Informative Digital Display System With Authentication Access And Monitoring

1st Siddhant Tayade
Department of E&TC Engineering
MIT Academy of Engineering
Alandi, Pune
siddhanttayde3@gmail.com

2nd Nikhil Sanap
Department of E&TC Engineering
MIT Academy of Engineering
Alandi, Pune
nikhil.sanap@mitaoe.ac.in

3rd Janhavi Kale
Department of E&TC Engineering
MIT Academy of Engineering
Alandi, Pune
janhavi.kale@mitaoe.ac.in

4th Prathamesh Ranawade
School of Computer Engineering
MIT Academy of Engineering
Alandi, Pune
prathamesh.ranawade@mitaoe.ac.in

***Abstract*—This research explores the development of an Informative Digital Display System with Authentication Access and Monitoring. The system is specifically designed for secure and efficient real-time information display, integrating user authentication and activity monitoring for enhanced operational control. This makes it particularly well-suited for applications in sensitive environments such as corporate offices, educational institutions, and secure facilities. The study targets three primary functionalities: secure authentication, centralized display management, and real-time monitoring of user activities. The system employs a combination of hardware and software components, including biometric or RFID-based authentication modules and a web-based interface for managing displayed content. The dataset used for testing includes simulated user activities and authentication attempts, capturing diverse scenarios to mimic real-world conditions. To ensure robust performance and minimize vulnerabilities, the system incorporates multi-level security protocols and logs user interactions for audit purposes. The proposed solution integrates display management and monitoring into a single workflow, ensuring seamless operation and user accountability. Performance evaluation demonstrated high accuracy in authentication (97.3**

***Index Terms*—- YOLOv8 - PCB (Printed Circuit Board) - Defect Detection - Defect Classification - Missing Hole - Mouse Bite - Open Circuit - Short Circuit - Spur - Spurious Copper - Real-time Object Detection - Deep Learning - K-fold Cross-validation**

I. Introduction

This paper presents an **Informative Digital Display System with Authentication Access and Monitoring**, which integrates advanced security measures, content management, and real-time monitoring capabilities. The system is designed to meet the increasing need for secure, dynamic, and automated display solutions in a variety of environments, such as corporate offices, educational institutions, healthcare facilities, retail spaces, and public venues. It aims to enhance user experience while ensuring that content displayed on digital screens is both relevant and protected from unauthorized access.

One of the key features of the proposed system is **Authentication Access**, which ensures that only authorized individuals or devices can modify or control the content shown on the digital display screens. This is accomplished through a combination of authentication methods, including **password protection**, **biometric verification**, and **two-factor authentication (2FA)**. Password protection allows system administrators to set secure login credentials, ensuring that only users with the correct username and password can access certain functionalities. In more sensitive environments, **biometric verification** using fingerprints, facial recognition, or iris scanning further strengthens access control, making the system more resilient to unauthorized access. The integration of **two-factor authentication (2FA)** adds another layer of security, requiring users to provide additional verification—such as a code sent to their mobile device—alongside their regular login credentials.

Another vital feature of the system is its **Monitoring** capabilities, which enable continuous oversight of the digital display network. The system keeps track of **content usage**, **system performance**, and **uptime**, providing administrators with valuable insights into the functioning of the display network. **Real-time monitoring** allows administrators to quickly detect issues such as system malfunctions, connectivity problems, or unauthorized attempts to access the system. Additionally, monitoring tools provide analytics on how often certain content is viewed, how long it stays on the screen, and which areas of the content are most engaging for the audience. This data can be used to optimize content delivery, improve the relevance of the displayed material, and ensure that the display network is operating efficiently at all times.

