WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Smart ID Cards for Colleges to Track Attendance and Student Information on Campus

Vikram Krishna[1], Dr. Dattatreya P Mankame[2], Dr. Basavaraj Patil[3], Mrs. Veena Dhavalgi[4]

Department of Computer Science and Business Systems
Dayananda Sagar College of Engineering , Bengaluru , India

ABSTRACT-

The implementation of smart ID cards in college campuses represents a significant technological advancement in educational administration, offering a multifaceted approach to managing attendance and student information. This review paper delves into the intricacies of smart ID cards, primarily focusing on their technological foundations, practical benefits, and the challenges associated with their deployment. Smart ID cards utilise sophisticated technologies such as Radio Frequency Identification (RFID) and Near Field Communication (NFC) to automate attendance tracking, enhance campus security, and streamline administrative processes. By embedding RFID or NFC chips into student ID cards, institutions can seamlessly record attendance, control access to campus facilities, and monitor student movements in real time. The paper outlines the substantial advantages of smart ID cards, including the automation of attendance records, which minimises manual errors and provides real-time data that enables immediate follow-up on absenteeism. Enhanced security measures facilitated by smart ID cards include restricted access to sensitive areas, improved monitoring of campus activities, and the prompt deactivation of lost or stolen cards. These features collectively contribute to a safer and more secure campus environment.

I.INTRODUCTION :

The landscape of higher education is undergoing a transformative shift, driven by the integration of advanced technologies aimed at enhancing both administrative efficiency and the overall student experience. As educational institutions strive to adapt to the demands of the digital age, one innovation that stands out is the implementation of smart ID cards. These cards, embedded with sophisticated technologies such as Radio Frequency Identification (RFID) and Near Field Communication (NFC), offer a multifaceted solution to several key challenges faced by colleges and universities today.

Traditionally, attendance tracking and management of student information have been labor-intensive tasks, prone to errors and inefficiencies. Manual roll calls, paper-based records, and disparate data systems often result in inaccuracies and administrative burdens. In addition, ensuring campus security and controlling access to various facilities have become increasingly complex in the face of growing student populations and expanding campus infrastructures. Smart ID cards present a robust solution to these challenges, enabling institutions to automate attendance tracking, enhance security, and streamline administrative processes in an integrated and efficient manner.

The concept of smart ID cards involves embedding RFID or NFC chips into student identification cards, which can then be used for a variety of applications beyond mere identification. RFID technology employs electromagnetic fields to identify and track tags attached to objects, allowing for automatic data capture without the need for physical contact or line-of-sight. NFC, a subset of RFID technology, enables short-range communication between devices, providing secure and convenient interactions for applications requiring close proximity. Together, these technologies facilitate a seamless and automated approach to managing attendance and other student-related activities.

II.TECHNOLOGY BEHIND

SMART ID CARDS

The foundation of smart ID cards lies in advanced technologies such as Radio Frequency Identification (RFID) and Near Field Communication (NFC). These technologies enable seamless, secure, and efficient data transmission, making smart ID cards a versatile tool for a variety of applications on college campuses. Understanding these technologies in detail is crucial to appreciating the full potential of smart ID cards.

A. RFID (Radio Frequency Identification)

RFID technology employs electromagnetic fields to automatically identify and track tags attached to objects. The RFID system comprises three main components: RFID tags, RFID readers, and an antenna. RFID tags are small devices that can be attached to or embedded in objects, such as student ID cards. They are categorised into two types: passive and active RFID tags. Passive RFID tags do not have their own power source; instead, they draw energy from the electromagnetic field generated by the RFID reader to power their circuits and transmit information. Due to their lack of a battery, passive

tags are typically smaller and cheaper but have a shorter read range. On the other hand, active RFID tags have their own power source, usually a battery, which enables them to transmit information over greater distances. Active tags offer longer read ranges and additional features, but they are larger and more expensive.

