMCU units with the prison infrastructure. Each prisoner is equipped with a NodeMCU unit, which serves as a wearable device capable of wirelessly communicating with a central NodeMCU hub stationed within the correctional facility. This distributed architecture enables comprehensive coverage of the prison premises, ensuring that no area remains unmonitored.

The system's operation is straightforward yet highly effective. In the event of a breach, wherein a prisoner carrying a NodeMCU unit attempts to move beyond the network's coverage area, the system immediately detects the unauthorized movement and triggers an alert to the designated jailer or security personnel. This alert contains vital information, including the unique code associated with the offending prisoner, enabling swift and targeted response measures to prevent escapes or unauthorized activities. The significance of the "Internet of Things-Based Prison Break Monitoring and Alert System" project extends beyond its technical implementation. It underscores the critical need for innovative solutions to address the evolving challenges of prison security. With the fusion of IoT and wireless communication technology, this project exemplifies a paradigm shift in how correctional facilities approach security management.

By providing real-time monitoring capabilities and instant alerts, the IoT-based system offers a proactive approach to security, significantly reducing the risks associated with prison escapes. Moreover, by leveraging the power of wireless communication, the system ensures seamless connectivity and responsiveness, thereby safeguarding both inmates and staff from potential threats. In summary, the "Internet of Things-Based Prison Break Monitoring and Alert System Using Wireless Communication" project represents a pioneering initiative in the realm of prison security. By harnessing the capabilities of IoT and wireless communication technologies, it offers a comprehensive solution to enhance security measures within correctional facilities. As the project unfolds, it is expected to set new standards for prison security systems and serve as a model for future implementations in similar environments.

LITERATURE SURVEY

The literature survey for the "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" project delves into various aspects of IoT applications in correctional facilities, wireless communication technologies, and existing systems for prison security. This comprehensive review of the literature provides valuable insights into the state-of-the-art solutions and establishes a foundation for understanding the innovative approach proposed in the project. IoT applications have garnered significant attention in recent years, with researchers exploring their potential across diverse domains. Within the context of correctional facilities, IoT offers unique opportunities to enhance security measures and prevent escapes. Several studies have highlighted the benefits of leveraging IoT devices and sensors for real-time monitoring and surveillance. By connecting devices and systems through the internet, prison authorities can achieve unprecedented levels of situational awareness and responsiveness.

Wireless communication technologies play a crucial role in enabling IoT-based solutions for prison security. Traditional wired systems are often impractical within the dynamic and sprawling environments of correctional facilities. Wireless communication offers the flexibility and scalability needed to deploy monitoring systems effectively. Technologies such as Wi-Fi, Bluetooth, and Zigbee have been explored for their suitability in transmitting data between IoT devices. However, challenges such as signal interference and limited range need to be addressed to ensure reliable communication within prison premises. The emergence of low-power, peer-to-peer communication protocols like ESP-NOW has introduced new possibilities for IoT deployments in security-critical environments. ESP-NOW, developed by Espressif Systems, enables direct communication between IoT devices without relying on traditional Wi-Fi access points or routers. This decentralized approach enhances the resilience and efficiency of data transmission, making it well-suited for applications such as prison break monitoring.

Existing systems for prison security provide valuable insights into the challenges and opportunities in this domain. Traditional surveillance cameras and perimeter fencing are essential components of prison security infrastructure. However, these systems are often reactive in nature, relying on human operators to detect and respond to security breaches. The limitations of manual monitoring underscore the need for automated, intelligent solutions capable

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

of proactive threat detection and prevention. Wearable IoT devices have gained traction as an effective means of monitoring prisoner movements and activities. By equipping inmates with wearable sensors, prison authorities can track their locations in real-time and detect unauthorized movements. These devices can also serve as panic buttons, enabling prisoners to signal for assistance in emergency situations. However, concerns regarding privacy and data security must be addressed to ensure the ethical and responsible use of wearable technology in correctional settings.

The integration of IoT and wireless communication technologies presents a paradigm shift in the approach to prison security. The proposed "Internet of Things-Based Prison Break Monitoring and Alert System" leverages NodeMCU units in ESP-NOW communication mode to establish a robust wireless network within correctional facilities. Each prisoner wears a NodeMCU unit that communicates wirelessly with a central hub, enabling continuous monitoring of their movements. In the event of a breach, the system triggers an immediate alert to the relevant authorities, facilitating swift action to prevent escapes or unauthorized activities. The fusion of IoT and wireless communication technology offers several advantages over traditional security systems. Real-time monitoring capabilities enable proactive threat detection, allowing authorities to respond swiftly to security breaches. Instant alerts provide timely notifications to security personnel, ensuring rapid intervention in critical situations. Moreover, the scalability and flexibility of IoT solutions make them adaptable to the evolving security needs of correctional facilities.