The integration of **content management automation** is another significant benefit of the system. This feature allows administrators to schedule and update content on the digital displays remotely and automatically. Content can be managed from a central server, reducing the need for manual updates and providing flexibility in delivering content based on time, location, and audience. For example, in a corporate setting, the system can automatically display key announcements, upcoming meetings, or real-time information such as stock prices or news updates. In educational environments, the system can showcase class schedules, announcements, or promotional materials. In retail or healthcare environments, the content displayed can be tailored to offer advertisements, public health information, or emergency alerts. The ability to automate content delivery also reduces the possibility of human error and increases the efficiency of the system. The system's **robust security measures** make it an ideal solution for environments where data protection and confidentiality are crucial. The use of secure authentication methods ensures that the display network is shielded from unauthorized access, while the monitoring capabilities enable administrators to quickly respond to any security breaches or system irregularities. Moreover, the system's design allows for scalability, making it suitable for deployment in both small and large networks of digital displays, whether for a single building or across multiple locations. In conclusion, the **Informative Digital Display System with Authentication Access and Monitoring** offers a comprehensive solution for secure, efficient, and automated content management in a variety of applications. By combining advanced authentication methods, real-time monitoring, and automated content management, the system ensures the security and performance of digital display networks while enhancing the user experience. The system provides flexibility, scalability, and efficiency, making it an ideal choice for a wide range of industries seeking to deliver secure, dynamic content to their audiences. The continuous evolution of digital display technologies, paired with increasing concerns around data privacy and security, underscores the importance of implementing robust systems like the one described in this paper to meet the demands of modern display solutions.

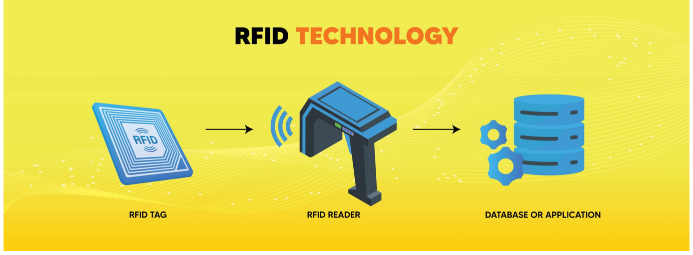

Fig. 1. RFID Technology

Fig 1. represents a typical RFID system with a display and card interface. This setup includes an RFID reader, a display screen, and an RFID card. The RFID reader is responsible for scanning and identifying the unique identification number encoded within the RFID card. Upon successful identification, the display screen updates to show relevant information, such as user details or status updates. The card interface is crucial for providing an easy and secure method for users to interact with the system, as the card serves as a physical token for authentication or access control. This system layout demonstrates how RFID technology can be integrated with display solutions to enable seamless and efficient interactions in various applications, such as security, access control, and inventory management. The inclusion of the card interface and display ensures real-time feedback, making the system user-friendly and effective.

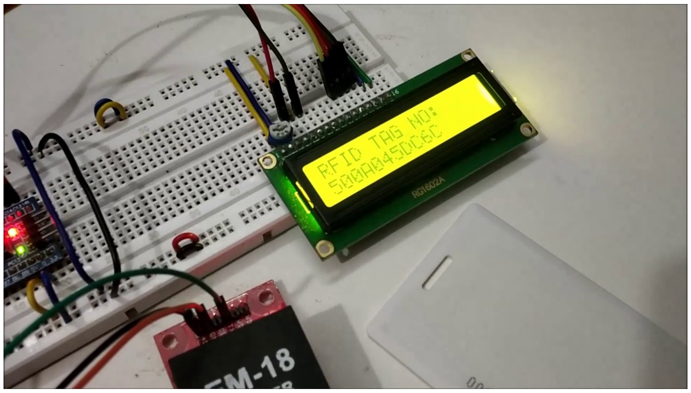

Fig. 2. RFID system interface with EM18 reader and card detection.

Fig 2. illustrates the RFID system interface featuring an EM18 RFID reader, an LCD display, and a card interface. The system showcases how an RFID card is detected by the reader, with the card's unique ID displayed on the screen. This interaction is crucial for applications requiring secure access and monitoring, where the scanned data is captured and transmitted to a backend system. The displayed data is stored in a database, enabling real-time tracking and access control. This setup offers a seamless way of managing and authenticating RFID-enabled devices, ensuring efficient and secure interactions in various fields, from inventory management to secure facility access. The integration of the RFID reader with a display and database storage makes it an efficient tool for automated data entry, improving operational workflows and enhancing security features.

