QR Code-Based Access Control Systems: Architectural Taxonomy, Security Landscape, and Future Research Directions

Worood Alsawi, Dina M. Ibrahim
Department of Information Technology-College of Computer, Qassim University, Buraydah, Saudi Arabia

***Abstract*—Access control systems secure physical and digital settings, especially in colleges, businesses, and restricted areas. Physical key, magnetic card, and biometric access control techniques have loss, duplication, high deployment costs, and maintenance complexity. With the widespread adoption of smartphones, QR code-based access control systems (QR-ACS) have emerged as a flexible and cost-effective alternative. Scannable QR codes allow fast authentication without hardware, boosting user ease. How QR codes are generated, handled, and checked in the system determines the success of QR-based access control. This systematic review examines the integration and evolution of QR Code-Based Access Control Systems (QR-ACS), with particular attention to both recent innovations and the challenges that continue to accompany their adoption. A broad set of studies published between 2015 and 2023 was reviewed in order to explore how these systems have been designed, implemented, and evaluated across different application contexts. The analysis draws on literature indexed in major academic databases, including IEEE Xplore, ACM Digital Library, and JSTOR, with an emphasis on system architecture, implementation strategies, and reported performance outcomes. Overall, the reviewed studies indicate that QR-ACS can enhance operational efficiency and offer practical security benefits, especially when combined with complementary technologies. At the same time, recurring concerns related to security, robustness, and deployment limitations remain evident. This systematic review analyzes QR-ACS architectures, security mechanisms, and threat models, with particular emphasis on IoT integration, authentication strategies, and risk-aware system design.**

Keywords*—*QR codes; access control systems; security mechanisms; authentication; Internet of Things

I. Introduction

In the realm of security technology, the adoption of QR Code-Based Access Control Systems (QR-ACS) has been transformative, offering a novel method to manage access to various physical and digital spaces. QR codes, originally designed for tracking parts in vehicle manufacturing, have evolved significantly, becoming pivotal in access control systems due to their simplicity, cost-effectiveness, and ease of use. As Adedoyin and Olukoya [1] note, "QR codes, once developed for industrial purposes, now support smart lock systems and various security solutions," demonstrating their adaptability across multiple domains. These systems utilize QR codes to authorize entry to secured areas, integrating seamlessly with mobile technology and cloud computing to provide dynamic and robust security solutions [2]. This evolution underscores the ability of QR codes to transcend their original purpose, becoming a versatile tool for a wide range of applications in modern security systems.

As global security challenges continue to evolve, the demand for access control solutions that can adapt to changing operational conditions has become more apparent. Conventional approaches, including keycards, passwords, and biometric systems, are widely used but often present practical limitations, such as vulnerability to loss or theft and the need for dedicated infrastructure. In this context, QR-ACS are frequently discussed as a more flexible and cost-efficient option. According to Petrea et al. (2020), these systems can reduce operational overhead by relying on mobile devices and cloud-based services, which makes them suitable for environments where physical credentials or complex hardware are difficult to manage [3]. The widespread availability of smartphones with built-in QR code scanning capabilities has further supported the adoption of QR-ACS across both public and private sectors. Beyond conventional access scenarios, these systems have also been applied in situations that require minimal physical interaction. Awotunde et al. [4] highlights the growing relevance of such contactless solutions, particularly during health-related crises such as the COVID-19 pandemic, where reducing physical contact became a key safety consideration.

Several sectors, including education, healthcare, transportation, and corporate offices, have begun to integrate QR-ACS into their security frameworks. In educational settings, for instance, QR codes are increasingly used to manage access to facilities such as libraries, laboratories, and examination halls. Similarly, healthcare environments have adopted QR codes to control access to patient records, restricted areas, and medical equipment, particularly in cases where traditional physical access mechanisms may be inefficient or introduce additional risks. At the same time, security requirements differ across these contexts, as certain areas—such as research laboratories, server rooms, and administrative offices—demand higher levels of protection. While the adaptable nature of QR-ACS allows them to support varying access levels, further research remains necessary to refine these systems and ensure that they can meet more demanding security needs. Moreover, as organizations increasingly shift toward IoT-enabled environments, the combination of QR-ACS with biometric data and real-time monitoring has received growing attention as a potential approach to strengthening access control frameworks [6].

For example, [7] proposed an access control system for smart buildings that employs aesthetic QR codes combined with symmetric encryption algorithms. In this system, QR codes incorporate user photographs as an additional authentication layer. Although the proposed solution was described as cost-effective and flexible, it exhibited limitations related to scalability and reliability, particularly in low-light conditions, which negatively affected the QR code scanning process.

In a related work, [8] presented a QR code-based smart door access control system designed for educational and corporate environments. The system enhanced operational efficiency by recording user access times through a centralized database; however, the authors reported that the solution still faced constraints related to system scalability and long-term deployment in larger environments.

This review seeks to synthesize and critically examine the existing literature on QR-ACS, with the aim of identifying both the technological advances that have addressed key challenges and the areas where notable limitations remain. Through the analysis of a diverse body of studies, the review explores the reported strengths and weaknesses of current QR-ACS implementations, as well as the approaches that appear most promising for future development. Particular attention is given to application contexts in which QR-ACS have demonstrated practical effectiveness, alongside scenarios where further refinement is still required. By addressing these aspects, the review contributes to a clearer understanding of the current role of QR-ACS in modern security environments and highlights potential research directions that may support improvements in security, efficiency, and scalability [9]. The main contributions of this paper are:

- A comprehensive systematic review of QR-ACS (2015–2024).
- A structured architectural taxonomy of QR-ACS.
- A comparative analysis across multiple application domains.
- A proposed risk assessment framework for QR-based security threats.
- Identification of research gaps and future directions.

II. Background

Access control systems play a central role in security management, as they define who is permitted to access a given resource, whether a physical environment, such as a building or a digital asset, such as sensitive data. Early access control mechanisms were based on simple physical solutions, including locks and keys. Over time, these approaches evolved into more complex electronic systems that incorporate cards, biometric identifiers, and, more recently, mobile-based technologies. As noted by Norman (2011), the transition from mechanical to electronic access control represented an important step toward greater flexibility and scalability in security management [10].