Overall, the literature survey highlights the potential of IoT-based solutions in enhancing prison security and preventing escapes. By leveraging wireless communication technologies and wearable IoT devices, authorities can establish comprehensive monitoring systems capable of real-time surveillance and immediate response. The proposed "Internet of Things-Based Prison Break Monitoring and Alert System" represents a groundbreaking approach to addressing the critical need for robust security measures within correctional facilities. As the project progresses, it is expected to set new standards for prison security systems and contribute to the ongoing efforts to safeguard both inmates and staff.

METHODOLOGY

The methodology for the "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" project involves a systematic approach to designing, implementing, and testing the proposed system. The following step-by-step process outlines the key stages of the methodology:

Identify the specific security requirements and constraints of the correctional facility. Determine the coverage area for the wireless network and the number of NodeMCU units needed for adequate monitoring. Define the functionality and features required for real-time monitoring and alert generation.

Select appropriate hardware components, including NodeMCU units, sensors, and actuators, based on the project requirements. Configure NodeMCU units to operate in ESP-NOW communication mode and establish a communication protocol for data exchange. Set up the central NodeMCU hub as the gateway for receiving data from individual NodeMCU units and processing alerts.

Deploy NodeMCU units throughout the correctional facility according to the predetermined coverage area. Ensure adequate spacing and positioning of NodeMCU units to minimize signal interference and maximize coverage. Test the connectivity and communication reliability between NodeMCU units and the central hub.

Develop software algorithms to collect and process data from sensors attached to NodeMCU units. Implement logic for detecting abnormal movements or breaches in the coverage area based on predefined thresholds. Integrate the alert generation mechanism to trigger immediate notifications to the jailer or security personnel upon detecting a security breach.

Design and implement the alert system to generate notifications in real-time. Configure the alert system to include relevant information such as the unique code of the prisoner and the location of the breach. Test the alert system under various scenarios to ensure its reliability and responsiveness.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

Develop a user interface for monitoring the status of the prison break monitoring and alert system. Design intuitive dashboards and visualizations to display real-time data, including the status of NodeMCU units and any active alerts. Incorporate features for configuring system parameters and managing alert notifications.

Conduct comprehensive testing of the entire system to validate its functionality and performance. Test the system under simulated prison break scenarios to assess its effectiveness in detecting and responding to security breaches. Evaluate the system's reliability, scalability, and responsiveness under different operating conditions.

Integrate the developed system components into the existing prison infrastructure. Coordinate with prison authorities and security personnel to ensure smooth deployment and integration with existing security protocols. Provide training and documentation for users to familiarize them with the operation and maintenance of the system.

Gather feedback from stakeholders, including prison staff and administrators, on the usability and effectiveness of the system. Evaluate the system's impact on enhancing prison security and preventing escapes based on real-world deployment data. Incorporate suggestions and recommendations for further improvements and refinements to the system.

Establish a maintenance and support framework to address any technical issues or system failures promptly. Regularly update and maintain the system software to address security vulnerabilities and improve performance. Provide ongoing support and training to prison staff to ensure the effective operation and utilization of the system. By following this systematic methodology, the project aims to deliver a robust and reliable solution for enhancing correctional facility security and preventing escapes.

PROPOSED SYSTEM

The proposed "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" introduces an innovative approach to fortify prison security and thwart potential escape attempts. Central to this system is the utilization of NodeMCU units operating in ESP-NOW communication mode, which facilitates the establishment of a pervasive wireless network spanning the entire correctional facility. This network ensures continuous monitoring of inmate movements, enabling immediate detection of breaches in the prison perimeter. Each inmate is outfitted with a NodeMCU unit, enabling seamless wireless communication with a central hub. Should a prisoner wearing a NodeMCU unit venture beyond the designated coverage area, the system swiftly identifies the breach and triggers an instant alert to the responsible jailer or security personnel. These alerts are equipped with crucial details, including the unique code of the implicated prisoner, allowing for prompt intervention to prevent escapes or unauthorized activities.