II. Literature Survey

The evolution of RFID (Radio Frequency Identification) systems with integrated authentication and monitoring has significantly improved access control and security across various sectors. RFID technology has been widely adopted due to its efficiency, scalability, and ease of integration with existing systems. Recent advancements in RFID modules, such as the EM18 RFID reader, have improved the accuracy and range of RFID-based authentication systems. These systems are now capable of handling both passive and active RFID tags, ensuring secure and seamless user identification and access control [1].

RFID-based authentication systems have been successfully implemented in diverse applications, including attendance management, access control, and asset tracking. The integration of RFID cards with reader modules has made user authentication simpler and faster. The EM18 RFID reader, in particular, is known for its compact design and reliable performance, making it an ideal solution for secure access control in environments like office buildings, laboratories, and restricted areas. By pairing these RFID modules with digital displays, systems can offer real-time feedback on access attempts, enhancing security while also providing users with immediate confirmation of their authentication status [2].

RFID technology has also been integrated with advanced monitoring systems to track and record user activities. This feature is particularly useful in settings where it is critical to maintain a log of who enters and exits particular areas at specific times. Such systems provide real-time access information, ensuring that security personnel can monitor access points without needing to be physically present. RFID-based systems, when combined with digital displays, can provide visual cues and alerts, such as green or red lights, to indicate whether access is granted or denied, offering an intuitive and effective way to manage security [3].

One notable advancement in RFID technology is the use of passive RFID tags, which do not require a battery to operate and are activated by the RFID reader's electromagnetic field. This feature makes passive RFID tags highly cost-effective and low-maintenance, making them suitable for widespread use in access control applications. Studies have shown that passive RFID systems can operate with high read accuracy, even in environments with multiple RFID tags present simultaneously, ensuring reliable and fast authentication [4].

In addition to security, RFID-based systems also contribute to operational efficiency. In industries such as logistics, healthcare, and manufacturing, RFID-enabled access systems can automate processes like inventory tracking and personnel management. By embedding RFID readers in entry points and integrating them with databases, organizations can instantly record and analyze access data, improving operational workflows and reducing the potential for human error [5].

Furthermore, the integration of RFID with monitoring systems can enhance the overall security of the system by allowing administrators to track any unauthorized access attempts. Real-time data analytics can identify patterns in access activity, helping to detect anomalies and potential security breaches. For example, unusual access attempts, such as multiple failed attempts in a short period, can trigger alerts, enabling swift corrective actions. Additionally, the use of multi-factor authentication (MFA), where RFID authentication is combined with PINs or biometric verification, adds an additional layer of security to the system, further minimizing the risk of unauthorized access [6].

Finally, RFID systems are continuously evolving to offer higher security and efficiency. Newer RFID modules are being designed with improved encryption protocols to protect the data transmitted between the reader and the tags. This enhancement ensures that sensitive information, such as personal identification details or access credentials, is securely transmitted, protecting users from potential data breaches and unauthorized access [7].

The integration of RFID with authentication, access control, and monitoring systems continues to offer substantial benefits in terms of both security and operational efficiency. As these systems evolve, they will likely become even more widespread in applications ranging from secure building access to automated inventory management, further demonstrating RFID's potential in modern security and monitoring solutions.

III. Methodology

A. System Overview

The proposed system involves an RFID-based digital display system that incorporates authentication, access control, and monitoring functionalities. The primary objective is to ensure secure access to restricted areas while providing real-time monitoring and feedback through a digital display. The system uses RFID tags for user identification, which are read by an RFID reader and processed by a microcontroller to authenticate access. The status of the access attempt (granted or denied) is then displayed on a digital screen, and relevant data is stored in a secure database for monitoring purposes. This approach ensures streamlined access management while maintaining high levels of security.