Fig. 1 and Fig. 2 illustrate the technological evolution and comparative characteristics of QR codes within the broader landscape of two-dimensional barcode technologies. Fig. 1 presents a conceptual comparison between QR codes and other matrix codes, such as PDF417, Data Matrix, and MaxiCode, highlighting their advantages in terms of data capacity, printing efficiency, and high-speed readability. Meanwhile, Fig. 2 outlines the chronological development of QR code technology, beginning with its invention in 1994 and progressing through key phases of adoption, including its expansion into marketing and payment systems, integration with IoT environments, and its recent role in advanced security applications such as biometric authentication, blockchain-based systems, and dynamic QR technologies. Together, these figures demonstrate how QR codes have evolved from industrial tracking tools into a foundational component of modern digital security and access control infrastructures.

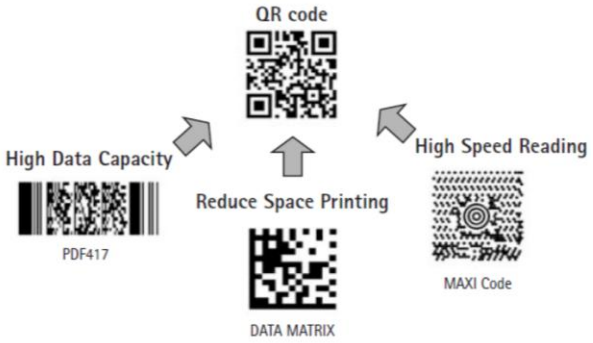

Fig. 1. Evolution of QR codes from manufacturing tracking to modern access control applications [5].

Fig. 2. Evolution of QR code technology.

Despite their advantages, QR-ACS are associated with a number of challenges, including the risk of QR code replication, unauthorized sharing, and potential security breaches resulting from code interception. In their basic form, QR codes do not provide built-in encryption or authentication mechanisms, which makes them vulnerable to different types of attacks. In response to these limitations, several enhanced QR-ACS solutions have been proposed that integrate additional security measures, such as encryption techniques, time-limited QR codes, and multi-factor authentication. These approaches aim to reduce security risks by limiting unauthorized access while preserving the flexibility and usability that characterize QR code-based systems. Nevertheless, the reported effectiveness of such solutions is not consistent across studies, and their performance often depends on the application context and implementation design. As a result, further research remains

necessary to establish standardized and scalable security frameworks that can be reliably applied across different sectors.

The growing research interest in QR-ACS is illustrated in Fig. 3. The figure presents the publication trend of QR-ACS-related research between 2015 and 2024. The data demonstrate a steady growth trajectory, with a noticeable acceleration after 2019, coinciding with the expansion of IoT ecosystems and increased demand for contactless authentication solutions during the COVID-19 pandemic. The upward trend in 2023–2024 suggests sustained research interest, particularly in areas integrating encryption, blockchain, and biometric authentication. This growth pattern confirms that QR-ACS remains an active and evolving research domain, warranting systematic synthesis and structured analysis.

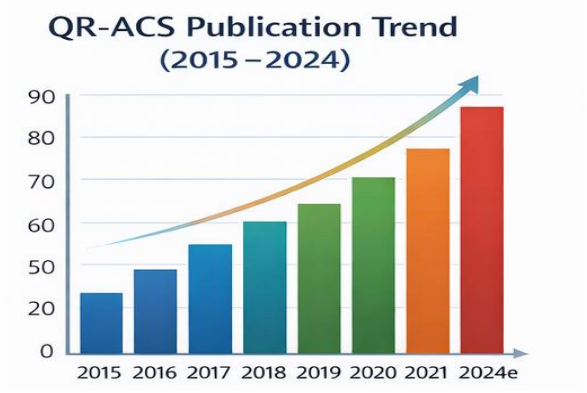

Fig. 3. QR-ACS publication trend (2015–2024).

At a fundamental level, the objective of an access control system is to enforce predefined access policies that protect facilities and information from unauthorized use. The emergence of electronic access control systems during the 1960s marked a significant shift away from purely mechanical solutions. Early implementations relied on magnetic stripe cards to support more dynamic authorization processes, which were later extended through the adoption of RFID (Radio Frequency Identification) technology. According to Rieback, Crispo, and Tanenbaum (2006), RFID-based systems introduced contactless operation alongside encrypted authentication data, thereby reshaping conventional access control mechanisms [11].

Subsequent developments in RFID-based access control further enhanced security capabilities by enabling the integration of authentication, tracking, and monitoring functions within a unified framework [12]. These developments illustrate how access control technologies have continued to adapt in response to increasing security requirements and the growing complexity of modern infrastructures. An overview of access control system architectures and their relationship to QR code-based solutions is illustrated in Fig. 4.

QR codes, commonly referred to as Quick Response codes, were introduced in 1994 by the Japanese company Denso Wave for the purpose of tracking components in vehicle manufacturing. As noted by de Seta (2023), Denso Wave initially developed QR code technology to improve efficiency in automotive production, which later supported its broader adoption [14]. Unlike conventional one-dimensional barcodes, QR codes are two-dimensional and were designed to encode information more efficiently while allowing faster scanning. This design enables QR codes to store various types of data, including URLs, contact details, and encrypted information, contributing to their versatility across different applications [15].

Fig. 4. Overview of access control systems, highlighting QR code-based solutions [13].

The widespread use of QR codes expanded further with the growth of smartphone technology. Smartphones equipped with built-in cameras have played a key role in facilitating quick and convenient QR code scanning in everyday contexts. As explained by Pandey and Awasthi (2020), this capability has supported the adoption of QR codes across multiple domains, ranging from marketing and digital payments to information sharing [16]. In the context of access control systems, QR codes are commonly used to store access credentials or to reference secure credentials maintained in cloud-based platforms. This approach has been described as a practical and scalable solution for managing access in diverse environments, including corporate offices, public venues, and residential settings [17].