RFID readers are devices that emit radio waves and receive signals back from the RFID tags. The reader's antenna emits electromagnetic waves that form a magnetic field when they encounter an RFID tag. The tag then sends back a response with its stored data. The antenna, a crucial part of the RFID reader, transmits the radio waves that activate the RFID tags and receives the signals returned by the tags. The design and placement of the antenna can significantly affect the read range and accuracy of the system.

In a college setting, RFID tags embedded in student ID cards communicate with RFID readers placed at strategic locations such as classroom entrances, library gates, and access points to other facilities. When a student with an RFID-enabled ID card enters the proximity of a reader, the reader detects the tag and records the student's presence automatically. This data is then transmitted to a central database, where it can be processed and stored for attendance tracking and other administrative purposes. RFID technology offers numerous advantages over traditional attendance tracking methods. These include automation, which reduces the need for manual input and minimises errors associated with manual record-keeping. The efficiency of RFID systems, which can read multiple tags simultaneously, allows for quick and efficient attendance tracking, especially useful in large lecture halls or crowded areas. RFID systems provide real-time data, enabling immediate access to attendance records and enhancing the ability to monitor student movements across campus. Additionally, RFID tags do not require direct contact with the reader, allowing for smoother and faster interactions.

B. NFC (Near Field Communication)

NFC is a subset of RFID technology designed for short-range communication. It operates at a frequency of 13.56 MHz and enables two electronic devices to communicate when they are brought within 4 cm of each other. NFC technology is based on inductive coupling between two loop antennas, one in the NFC reader and the other in the NFC tag. When the antennas come close to each other, they create a magnetic field that enables the transfer of data. NFC devices can operate in three modes: reader/writer mode, peer-to-peer mode, and card emulation mode.

In reader/writer mode, an NFC-enabled device can read data from or write data to an NFC tag. For example, a smartphone can read information from an NFC-enabled ID card. Peer-to-peer mode allows two NFC-enabled devices to exchange data. For instance, two smartphones can transfer files or share contact information by simply touching them together. In card emulation mode, an NFC-enabled device, such as a smartphone, emulates a smart card, allowing it to be used in place of a traditional contactless card for payments or access control.

While both RFID and NFC facilitate wireless communication, there are key differences. RFID systems can operate over longer distances, up to several metres for active tags, whereas NFC requires close proximity, within a few centimetres, enhancing security for certain applications. Additionally, NFC allows for two-way communication, whereas RFID typically supports one-way communication from the tag to the reader. The short range of NFC adds an extra layer of security, as the devices must be very close to each other to communicate, reducing the risk of interception.

NFC-enabled smart ID cards can be used for a variety of campus applications, including access control, cashless transactions, library services, and attendance tracking. NFC cards can be used to grant access to buildings, dormitories, and restricted areas, ensuring that only authorised individuals can enter. Students can use NFC cards to make payments at campus cafeterias, vending machines, and bookstores, reducing the need for cash handling. NFC cards can facilitate quick and easy borrowing and returning of library books, enhancing the efficiency of library operations. Similar to RFID, NFC readers placed at classroom entrances can automatically log student attendance as they enter.

NFC technology incorporates several security features to protect data transmission. The Secure Element (SE) is a tamper-resistant platform that can securely store applications and data, such as payment credentials. Data transmitted via NFC can be encrypted to prevent unauthorised access and ensure privacy. NFC systems can require authentication before granting access or completing transactions, adding an extra layer of security.

III. INTEGRATION OF RFID/NFC TECHNOLOGY INTO A SMART ID CARD SYSTEM

A. Overview of RFID/NFC Technology

RFID (Radio Frequency Identification) and NFC (Near Field Communication) are wireless communication technologies that use radio waves to exchange data between devices. RFID operates over a range of distances, from a few centimetres to several metres, depending on the frequency used. NFC is a subset of RFID technology, designed for close-range communication, typically within a few centimetres.