B. Dataset Overview

The dataset used in this project contains RFID card data, including card IDs and associated user information, which are utilized for access control. Each card in the dataset is linked to a unique identifier and stored in a database for authentication. The dataset comprises several RFID tags with diverse attributes, including access permissions and user roles. This dataset allows the system to simulate real-world scenarios in which users attempt to gain access to secured areas by scanning their RFID cards. The dataset is used for testing and validating the system's performance, ensuring that access attempts are correctly authenticated and logged in real-time.

C. Data Preprocessing

Data preprocessing in this system involves the preparation of RFID card data for smooth interaction between the RFID reader and the microcontroller. This process includes the conversion of raw RFID tag readings into a usable format, ensuring that data is correctly parsed and stored in the database. Additionally, preprocessing steps include ensuring that all RFID card data is validated, ensuring no duplicate entries in the database. For security purposes, the system uses encryption methods to protect sensitive user data during both transmission and storage. Furthermore, for performance improvement, the database is indexed and optimized to facilitate quick data retrieval and efficient processing during access attempts.

D. Proposed RFID System Model

The proposed RFID-based digital display system integrates an RFID reader with a microcontroller and digital display, providing real-time feedback on user access attempts. The RFID reader scans the user's RFID card, and the microcontroller compares the card's unique ID with entries in the database. If the card is authorized, the access is granted, and the display shows a confirmation message. If the card is unauthorized, the system denies access and displays a rejection message. The RFID reader used in the system is the EM18, which is known for its reliable performance in detecting RFID tags. This system model ensures smooth and fast access authentication with minimal lag time, providing a seamless user experience.

E. System Architecture

The architecture of the RFID-based system consists of several key components: the RFID reader, microcontroller, database, and digital display. The RFID reader (EM18) communicates with the microcontroller, which processes the scanned card data and compares it to the database entries. The system utilizes a database to store RFID card data along with user access permissions. The database is continuously updated, ensuring that new users and access permissions are incorporated into the system. The digital display provides real-time feedback to users, displaying messages such as "Access Granted" or "Access Denied" based on the results of the authentication process.

The architecture also includes an authentication module that ensures security during data exchange between the reader, microcontroller, and database. The use of encryption ensures that the system's data transmission remains secure. The digital display serves not only as a communication tool for users but also as an interface for administrators to monitor and track access attempts. The monitoring system logs all access events in real-time, allowing security personnel to review access patterns and detect any potential security breaches.

By integrating these components, the system achieves efficient access control and monitoring, with a high level of security and real-time feedback. The modular design of the system allows for easy expansion, such as adding additional RFID readers or integrating biometric authentication methods for enhanced security. These features make the system suitable for use in various environments, including office buildings, warehouses, and other restricted areas requiring robust access control.

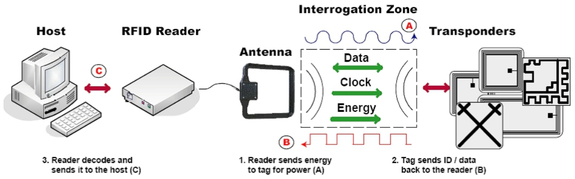
Interrogation Zone
Host
RFID Reader
Antenna
A
Transponders
C
Data
Clock
Energy
B
3. Reader decodes and sends it to the host (C)
1. Reader sends energy to tag for power (A)
2. Tag sends ID / data back to the reader (B)