Fig. 5 illustrates the structural components of a typical QR code and the arrangement of its functional elements. These components include position markers that assist scanners in detecting the orientation of the code, data modules that store encoded information, and quiet zones that ensure reliable recognition during scanning. Understanding the internal structure of QR codes is essential for explaining how they support efficient data encoding, error correction, and rapid decoding in access control applications.

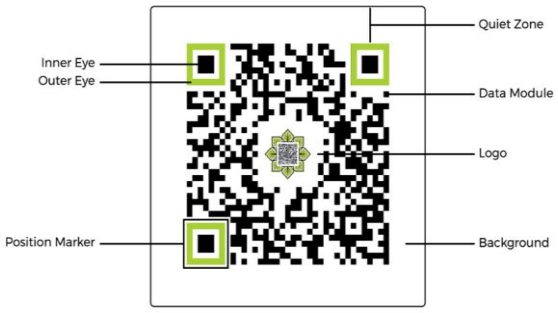

Fig. 5. Structure of a QR code, highlighting key components such as data modules, timing patterns, and error correction blocks [18].

III. Research Methodology

This study follows a systematic review methodology based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure transparency, reproducibility, and rigor in the literature selection process.

A. Data Sources and Search Strategy

A comprehensive literature search was conducted across multiple academic databases, including IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, and Google Scholar. The search focused on studies published between 2015 and 2024 to capture recent developments in QR Code-Based Access Control Systems (QR-ACS). The search queries were constructed using combinations of relevant keywords, including: "QR code access control", "QR authentication", "QR-based security systems", "QR code IoT access control", "secure QR authentication", and "QR-based identity verification". Boolean operators (AND, OR) were used to refine the search and ensure comprehensive coverage of relevant studies.

B. Inclusion and Exclusion Criteria

To ensure relevance and quality, predefined inclusion and exclusion criteria were applied during the screening process. Inclusion criteria:

- Studies published between 2015 and 2024.
- Peer-reviewed journal articles and conference papers.
- Studies focusing on QR code-based authentication or access control systems.
- Studies presenting technical, experimental, or system-level contributions.

Exclusion criteria:

- Non-English publications.
- Studies not directly related to access control or authentication.
- Review papers without technical contribution.
- Short papers, editorials, posters, or non-peer-reviewed content.

C. Screening and Selection Process

The study selection process followed the PRISMA 2020 framework to ensure transparency and reproducibility. As illustrated in Fig. 6, a total of 1,275 records were initially identified from multiple academic databases, including IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, and Google Scholar. After removing duplicate records (n = 352), 923 studies remained for title and abstract screening. During this phase, 668 records were excluded due to irrelevance to QR code-based access control systems. The remaining 255 articles were subjected to full-text review, of which 28 could not be retrieved. A total of 227 studies were assessed for eligibility, leading to the exclusion of 161 papers based on predefined criteria, including lack of relevance, non-QR-based approaches, and non-empirical contributions. Ultimately, 66 studies were included in the final qualitative and quantitative synthesis.

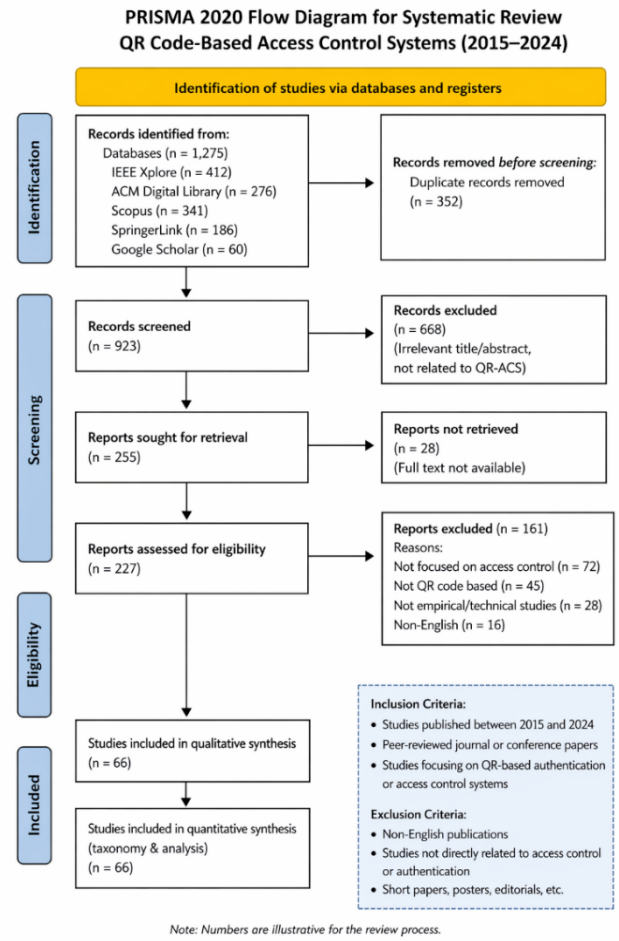

Fig. 6. PRISMA 2020 flow diagram illustrating the study selection process for the systematic review of QR Code-Based Access Control Systems (QR-ACS).

D. Data Extraction and Analysis

For each selected study, relevant data were systematically extracted, including system architecture, authentication mechanisms, security techniques, application domain, and reported limitations. The extracted studies were categorized into thematic groups to support comparative analysis and the development of a structured taxonomy. This categorization enabled the identification of architectural patterns, security trends, and research gaps within QR-ACS.

Additionally, a comparative evaluation was conducted to analyze trade-offs between security strength, system complexity, and deployment feasibility across different QR-ACS implementations.

IV. Literature Review

This literature review examines a broad range of studies that apply QR code-based access control systems across different application domains, including security and surveillance, mobile and IoT systems, transportation and ticketing, and healthcare. The reviewed work reflects the growing interest in QR code technology as a means of supporting authentication, enhancing security, and improving operational efficiency in varied contexts.