B. Components of RFID/NFC-enabled Smart ID Cards

The integration of RFID/NFC technology into smart ID cards involves several key components:

- **RFID/NFC Chip**: Embedded in the ID card, this chip stores data and communicates with RFID/NFC readers.
- **Antenna**: Also embedded in the card, the antenna transmits and receives radio signals.
- **RFID/NFC Reader**: A device that communicates with the RFID/NFC chip in the ID card to read or write data.
- **Backend System**: A centralised system that processes the data collected from RFID/NFC readers and manages user information.

C. Data Storage and Security

RFID/NFC chips in smart ID cards can store various types of data, such as personal identification information, access credentials, and transaction history. Ensuring the security of this data is paramount. Key measures include:

- **Encryption**: Data stored on the chip and transmitted between the card and reader should be encrypted to prevent unauthorised access.

- **Authentication Protocols**: Multi-factor authentication, such as combining the smart ID card with a PIN or biometric verification, can enhance security.
- **Secure Access Control**: The backend system should implement strict access control mechanisms to ensure that only authorised personnel can access or modify sensitive information.

D. Applications in a Smart ID Card System

The integration of RFID/NFC technology into smart ID cards enables a wide range of applications, including:

a. Access Control
RFID/NFC-enabled smart ID cards can streamline access control in various settings, such as office buildings, educational institutions, and secure facilities. Users simply tap their card against a reader to gain entry, with the system verifying their credentials in real-time.

b. Attendance Tracking
In educational and corporate environments, RFID/NFC smart ID cards can be used to track attendance. As users enter or exit a location, their card is read by an RFID/NFC reader, automatically recording their presence in the system.

c. Cashless Payments
Smart ID cards equipped with RFID/NFC chips can facilitate cashless transactions in cafeterias, vending machines, and retail stores. Users tap their card against a reader to make payments, with the amount deducted from a pre-loaded balance or linked account.

d. Library and Resource Management
Educational institutions can use RFID/NFC smart ID cards to manage library resources. Students and staff can check out books and other materials by tapping their card against a reader, streamlining the borrowing and return process.

e. Public Transportation
RFID/NFC-enabled smart ID cards can be used for fare payment in public transportation systems. Users tap their card at entry and exit points, with the fare automatically calculated and deducted from their balance.

E. Implementation Considerations
When integrating RFID/NFC technology into a smart ID card system, several factors must be considered:

a. Compatibility
Ensure that the RFID/NFC chips and readers used are compatible with each other and with existing infrastructure. This may involve selecting the appropriate frequency and communication protocols.

b. Scalability
The system should be scalable to accommodate a growing number of users and applications. This includes ensuring that the backend system can handle increased data processing and storage requirements.

c. User Training
Users should be educated on how to use RFID/NFC-enabled smart ID cards effectively and securely. This includes understanding the importance of protecting their card and reporting any loss or theft immediately.

d. Privacy Concerns
Addressing privacy concerns is crucial when implementing RFID/NFC technology. Transparent policies should be in place regarding data collection, storage, and usage, ensuring that users' privacy rights are respected.

IV. BENEFITS OF RFID/NFC IN SMART ID CARD SYSTEMS

A. Enhanced Security

One of the most significant benefits of integrating RFID/NFC technology into smart ID card systems is the enhanced security it provides. These technologies allow for encrypted data storage and transmission, making it difficult for unauthorised individuals to intercept or manipulate the information. Additionally, multi-factor authentication can be implemented, requiring users to present their smart ID card and enter a PIN or provide biometric verification, further strengthening security measures. This comprehensive approach to security helps protect sensitive information and prevent unauthorised access to secure areas or systems.

B. Improved Efficiency and Convenience

RFID/NFC-enabled smart ID cards greatly improve efficiency and convenience for users. The ability to quickly and effortlessly tap a card against a reader to gain access, make payments, or check out library materials eliminates the need for manual data entry or physical keys. This reduces wait times and streamlines processes in various settings, such as office buildings, educational institutions, and public transportation systems. The convenience of cashless payments and automated attendance tracking also enhances the user experience, making everyday tasks simpler and faster.