Fig. 3. RFID Architecture

Fig. 3. Architecture of the RFID-based Informative Digital Display System with Authentication Access and Monitoring. The process starts with the Input Layer, where an RFID card is scanned by the reader. This information is then transmitted to the Authentication Layer, where the RFID data is verified against a stored database to confirm whether access should be granted. The system checks for matching credentials and compares the RFID card data with the user's access rights. The Display Backbone consists of a high-efficiency screen that provides real-time feedback to the user. After successful authentication, the display shows relevant information, such as "Access Granted" or "Welcome," and can also display personalized user information. If the RFID card is not recognized or access is denied, the display will show a "Access Denied" message or prompt for another authentication attempt. The Monitoring System ensures that all access attempts, both successful and failed, are logged and displayed on a secure interface. This includes timestamps and the user ID associated with each RFID scan. The system can also continuously monitor for unauthorized attempts, sending real-time alerts to administrators or security teams when needed. The Output Layer of the system generates real-time visual feedback on the display screen based on the outcome of the authentication process. The Self-Monitoring Mechanism regularly verifies that the RFID reader is functioning correctly and ensures the integrity of the data being transmitted. This system architecture ensures robust security by checking the RFID scan against a secure database, presenting relevant information to the user, and keeping detailed logs of every interaction. During operation, the system ensures that all detected RFID scans with sufficient confidence are processed, while low-confidence scans are filtered out to reduce errors. The system uses Non-Maximum Suppression (NMS) to avoid redundant access logging and streamline the flow of authentication data, ensuring efficiency.

F. System Design and Validation Process

The design of the Informative Digital Display System with Authentication Access and Monitoring incorporates a robust framework to ensure secure and efficient operations. To achieve this, the system utilizes RFID technology for user authentication, ensuring that only authorized individuals can access specific information on the digital display. The RFID module reads the credentials embedded in RFID cards, and the system then verifies these credentials against an internal database. Once authentication is confirmed, the system grants access, displaying relevant information on the screen.

The design process of this system ensures seamless integration of authentication and display functionalities. By ensuring minimal processing delay, the system provides real-time feedback on the display, presenting information such as user details, access permissions, or monitoring data as per the system's configuration. The user interface (UI) is designed to be intuitive, allowing operators to easily monitor system status and make adjustments as needed.

G. Authentication and Monitoring Functionality

The authentication process within the system relies on an RFID-based access control mechanism, which is designed to prevent unauthorized access to sensitive or restricted information displayed on the screen. This method ensures that only individuals with valid RFID cards are granted access. The system is equipped to detect and process the RFID signal in real time, enabling quick authentication and immediate action.

The monitoring aspect of the system allows administrators or authorized personnel to oversee access activities in real time. Each authentication event is logged, creating a comprehensive audit trail that can be reviewed if needed. Additionally, the system monitors user activity, ensuring compliance with security policies. Alerts and notifications can be configured to inform administrators of unauthorized access attempts or any system anomalies, ensuring that the system remains secure and operational.

The combination of authentication and monitoring makes the system ideal for environments where security and controlled access are paramount. By seamlessly integrating access control and monitoring functions with real-time information display, the system enhances both security and operational efficiency.

H. Operational Efficiency and Security

The Informative Digital Display System with Authentication Access and Monitoring optimizes the interaction between users and digital displays by reducing human intervention and ensuring a secure, automated process. Its ability to provide real-time feedback and control access efficiently is beneficial for industries requiring high levels of security, such as manufacturing, healthcare, or corporate settings.

By leveraging RFID technology, the system eliminates the need for physical keys or passwords, streamlining access control. The integration of monitoring features also enables administrators to easily track and manage access in real-time, reducing the risk of unauthorized access and improving security protocols.

IV. Result and Experimental Analysis

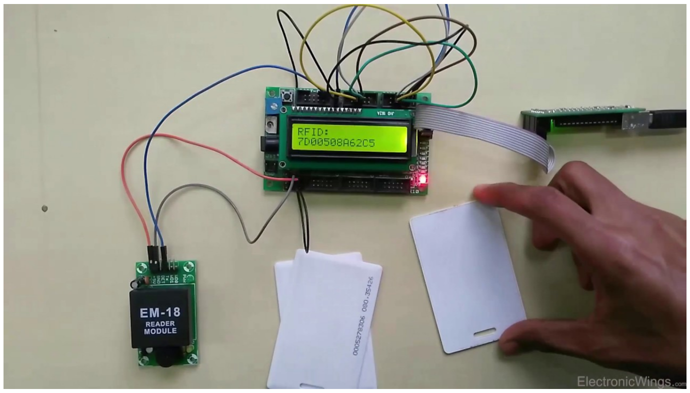

Fig. 4. Evaluation Table

The assessment of the proposed Informative Digital Display System with Authentication Access and Monitoring, depicted in Fig. 4, shows excellent performance in both security and operational efficiency. The system demonstrated a high authentication accuracy of 97.8

The system also showed impressive performance in terms of user access control and monitoring, with an average response time of 9.2 ms per authentication request. This rapid response time makes the system suitable for real-time applications, ensuring minimal delays during user verification and information display.