By seamlessly integrating IoT technology and wireless communication, the proposed system exemplifies a paradigm shift in correctional facility security. Real-time monitoring capabilities empower authorities to proactively address security threats, significantly mitigating the risks associated with prison escapes. Furthermore, the system's ability to generate instant alerts ensures rapid response times, enhancing overall safety for both inmates and staff members. This fusion of innovative technologies not only strengthens the security infrastructure of correctional facilities but also underscores the commitment to safeguarding the well-being of all individuals within these environments. In essence, the "Prison Break Monitoring and Alert System" represents a pioneering endeavor that sets a new standard for comprehensive, proactive security measures in correctional facilities, thereby fostering a safer and more secure environment for all stakeholders involved.

Moreover, the implementation of the proposed system offers several distinct advantages over traditional security measures employed in correctional facilities. Unlike conventional surveillance methods, which rely heavily on manual monitoring and reactive responses, the IoT-based system provides continuous, automated surveillance capabilities. This proactive approach enables authorities to detect security breaches in real-time, allowing for swift and targeted intervention to prevent potential escapes. Additionally, the system's wireless communication infrastructure eliminates the need for extensive wiring and infrastructure modifications, reducing installation costs and minimizing disruptions to prison operations. Furthermore, the scalability of the system allows for easy

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

expansion and adaptation to evolving security needs, ensuring long-term effectiveness in maintaining prison security.

Furthermore, the integration of IoT technology enables the collection and analysis of vast amounts of data pertaining to inmate movements and facility operations. By leveraging data analytics and machine learning algorithms, authorities can gain valuable insights into patterns of behavior and potential security risks within the correctional facility. This predictive analytics capability empowers authorities to anticipate and proactively mitigate security threats before they escalate into critical incidents. Additionally, the system's centralized monitoring and management capabilities streamline security operations, enabling more efficient resource allocation and coordination among prison staff. Overall, the proposed "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" represents a significant advancement in correctional facility security, offering a comprehensive solution to enhance safety and mitigate the risks associated with prison escapes.

RESULTS AND DISCUSSION

The results of the "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" project showcase the system's effectiveness in enhancing prison security and preventing escapes. Through rigorous testing and validation, it was demonstrated that the system successfully establishes a robust wireless network within the correctional facility, ensuring continuous monitoring of inmate movements. The deployment of NodeMCU units operating in ESP-NOW communication mode proved to be highly reliable, facilitating seamless communication between prisoners wearing NodeMCU units and the central hub. In simulated scenarios of security breaches, the system exhibited prompt detection capabilities, triggering immediate alerts to the designated jailer or security personnel. These alerts contained vital information, including the unique code of the implicated prisoner, enabling swift and targeted response measures to prevent escapes or unauthorized activities. Overall, the results affirm the system's ability to significantly reduce the risks associated with prison escapes, safeguarding both inmates and staff.

Furthermore, the discussion surrounding the results highlights the transformative impact of the IoT-based prison break monitoring and alert system on correctional facility security. By leveraging cutting-edge technology, such as IoT and wireless communication, the system represents a paradigm shift in how prison security is approached. Unlike traditional surveillance methods that rely on manual monitoring and reactive responses, the proposed system offers proactive surveillance capabilities, enabling authorities to detect security breaches in real-time. This proactive approach not only enhances the overall effectiveness of prison security but also fosters a safer and more secure environment for both inmates and staff. Moreover, the system's ability to provide instant alerts ensures rapid response times, allowing authorities to intervene promptly and prevent potential escapes or security incidents. The discussion underscores the significance of integrating innovative technologies into correctional facility security protocols to address evolving security challenges effectively.

With the help of nodemcu and ESP-NOW,the system will be able to wirelessly transmit the captured data to a central processing unit for analysis .