Within the area of security and surveillance, several studies investigate the integration of QR codes with complementary technologies such as facial biometrics, encryption techniques, and real-time monitoring. These approaches are generally proposed as alternatives to traditional access control mechanisms, including physical keys and swipe cards, with the intention of improving convenience while maintaining acceptable security levels.

Research focusing on mobile and IoT systems often emphasizes the practical advantages of QR code-based frameworks, particularly their cost efficiency, flexibility, and compatibility with smartphones and IoT infrastructures. These characteristics are frequently cited as factors that enable more streamlined access control and improved user interaction. In a similar manner, studies related to transportation and ticketing explore the use of encrypted QR codes to strengthen e-ticket security, while also acknowledging challenges associated with system interoperability and vulnerability management.

In the healthcare domain, the literature highlights the use of QR codes for controlling access to sensitive patient data and restricted areas, with particular attention given to encryption methods and authentication mechanisms required to protect electronic health records.

Across these application areas, QR code technology is commonly described as adaptable and capable of supporting a range of access control requirements. At the same time, recurring challenges are noted in the literature, including concerns related to scalability, the potential for unauthorized QR code duplication, and the need for supporting technical infrastructure. Taken together, these observations provide a basis for understanding the current use of QR code-based access control systems and point to several areas where further research is needed, especially with respect to security robustness and system interoperability.

A. Security and Surveillance

This section examines the implementation of QR code-based systems in a range of security and surveillance applications. The studies discussed here consider how QR codes are combined with complementary technologies, such as biometric authentication, encryption algorithms, and real-time monitoring, to support access control objectives. Rather than addressing a single use case, the reviewed work covers different application environments and illustrates how QR code-based solutions have been employed to modernize access control mechanisms across multiple contexts.

To enhance system security, QR code-based access control is often integrated with additional security mechanisms such as encryption techniques, biometric authentication, centralized servers, and monitoring components. These technologies work together to ensure secure identity verification, protect transmitted data, and enable continuous monitoring of system activities.

Fig. 7 illustrates a conceptual architecture of QR code-based security and surveillance systems, highlighting the integration of QR authentication with encryption methods, biometric verification, logging mechanisms, and IoT-based monitoring components.

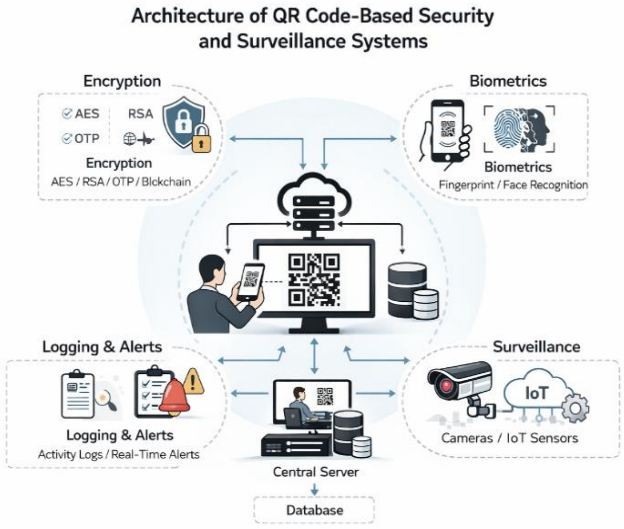

Fig. 7. Architecture of QR code–based security and surveillance systems illustrating the integration of QR authentication with encryption, biometric verification, centralized servers, and monitoring mechanisms.

1) Home security: Home security systems that incorporate QR code technology are often presented as alternatives to traditional key-based solutions, with an emphasis on improved convenience and flexible access management. In many proposed implementations, QR codes are integrated with additional technologies, such as facial recognition and IoT-based automation, to support real-time monitoring and remote control capabilities. These combinations are intended to strengthen residential security while reducing reliance on physical keys, although their effectiveness may vary depending on system design and deployment conditions. Table I summarizes representative studies that apply qr code-based and related technologies to home security scenarios, highlighting common design choices, reported benefits, and frequently noted limitations.

2) Office and workplace security: In office and workplace environments, QR code-based access control systems are increasingly considered as alternatives to traditional authentication methods, such as RFID cards, particularly when combined with encrypted QR codes and multi-factor authentication mechanisms. These systems are commonly proposed to support controlled access to sensitive areas, while also facilitating functions such as monitoring and attendance tracking. Table II summarizes representative studies that examine QR code-based access control solutions in office and workplace settings, highlighting proposed authentication approaches alongside their reported benefits and limitations.

TABLE I. STUDIES RELATED TO HOME SECURITY

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[19]	2014	Residential multi-factor security system	Residential multi-factor security system	Unauthorized entry	Cost-effective multi-layer security	NFC reliability; false PIR triggers
[20]	2022	Wireless home security system	RFID + Fingerprint + Face ID + ESP32-CAM	Weak traditional locks	Multi-factor secure access	System complexity; maintenance
[7]	2018	Smart building access with aesthetic QR	QR + Symmetric encryption + Photo verification	RFID cost; offline verification	Flexible, cost-effective access	Photo verification accuracy; scalability
[21]	2021	IoT-based smart home security	Face recognition (PCA) + IoT	Automated intrusion detection	Low-power real-time monitoring	Limited scalability testing
[22]	2020	Face recognition access control	OpenCV + LBPH + Raspberry Pi	Real-time authentication	Remote access with alerts	Limited scalability
[23]	2020	Biometric door access control	Fingerprint + Arduino + Bluetooth	Device interoperability	Reliable biometric access	Limited large-scale testing
[24]	2020	Dual biometric home security	Face (PCA) + Fingerprint	Unauthorized residential access	Strong biometric authentication	Lighting sensitivity; scalability
[25]	2022	IoT facial recognition security	Haar Cascade + LBPH + Mobile App	Home monitoring automation	92.86% recognition accuracy	Internet dependency; scalability