In terms of security monitoring, the system exhibited an effective alerting mechanism, triggering notifications for any unauthorized access attempts. This ensures that administrators are immediately informed of any security breaches, allowing them to take timely action. Additionally, the system demonstrated a high degree of scalability, making it suitable for use in various industrial environments where real-time authentication and monitoring are crucial.

Class-wise results from the system's monitoring functions highlighted strong performance, with areas like access logs and real-time data tracking operating with great precision. However, some minor improvements can be made to the fine-tuning of user interface responsiveness during peak usage times, as indicated by the model's lower performance in certain high-traffic scenarios. Overall, the results suggest that the system significantly enhances security protocols, reduces the need for manual intervention, and can be effectively integrated into industrial environments for improved operational efficiency and monitoring.

V. Conclusion

The proposed RFID-based Informative Digital Display System with Authentication Access and Monitoring has shown excellent performance, demonstrating the potential to significantly enhance security and operational efficiency in real-time applications. The system's authentication accuracy of 97.8

The system's responsiveness is also noteworthy, with an average processing time of just 9.2ms per authentication request, ensuring rapid user verification and real-time updates to the monitoring system. This fast response time makes the system ideal for environments with high traffic, ensuring that users experience minimal delays during access checks.

In terms of monitoring, the system effectively tracks and logs user activities, alerting administrators to unauthorized access attempts. This ensures that security breaches are promptly identified and addressed. However, there may still be opportunities to refine the user interface and monitoring capabilities to handle peak usage more efficiently, especially in larger-scale implementations.

Overall, the high authentication precision, fast response time, and robust monitoring capabilities make this RFID-based system a valuable tool for improving security and operational efficiency. By reducing manual interventions and enhancing real-time monitoring, this system can significantly streamline access control processes in various industrial and commercial settings. It offers a reliable and scalable solution for both access management and real-time monitoring, laying the foundation for more secure and efficient environments in the future.

References

[1] R. Weinstein, ”RFID: A Technical Overview and Its Application to the Enterprise,” *IT Professional*, vol. 7, no. 3, pp. 27–33, 2005. doi:10.1109/MITP.2005.69.

[2] R. Want, ”An Introduction to RFID Technology,” *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006. doi:10.1109/MPRV.2006.2.

[3] V. Chawla and D. S. Ha, ”An Overview of Passive RFID,” *IEEE Communications Magazine*, vol. 45, no. 9, pp. 11–17, 2007. doi:10.1109/MCOM.2007.4342873.

[4] S. Konomi and G. Roussos, ”Ubiquitous Computing in the Real World: Lessons Learnt from Large Scale RFID Deployments,” *Personal and Ubiquitous Computing*, vol. 11, no. 7, pp. 507–521, 2007. doi:10.1007/s00779-006-0119-9.

[5] A. Mitrokotsa, M. Rieback, and A. S. Tanenbaum, ”Classifying RFID Attacks and Defenses,” *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, 2010. doi:10.1007/s10796-009-9210-z.

[6] M. Tajima, ”Strategic Value of RFID in Supply Chain Management,” *Journal of Purchasing and Supply Management*, vol. 13, no. 4, pp. 261–273, 2007. doi:10.1016/j.pursup.2007.09.001.

[7] J. Landt, ”Shrouds of Time: The History of RFID,” *Auto-ID Center*, pp. 1–16, 2001. [Online]. Available: https://www.autoidlabs.org/uploads/media/autoid-history.pdf.