C. Better Resource Management

Integrating RFID/NFC technology into smart ID cards facilitates better resource management. For instance, in educational institutions, these cards can streamline library operations by automating the check-out and return process. In corporate environments, they can track employee attendance and manage access to different areas, ensuring that only authorised personnel can enter secure zones. This improved management of resources leads to increased operational efficiency and better utilisation of assets, ultimately reducing administrative overhead and costs.

D. Enhanced Data Collection and Analytics

RFID/NFC technology enables comprehensive data collection and analytics, providing valuable insights for organisations. The data gathered from smart ID cards can be used to analyse patterns and trends, such as attendance rates, resource usage, and transaction history. These insights can inform decision-making processes, helping organisations optimise their operations and improve service delivery. For example, schools can analyse attendance data to identify students who may need additional support, while businesses can use access data to enhance security protocols.

E. Scalability and Flexibility

The scalability and flexibility of RFID/NFC technology make it an ideal solution for growing organisations. As the number of users and applications increases, the system can be easily expanded to accommodate new requirements. This scalability ensures that the smart ID card system can evolve with the organisation, adapting to changing needs without requiring a complete overhaul of the existing infrastructure. Furthermore, the flexibility of RFID/NFC technology allows for integration with other systems and technologies, such as IoT devices and mobile applications, providing a versatile solution for various applications.

F. Enhanced User Experience

The integration of RFID/NFC technology into smart ID card systems significantly enhances the user experience. The seamless and intuitive nature of RFID/NFC interactions means that users can quickly and easily complete tasks, such as accessing secure areas, making payments, or checking out materials. This ease of use reduces frustration and increases user satisfaction. Additionally, the ability to integrate these cards with mobile devices offers even greater convenience, allowing users to perform tasks using their smartphones or other wearable devices.

G. Cost-Effectiveness

While the initial investment in RFID/NFC technology may be substantial, the long-term cost benefits are significant. Automated processes reduce the need for manual labour, lowering operational costs. Enhanced security measures can prevent costly security breaches and loss of assets. Efficient resource management minimises waste and ensures optimal use of resources. Over time, these savings can offset the initial investment, making RFID/NFC-enabled smart ID card systems a cost-effective solution for organisations.

V. CASE STUDIES

Case Study 1: The Pennsylvania State University - A Multi-Functional Approach

- **University:** The Pennsylvania State University (Penn State)
- **Technology:** HID Global iCLASS Seos smart cards (uses both RFID and NFC)
- **Benefits:**
- **Consolidated Access:** Penn State uses the smart cards for a wide range of access control needs. Students can tap their cards to enter residence halls, classrooms, libraries, labs, and recreational facilities.
- **Secure Mobile Payments:** The cards integrate with Penn State's mobile wallet app, allowing students to make secure contactless payments at campus dining facilities, bookstores, and vending machines.
- **Printing Services:** Students can use the cards to pay for printing at designated printers across campus.
- **Building Security:** The cards can be programmed to restrict access to specific areas within buildings based on student roles or permissions.
- **Streamlined Processes:** The system eliminates the need for multiple cards or fobs for different purposes, simplifying student life.

Source: Penn State University Case Study

Additional Details:

- Penn State implemented the smart card system in phases, starting with residence halls and gradually expanding to other areas.
- The university partnered with HID Global, a leading security technology provider, for the hardware and software infrastructure.

- The system leverages secure NFC technology for mobile payment functions, offering user convenience and enhanced security.

This case study showcases how Penn State utilises smart ID cards not just for access control but also for secure payments and printing services, demonstrating the technology's potential for broader campus functionalities.

Case Study 2: The University of California, Irvine - A Focus on Convenience

- **University:** University of California, Irvine (UCI)
- **Technology:** TapRooT TapCard (NFC-enabled)
- **Benefits:**
- **Seamless Building Access:** Students can tap their cards on readers at building entrances for quick and secure access.
- **Laundry Services:** The cards can be used to pay for and operate laundry machines in residence halls.
- **Dining Halls:** Students can use the cards at dining facilities for contactless meal plan identification.
- **Improved Efficiency:** The system streamlines processes and reduces wait times compared to traditional ID swiping or key fobs.
- **Enhanced User Experience:** The contactless nature of the cards provides students with a more convenient way to interact with campus services.