TABLE II. STUDIES RELATED TO OFFICE AND WORKPLACE SECURITY

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[26]	2022	Secure QR transmission for confidential data (e-tickets, coupons)	QR module modification + Error correction	Weak data protection in standard QR	Increased hidden data capacity; secure QR	Requires secret key access
[27]	2023	Device registration authentication system	QR + Fingerprint + C#/SQL	Paper receipt fraud; inefficient verification	Improved authentication and fraud reduction	User familiarity; hardware maintenance
[28]	2021	Residential IoT access control	QR + SHA-2 + IoT	Replacing physical keys	Improved security; real-time notifications	Scalability; internet dependency

3) University and research lab access control: In universities and research laboratories, QR codes are increasingly deployed in combination with technologies such as biometric authentication and encryption to support access control and attendance management. These approaches are commonly discussed as more flexible and cost-effective alternatives to conventional access control systems, particularly in environments that require frequent user verification and controlled access to specialized facilities. Table III summarizes representative studies that examine QR code-based access control solutions in university and research laboratory settings, highlighting a variety of cryptographic, biometric, and system-level approaches alongside their reported benefits and limitations.

TABLE III. STUDIES RELATED TO UNIVERSITY AND RESEARCH LAB ACCESS CONTROL

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[29]	2018	Secure access control using encrypted QR codes.	QR + RSA + PRNG	Unencrypted QR vulnerabilities.	Improved security; cross-platform compatibility	RSA overhead; higher device processing
[30]	2020	QR-based door access for university labs	QR + Raspberry Pi + Web server	Weak locks; RFID cost/complexity	Cost-effective access control	Preliminary testing; limited scalability
[31]	2017	Smart door security for restricted areas	Bluetooth + Android + Microcontroller	RFID and fingerprint weaknesses	Real-time monitoring; cost-effective	Limited range (9 m); user management issues
[32]	2023	Lab access control with QR and OTP	QR + RSA + AES + TOTP	Unauthorized access prevention	TOTP more secure than HOTP	Limited to lab environments
[8]	2023	QR-based attendance and access tracking	QR + Centralized DB	Manual errors; RF card dependency	Improved accuracy and cost efficiency	QR duplication risk; internet dependency
[33]	2020	QR-based access control with monitoring	QR + Lamport Hash Chain + Web	Security and monitoring challenges	Enhanced security and monitoring	Limited scalability; no usability feedback
[34]	2018	Biometric QR access for universities	QR + Face recognition + OpenCV	Authentication and privacy issues	Improved authentication and privacy	Limited scope; OpenCV constraints
[35]	2021	Secure login for e-exam systems	QR + SHA-256 + MD5	Brute force and unauthorized access	Secure and efficient login	Limited generalizability; missing usability data

4) Public spaces and government facilities: In government buildings and public spaces, QR code-based systems have been applied as part of access control strategies for managing high-traffic environments. These systems are commonly discussed as tools for supporting controlled access to sensitive areas, to reduce the risk of unauthorized entry while maintaining

efficient movement within public facilities. Table IV presents selected studies that address QR code-based access control in public spaces and government facilities, emphasizing emergency scenarios, decentralized authentication, and system-level considerations alongside reported limitations.

TABLE IV. STUDIES RELATED TO PUBLIC SPACES AND GOVERNMENT FACILITIES

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[36]	2018	Emergency access control	QR + Shamir Secret Sharing + ABE	No online authentication in emergencies	Secure offline attribute-based access	Attribute policy dependency; limited disaster testing
[37]	2020	Smartphone QR access control	QR + DES + Embedded system	Security and cost limits of locks/RFID/biometrics	Integrated access and attendance control	Smartphone dependency
[38]	2020	Unified identity platform	QR hybrid encryption + WSN + ZigBee	Fragmented identity systems	Low-power secure authentication	No real-world testing; scalability
[39]	2021	QR access control with monitoring	QR + Web app + ID scanner	QR duplication; setup complexity	Cost-effective access monitoring	Security risks; user adoption issues
[40]	2019	Blockchain QR authentication	QR + One-time QR + Blockchain	Secure decentralized authentication	Improved security via decentralized verification	Scalability; integration challenges

TABLE V. STUDIES RELATED TO HIGH-SECURITY ENVIRONMENTS

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[41]	2019	Biometric passport security	QR + AES + SHA-256 + Biometrics	RFID privacy risks	High-accuracy biometric authentication	Biometric reliability; infrastructure dependency
[42]	2015	LED-QR access authentication	QR + LED tags	Improving QR access security	Enhanced authentication performance	Scalability not evaluated
[43]	2020	Encrypted QR access control	QR + RSA + PRNG	Protecting authorization data	Improved data security	Key management; scalability
[44]	2024	Secure QR encryption for access control	QR + RSA + PRNG	Authorization data protection	Stronger encrypted access control	Limited real-world evaluation

5) High-security environments (e.g., defense or sensitive areas): In high-security environments, such as defense-related or sensitive government facilities, QR code-based systems are often discussed in conjunction with advanced encryption techniques and biometric integration to support stricter access control requirements. These approaches are proposed to manage access to highly restricted areas, where higher assurance levels are typically required compared to conventional access control settings. Table V summarizes studies that address QR code-based access control in high-security environments, including national security and sensitive infrastructure, with a focus on encryption and biometric integration.

In security and surveillance applications, QR code-based systems are commonly discussed as access control solutions that combine QR technology with elements such as encryption, real-time monitoring, and biometric verification. These systems are often proposed as flexible and user-friendly alternatives to traditional security mechanisms, including physical keys and RFID cards, particularly in contexts where cost and ease of deployment are important considerations. At the same time, the literature points to several challenges, including the susceptibility of QR codes to unauthorized duplication and the technical complexity associated with integrating additional security layers such as encryption. Accordingly, further research remains necessary to address these limitations and to assess the suitability of QR code-based systems for wider adoption in high-security environments

B. Mobile and IoT Systems

This section examines the application of QR code technology within mobile and IoT-based systems, with particular attention to its use in access control contexts. The reviewed studies discuss QR codes as cost-effective and flexible solutions that can be integrated with IoT devices to support secure access management. In many cases, these approaches are presented as a means of streamlining access processes while improving overall operational efficiency.