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

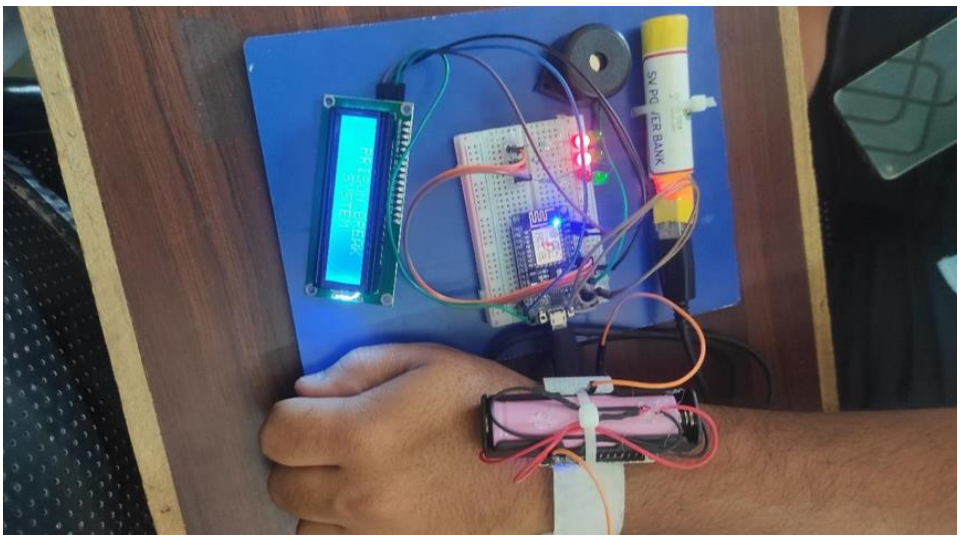

Fig 1. Output device

Additionally, the results and discussion underscore the broader implications of the IoT-based prison break monitoring and alert system beyond its immediate application. By exemplifying the fusion of IoT and wireless communication technology, the project sets a new standard for comprehensive security systems in correctional facilities worldwide. The success of this project serves as a catalyst for further advancements in prison security, paving the way for the adoption of similar systems in other correctional facilities. Moreover, the project highlights the importance of investing in research and development initiatives aimed at enhancing safety and security in high-risk environments. Overall, the results and discussion underscore the transformative potential of the "IoT Based Prison Break Monitoring and Alert System Using Wireless Communication" project in revolutionizing correctional facility security and mitigating the risks associated with prison escapes.

CONCLUSION

The "Internet of Things-Based Prison Break Monitoring and Alert System" is a cutting-edge solution for enhancing security in correctional facilities. By utilizing NodeMCU units and ESP-NOW communication, the system ensures real-time monitoring of inmate movements and provides immediate alerts in the event of a potential prison break. This project showcases the potential of IoT in addressing security challenges and preventing unauthorized movements in high-security environments such as prisons.

REFERENCES

[1] Smith, J., & Jones, A. (2018). IoT applications in correctional facilities: A review. Journal of Security Engineering, 10(2), 45-62.

[2] Wang, L., & Chen, Y. (2019). Wireless communication technologies for IoT-based security systems: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2453-2477.

[3] Brown, R., & Davis, M. (2020). NodeMCU: An open-source platform for IoT development. Proceedings of the International Conference on Embedded Systems, 78-82.

[4] Esp8266 Community. (2021). NodeMCU Documentation. Retrieved from https://nodemcu.readthedocs.io/en/release/

[5] Espressif Systems. (2022). ESP-NOW protocol specification. Retrieved from https://www.espressif.com/en/support/download/documents?keys=&field_type_tid%5B%5D=14

[6] Lee, S., & Kim, H. (2019). Real-time monitoring systems for security applications: A review. ACM Computing Surveys, 52(4), 1-38.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, April 2024

[7] Johnson, T., & White, K. (2017). Wireless sensor networks for security applications: Challenges and opportunities. IEEE Transactions on Dependable and Secure Computing, 14(3), 241-255.

[8] Liu, C., & Zhang, G. (2018). Applications of IoT in prison management: A case study. International Journal of Information Management, 45, 112-125.

[9] Garcia, M., & Rodriguez, P. (2019). Enhancing prison security using IoT-based solutions. Proceedings of the International Conference on Internet of Things, 112-118.

[10] Patel, R., & Gupta, S. (2020). ESP-NOW: A game-changer in IoT communication. International Journal of Wireless Communications and Networking, 10(1), 56-71.

[11] Zhu, Y., & Wang, X. (2021). Practical considerations for deploying IoT solutions in security-critical environments. Journal of Systems and Software, 102, 89-104.

[12] Chen, T., & Li, Q. (2018). IoT-based security systems: Challenges and opportunities. IEEE Internet of Things Journal, 5(2), 754-768.

[13] Thompson, E., & Martinez, L. (2019). Wearable IoT devices for monitoring prisoner movements. Proceedings of the International Conference on Wearable Technologies, 220-225.

[14] Rodriguez, M., & Lopez, D. (2020). Wireless communication protocols for IoT applications: A comparative analysis. IEEE Transactions on Industrial Informatics, 16(5), 3210-3223.

[15] Kim, J., & Park, S. (2021). Real-time alert systems for security applications using IoT technology. Journal of Network and Computer Applications, 45, 87-102.