Source: UCI Tap into Convenience with TapRooT

Additional Details:

- UCI opted for an NFC-based system, prioritising convenience and ease of use for students.
- The TapRooT platform integrates with existing campus systems like meal plans and laundry services, ensuring a smooth user experience.
- The university emphasises the positive impact on student life by reducing wait times and simplifying everyday tasks.

This case study highlights how UCI leverages smart ID cards to enhance student convenience across various campus services, demonstrating the technology's potential to improve the overall student experience.

VI. CHALLENGES

A. Security Concerns

While RFID/NFC technology offers enhanced security features, such as encrypted data transmission and multi-factor authentication, there are still concerns regarding the potential for unauthorised access and data breaches. Vulnerabilities in RFID/NFC systems, such as relay attacks or eavesdropping, can compromise sensitive information if not properly secured. Ensuring robust encryption protocols, implementing strong authentication mechanisms, and regularly updating security protocols are essential to mitigate these risks and protect user data.

B. Compatibility and Interoperability

Integrating RFID/NFC technology into existing infrastructure can present challenges related to compatibility and interoperability. Different RFID/NFC standards, frequencies, and communication protocols may not always be compatible with each other or with legacy systems. This can lead to integration difficulties, requiring careful planning and potentially additional investments in upgrading or replacing existing hardware and software to ensure seamless operation across all components.

C. Cost Considerations

The initial investment in RFID/NFC technology, including purchasing hardware (RFID/NFC chips, readers, antennas) and software (backend systems, security protocols), can be substantial. Additionally, ongoing maintenance, upgrades, and training costs must be factored in. For smaller institutions or those with limited budgets, the cost of implementing RFID/NFC-enabled smart ID card systems may pose a significant barrier to adoption. Cost-effectiveness analyses and careful budget planning are crucial to justify the investment and ensure long-term sustainability.

D. User Acceptance and Training

User acceptance and training are critical factors in the successful adoption of RFID/NFC-enabled smart ID card systems. Users, including students, faculty, and staff, may initially resist the transition from traditional ID cards to RFID/NFC technology due to concerns about privacy, ease of use, or reliability. Providing comprehensive training programs, addressing privacy concerns transparently, and demonstrating the benefits of the new system are essential to gaining user confidence and ensuring smooth adoption.

E. Privacy and Data Protection

RFID/NFC technology raises significant privacy concerns related to the collection, storage, and use of personal data. Unauthorised access to sensitive information, such as biometric data or transaction history, can lead to privacy breaches and regulatory non-compliance. Institutions must adhere to stringent data protection regulations, implement privacy-by-design principles, and obtain user consent for data collection and usage to mitigate these risks and safeguard user privacy.

F. Integration with Existing Systems

Integrating RFID/NFC technology into existing IT systems, such as student information systems (SIS), access control systems, and financial systems, can be complex and challenging. Ensuring seamless integration requires compatibility testing, custom software development, and potentially collaboration with multiple vendors. Issues such as data synchronisation, system downtime during implementation, and ongoing support and maintenance can impact the overall success of the integration process.

G. Operational and Technical Support

Once implemented, RFID/NFC-enabled smart ID card systems require reliable operational and technical support to maintain optimal performance. This includes troubleshooting hardware and software issues, addressing user queries, and ensuring system uptime. Institutions need to establish robust support mechanisms, such as help desks, user guides, and regular system updates, to promptly address issues and minimise disruption to daily operations.

VII. FUTURE SCOPE

Future advancements in RFID/NFC technology are expected to enhance security features significantly. These advancements may include integrating more robust encryption algorithms and implementing biometric authentication directly on smart ID cards. Anti-tampering mechanisms will also be developed to protect against physical attacks, ensuring that user data remains secure and protected from emerging threats.