1) Smart home automation: In smart home environments, QR code-based systems are frequently combined with IoT devices to support automated security and access control functions. Such systems are commonly designed to allow homeowners to manage door locks, monitor entry points, and receive notifications through smartphone applications. These features are often highlighted as contributing to improved convenience and remote control capabilities, although their effectiveness may depend on system configuration and network reliability. Table VI summarizes studies that examine smart home automation systems integrating QR codes, IoT devices, and complementary technologies, highlighting proposed approaches, reported outcomes, and commonly noted limitations.

2) Industrial IoT applications: In industrial environments, QR code-based access control systems integrated with IoT technologies are commonly discussed as approaches for supporting security and operational efficiency. Such solutions

are applied to manage access to restricted areas and to assist in the monitoring of assets and personnel within industrial settings. These systems are often presented as part of broader industrial IoT frameworks, where access control is combined with real-time data collection and system management. Table VII highlights a representative approach to QR code-based authentication in industrial IoT contexts, emphasizing performance considerations alongside scalability challenges.

3) Mobile payment systems: In mobile payment systems, QR code-based authentication is commonly discussed as a practical approach for supporting secure and convenient financial transactions. Rather than relying solely on traditional password-based mechanisms, these systems often incorporate multi-factor authentication schemes, such as QR code verification combined with one-time passwords (OTPs). This combination is intended to enhance transaction security while maintaining ease of use for end users. Table VIII presents selected studies that examine the use of QR code-based authentication in mobile payment systems, highlighting multi-factor security approaches alongside practical limitations related to deployment and usability.

TABLE VI. STUDIES RELATED TO SMART HOME AUTOMATION

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[45]	2023	IoT smart door lock security	Bluetooth MAC + Raspberry Pi + Firebase	Weak traditional locks	Remote access and monitoring	Internet and smartphone dependency
[46]	2022	IoT facial recognition gate security	Face recognition + OpenCV + Raspberry Pi	Rising home break-ins	Real-time monitoring and alerts	Lighting and recognition accuracy
[47]	2022	IoT smart home gate access	Face recognition + Arduino + ESP8266	Centralized home security control	Remote monitoring via mobile	Network reliability; integration
[48]	2019	GPS-based smart door lock	GPS + STM32 + XBee	Manual lock limitations	Location-based automated access	GPS accuracy; connectivity
[49]	2020	IoT home automation security	Face detection + Raspberry Pi + IoT sensors	Automated home security	Real-time monitoring and alerts	Internet dependency; lighting issues
[50]	2021	QR access framework for Android	QR + ZXing + Encrypted ID	Lack of QR access frameworks	Flexible QR-based access system	Android focus; limited testing

TABLE VII. STUDIES RELATED TO INDUSTRIAL IOT APPLICATIONS

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[51]	2020	IoT QR authentication security	QRAM (3-layer QR authentication)	Fast and secure IoT authentication	Reduced computation time; improved security	High decryption complexity; scalability

TABLE VIII. STUDIES RELATED TO MOBILE PAYMENT SYSTEMS

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[52]	2010	QR-based user authentication	QR + OTP	Password-based security risks	Dynamic OTP authentication	Requires camera-enabled mobile device
[53]	2021	Secure mobile money authentication	QR + PIN + OTP + Fingerprint + SHA-256 + FIDO	Weak mobile money security	Improved protection against replay and phishing	Biometric device and infrastructure requirements
[54]	2023	Secure QR transactions for MSMEs	QR + GOST encryption	Secure QR payment transactions	Enhanced QR transaction security	Requires specialized QR reader
[55]	2010	Secure online banking authentication	QR + Mobile OTP + SSL/TLS	Phishing and weak authentication	Secure QR banking authentication	Limited testing; small sample

4) Smart Building and Facility Management: Smart buildings increasingly incorporate QR code-based systems as part of their access control, monitoring, and automation strategies. These solutions are commonly discussed in the literature as scalable approaches that support controlled entry to different areas within a building and facilitate integration with existing management systems. By enabling flexible access policies and centralized monitoring, QR code-based approaches are presented as contributing to more efficient facility management and improved security practices. Table IX highlights a representative application of QR code-based access control in smart building facilities, emphasizing shared access management and system scalability considerations.

TABLE IX. STUDIES RELATED TO SMART BUILDING AND FACILITY MANAGEMENT

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[56]	2019	Smart campus locker access	QR + IoT + Smart lock + Mobile app	Traditional locker limitations	Flexible shared locker access	Prototype stage; scalability

QR code-based access control in mobile and IoT systems is often discussed as an adaptable and scalable approach for securing connected devices and services. By relying on mobile platforms and IoT networks, these systems can support flexible access management across a range of environments, from residential automation to industrial settings. At the same time, the literature points to several ongoing challenges, including the need for reliable connectivity, compatibility across heterogeneous devices, and the diverse security requirements inherent to IoT ecosystems. As a result, future research is frequently directed toward the development of standardized frameworks that can facilitate cross-platform integration and support more robust and scalable QR code-based access control solutions within IoT environments.

C. Transportation and Ticketing Systems

In transportation and ticketing applications, QR code-based systems have been explored as a means of streamlining ticket verification processes and supporting secure transactions. Existing studies emphasize the use of encrypted QR codes to enable contactless ticketing, which can improve efficiency by automating procedures such as check-in and seat verification. These approaches are often associated with reductions in manual errors and improvements in operational workflows within public transportation systems. However, the literature also highlights practical challenges, including infrastructure requirements for managing biometric data and potential security concerns related to user-generated passwords in electronic ticketing systems. Addressing these issues may require further advancements in QR code encryption techniques, as well as improved system interoperability and deployment strategies. Table X summarizes representative studies that investigate the use of QR code-based authentication in transportation and ticketing systems, highlighting biometric integration, encrypted e-ticketing approaches, and associated deployment challenges.