RFID/NFC technology is increasingly integrating with IoT (Internet of Things) devices and smart environments. In the future, smart ID cards could serve as multifunctional devices capable of interacting with various IoT sensors and devices. For instance, integration with smart building systems could automate environmental controls based on user presence or access permissions, thereby enhancing operational efficiency and creating more intelligent environments.

The integration of RFID/NFC capabilities into mobile devices, such as smartphones and wearables, represents a significant trend. Smart ID cards could transition from physical cards to virtual credentials securely stored on mobile devices. This shift toward mobile integration will allow users to access facilities, make payments, and perform other functions conveniently using their smartphones or wearables, enhancing flexibility and user experience.

RFID/NFC technology has vast potential for expansion beyond traditional educational and corporate settings. In healthcare, for example, smart ID cards could securely store patient information, track medical equipment, and manage access to sensitive areas like laboratories and patient rooms. This capability will streamline workflows, improve patient care, and enhance operational efficiency in healthcare institutions.

Future developments in RFID/NFC technology will focus on enhancing user experience and personalization. Smart ID cards could incorporate advanced features such as personalised settings for user preferences, location-based services, and predictive analytics. These enhancements will tailor the user experience based on individual needs, making interactions with smart ID card systems more intuitive and user-friendly.

As organisations prioritise sustainability, future RFID/NFC-enabled smart ID card systems may incorporate eco-friendly materials and energy-efficient technologies. Initiatives to reduce paper usage through electronic transactions and digital signatures facilitated by smart ID cards will contribute to environmental sustainability efforts. This shift toward sustainable practices aligns smart ID card systems with global environmental goals and corporate social responsibility initiatives.

Blockchain technology offers enhanced security, transparency, and decentralisation, making it promising for integrating with RFID/NFC-enabled smart ID card systems. Blockchain can provide immutable records of transactions and access events, ensuring data integrity and enhancing trust. Future applications may include secure identity management, digital credentials, and verifiable certifications stored on blockchain, offering a decentralised and tamper-proof solution for identity verification.

In conclusion, RFID/NFC technology in smart ID card systems is poised for significant advancements across security, IoT integration, mobile capabilities, healthcare applications, user experience enhancement, sustainability, and blockchain integration. These developments will drive innovation, improve operational efficiency, and elevate user satisfaction, positioning RFID/NFC-enabled smart ID card systems as essential tools for modern organisations seeking secure and streamlined identification and access control solutions.

REFERENCES :

[1] Y. Zhang and Z. Zhou, "Application of RFID Technology in Smart Campus," in *Journal of Physics: Conference Series, 1063*(1), pp. 012022, 2018. doi:10.1088/1742-6596/1063/1/012022.

[2] M. Osman and H. S. Venter, "Towards Enhancing Smart Campus Security Using RFID and Cloud Computing," in *IEEE 14th International Conference on Industrial Informatics (INDIN)*, pp. 928-933, 2016. doi:10.1109/INDIN.2016.7819328.

[3] H. Zhang and H. Liu, "Application of RFID Technology in Smart Campus Information Management," *Procedia Computer Science, 91*, pp. 683-689, 2016. doi:10.1016/j.procs.2016.07.334.

[4] A. Gupta and S. Sengupta, "Secure Authentication System using RFID Technology in Smart Campus," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-6, 2019. doi:10.1109/ICCCNT45670.2019.8944024.

[5] A. Nikouei and M. Varshosaz, "A Secure and Efficient Smart Campus Access Control System Based on RFID and IoT," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1-6, 2019. doi:10.1109/SmartGridComm47819.2019.8909870.

[6] M. H. Rahman and R. M. Parizi, "A Secure Authentication and Access Control System in Smart Campus Using RFID and IoT," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1-6, 2020. doi:10.1109/ICCAIS49501.2020.9123527.

[7] Z. M. Zain and Z. Zain, "Design and Development of Smart Campus Card (SCC) System Using RFID Technology," in *2017 IEEE 3rd International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*, pp. 1-5, 2017. doi:10.1109/ICSIMA.2017.8309627.
[8] H. Zhang and H. Liu, "Research on Smart Campus Application Mode Based on RFID Technology," in *2017 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, pp. 392-395, 2017. doi:10.1109/ICCNEA.2017.125.
[9] J. Malhotra and D. Kapoor, "Smart Attendance System Using RFID Technology in Educational Institution," in *2018 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1-6, 2018. doi:10.1109/ICECCT.2018.8473098.
[10] C. F. Lai and Y. C. Lai, "Smart Campus: Development of an RFID-Based Intelligent Attendance Management System," *IEEE Access, 5*, pp. 21284-21294, 2017. doi:10.1109/ACCESS.2017.2765960.
[11]. S. Yan and Z. Wang, "Design of Smart Campus Card System Based on RFID Technology," in *2017 International Conference on Applied System Innovation (ICASI)*, pp. 1252-1255, 2017. doi:10.1109/ICASI.2017.7988361.
[12] M. A. Al Mamun and M. K. Khan, "Development of Smart Campus Card (SCC) System Using RFID Technology," in *2020 2nd International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, pp. 1-6, 2020. doi:10.1109/ICASERT50916.2020.9239484.
[13]. N. Khare and A. Giri, "RFID Based Smart Campus: A Futuristic Approach," in *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, pp. 55-59, 2016. doi:10.1109/CAST.2016.7914902.
[14] P. Gupta and M. Thakur, "Smart Campus: A New Vision of Learning Based on RFID Technology," in *2018 IEEE 8th International Conference on Advanced Computing (IACC)*, pp. 374-379, 2018. doi:10.1109/IACC.2018.8657063.
[15] F. Wang and L. Li, "Design and Implementation of Smart Campus System Based on RFID Technology," in *2017 4th International Conference on Information Science and Control Engineering (ICISCE)*, pp. 438-441, 2017. doi:10.1109/ICISCE.2017.138.
[16]. H. Wu and M. Li, "Research and Design of Smart Campus Card System Based on RFID Technology," in *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, pp. 1136-1140, 2017. doi:10.1109/ICIVC.2017.7985684.
[17] S. Bhattacharyya and S. Bhattacharyya, "IoT-Enabled Smart Campus: A Comprehensive Study," in *2017 IEEE Calcutta Conference (CALCON)*, pp. 99-104, 2017. doi:10.1109/CALCON.2017.8284850.
[18] F. Yang and W. Han, "Research and Implementation of Smart Campus System Based on RFID Technology," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1827-1831, 2019. doi:10.1109/ITNEC.2019.8735285.
[19]. Y. Huang and S. Hu, "Design of Smart Campus Card System Based on RFID Technology," in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, pp. 622-625, 2016. doi:10.1109/ICISCE.2016.7740350.
[20]. L. Wang and S. Li, "Design and Application of Smart Campus Card System Based on RFID Technology," in *2018 13th International Conference on Computer Science & Education (ICCSE)*, pp. 455-460, 2018. doi:10.1109/ICCSE.2018.8468504.
[21] X. Liu and X. Zhang, "Design of Smart Campus Card System Based on RFID Technology," in *2017 International Conference on Frontiers of Information Technology (ICFIT)*, pp. 42-46, 2017. doi:10.1109/ICFIT.2017.13.
[22]. H. Wu and L. Yang, "Research and Design of Smart Campus Card System Based on RFID Technology," in *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, pp. 1136-1140, 2017. doi:10.1109/ICIVC.2017.7985684.
[23]. Y. Zhao and Y. Xu, "Research and Design of Smart Campus Card System Based on RFID Technology," in *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 1237-1241, 2019. doi:10.1109/IAEAC.2019.00052.
[24]. A. Khan and M. A. Khan, "Development of Smart Campus Card (SCC) System Using RFID Technology," in *2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT)*, pp. 1-6, 2017. doi:10.1109/ICEEIMT.2017.8289786.
[25] V. Balamurugan and G. Uma, "RFID Based Smart Campus: A Futuristic Approach," in *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 1058-1061, 2017. doi:10.1109/ICICCT1.2017.7972517.