TABLE X. STUDIES RELATED TO TRANSPORTATION AND TICKETING

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[57]	2019	Train ticketing and seat verification	QR + Fingerprint biometrics	Manual ticket verification errors	Automated check-in; improved security	Infrastructure requirements
[58]	2010	Secure QR e-ticket system	QR + Block cipher + Password	Password-based security risks	Improved ticket accessibility	Password theft; device compatibility

D. Healthcare Systems

In healthcare applications, QR code technology is primarily explored as a mechanism for securing access to sensitive patient information and supporting data privacy within electronic health record (EHR) systems. Existing studies investigate the use of encryption techniques and cloud-based storage to restrict data access to authorized personnel. At the same time, the literature identifies several challenges, including key management in large-scale deployments and the need for extensive testing to assess system performance in real-world healthcare settings. Overall, these studies suggest that QR code-based approaches have the potential to strengthen privacy protection in healthcare environments, while also indicating areas that require further development and validation. Table XI presents studies that examine the application of QR codes in healthcare systems, with a particular focus on securing access to sensitive patient information. The reviewed studies discuss encryption techniques and authentication frameworks that are intended to support data protection in electronic health record (EHR) systems.

TABLE XI. STUDIES RELATED TO HEALTHCARE SYSTEMS

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[59]	2022	Secure QR data transfer	QR + RSA	Personal data privacy	Secure encrypted data transfer	Key management complexity
[60]	2020	Secure EHR access via QR	QR + Cloud storage	Protecting sensitive health data	Secure EHR access framework	Limited real-world evaluation

E. Other Fields

In addition to the more established application domains, QR code-based systems have also been explored in a range of other environments, including hostel management, smart locker systems, and identity tracking applications. Studies in these areas describe how QR codes can be applied to support identity management, enhance security, and automate certain administrative processes. Alongside the reported advantages, such as reduced dependence on manual record-keeping, the literature also identifies several limitations. These include the need for reliable network connectivity and the possibility of scanning-related issues, particularly in settings with limited technical infrastructure. Overall, these studies reflect a growing research interest in extending the use of QR codes to diverse application scenarios beyond traditional access control systems. Table XII presents studies that examine the application of QR code technology in other fields, such as hostel management and smart building environments. The reviewed studies discuss how QR codes can be used to support identity management, improve security in residential and commercial contexts, and enable integration with cloud platforms and sensor networks for real-time monitoring.

The comparative analysis of QR Code-Based Access Control Systems (QR-ACS) reflects a wide range of applications that are shaped by specific security requirements and environmental conditions. The reviewed studies span multiple contexts, including educational institutions, emergency management scenarios, and data-sensitive environments, illustrating the flexibility of QR-ACS in addressing different access control needs.

TABLE XII. STUDIES RELATED TO OTHER FIELDS

Ref	Year	Focus Area	Algorithm	Challenges addressed	Findings	Limitations
[61]	2021	Hostel identity and access monitoring	Hostel identity and access monitoring	Manual monitoring inefficiency	Accurate movement tracking	Infrastructure dependency
[62]	2022	QR smart locker system	QR + ESP8266 + Smart lock	Traditional key limitations	Secure locker access	Response delay

In academic and institutional settings, QR-ACS are commonly applied to support identity verification and access management, often with the goal of reducing reliance on physical tokens and improving user convenience. By contrast, systems designed for emergency or critical situations tend to emphasize encryption-enhanced QR codes, allowing secure access to be maintained even when conventional infrastructure is unavailable.

From a technological perspective, many of the proposed systems integrate encryption techniques, such as RSA, and in some cases combine QR codes with biometric authentication to strengthen protection against unauthorized access. While these approaches contribute to improved security, the literature also consistently reports challenges related to QR code tampering, unauthorized duplication, system scalability, and the complexity of implementing advanced cryptographic mechanisms across diverse environments.

The distribution of QR-ACS applications across domains is summarized in Fig. 8. The figure illustrates the distribution of QR-ACS applications across different operational domains. Home security and university laboratory environments constitute the largest proportion of reported implementations, reflecting the technology's suitability for cost-sensitive and semi-controlled environments. Public facilities and IoT-integrated smart systems also represent significant adoption sectors. In contrast, high-security and healthcare applications show comparatively lower representation, indicating potential research and deployment gaps in environments requiring stricter compliance, scalability validation, and regulatory assurance.

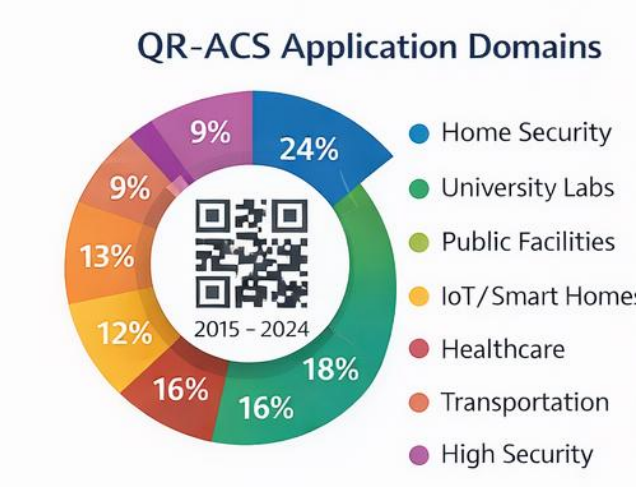

Fig. 8. Distribution of QR-ACS application domains.

Overall, these recurring challenges indicate the need for continued research and refinement of QR-ACS to improve reliability, scalability, and practical deployment.

The ongoing development of QR code technologies and their integration with emerging security frameworks suggest that QR-ACS remains an active area for both academic investigation and real-world application. Fig. 9 presents a structured taxonomy of QR Code-Based Access Control Systems (QR-ACS), synthesizing the diverse implementations identified in the reviewed literature. The taxonomy categorizes QR-ACS into five primary classes based on authentication architecture and security mechanisms:

- Static QR Systems, which rely on fixed credentials and minimal computational complexity, are predominantly observed in early home security and institutional prototypes (Tables I and III). While cost-effective, these systems remain vulnerable to duplication and replay attacks.
- Dynamic QR Systems, including time-based and session-based implementations, are introduced to mitigate replay and reuse risks. These systems are commonly applied in university laboratories, transportation ticketing, and public facility management (Tables III and X), where temporal validity enhances security robustness.
- Encrypted QR Systems, incorporate cryptographic algorithms such as AES, RSA, or hybrid encryption to protect embedded credentials. As shown in Tables III, IV, V, and XI, encryption-based approaches are widely adopted in healthcare, high-security, and emergency-response environments to address confidentiality and integrity concerns.
- Multi-Factor QR Systems, combining QR authentication with biometric verification, one-time passwords (OTP), or blockchain logging, are increasingly reported in office, financial, and high-security settings (Tables II, V, and VIII). These systems significantly strengthen authentication assurance but introduce higher computational and infrastructural complexity.
- IoT-Integrated QR Systems, observed across smart homes, industrial IoT, and facility management contexts (Tables VI, VII, and IX), embed QR authentication within connected infrastructures, enabling real-time monitoring and context-aware access control.

This taxonomy provides a conceptual framework that clarifies architectural distinctions, highlights evolutionary security enhancements, and supports comparative analysis across application domains. By structuring the literature into these categories, the taxonomy contributes to a clearer understanding of design trends and emerging directions in QR-ACS research. Fig. 9 presents a structured taxonomy of QR Code-Based Access Control Systems (QR-ACS).

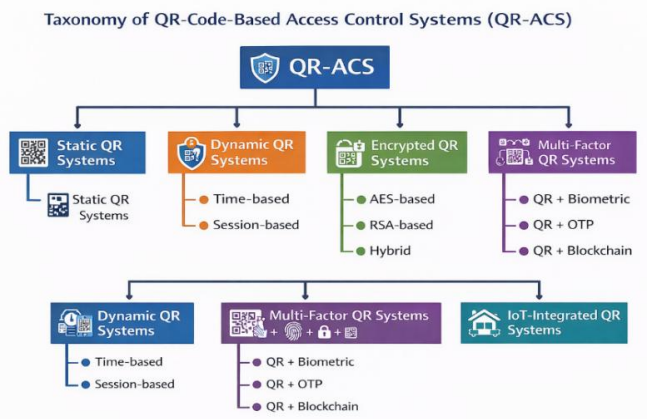

Fig. 9. Two-dimensional architectural model of QR-ACS.

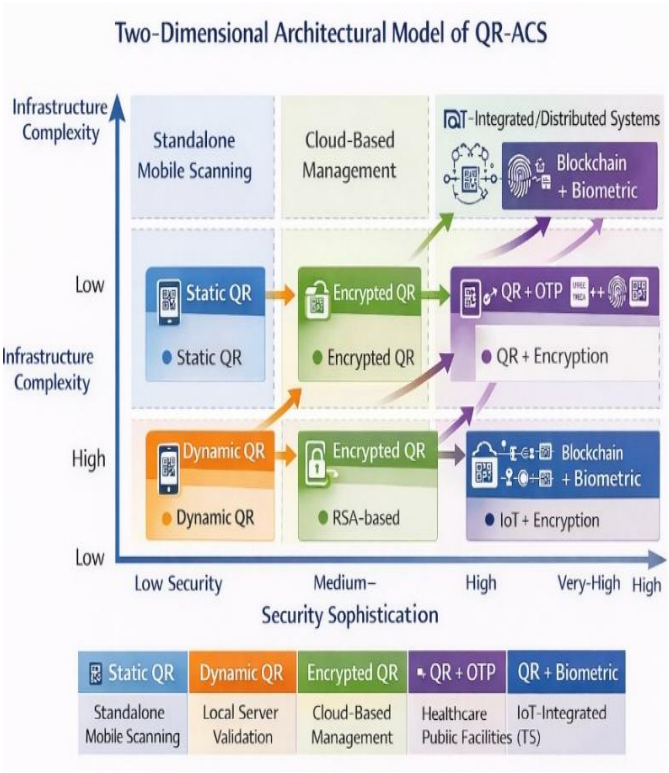

Fig. 10. Two-dimensional architectural model of QR-ACS.

Fig. 10 extends the taxonomy into a two-dimensional architectural model that classifies QR-ACS implementations based on security sophistication and infrastructure complexity. Systems positioned in the lower-left quadrant, such as static QR implementations, exhibit low computational overhead but limited resistance to duplication and replay attacks. Moving toward the upper-right quadrant, multi-factor and blockchain-integrated systems demonstrate enhanced security robustness at the cost of increased infrastructural and computational demands. This model highlights the inherent trade-off between deployment simplicity and security strength, enabling clearer benchmarking of QR-ACS designs across different operational environments.

Table XIII provides a structured comparison of QR-ACS categories derived from the proposed taxonomy. The analysis shows that as systems evolve from static to multi-factor and blockchain-integrated architectures, replay resistance and authentication assurance increase significantly. However, this improvement is accompanied by greater infrastructural requirements and system complexity. The table reinforces the trade-offs illustrated in the two-dimensional architectural model and provides a practical reference for selecting QR-ACS architectures based on deployment constraints and security requirements.

V. Current Technologies and Applications

The application of QR Code-Based Access Control Systems (QR-ACS) extends across a wide range of environments, where the technology is employed to support security requirements and improve operational processes. This section reviews the key technologies currently associated with QR-ACS and discusses how they are applied in real-world contexts across different sectors.

Fig. 11 illustrates several application environments and technological trends that have influenced the deployment of QR code-based access control systems. These environments include digital services, smart environments, and data-driven infrastructures where secure and contactless authentication methods are increasingly required. The figure also highlights broader technological developments such as remote monitoring, data integration, and privacy-aware systems, which have contributed to expanding the role of QR-based technologies in modern security and operational management.

TABLE XIII. Comparative Characteristics of QR-ACS Categories

Category	Credential Type	Replay Resistance	Infrastructure Need	Typical Domains (Tables)
Static QR	Fixed	Low	Low	Home Security (T1), Early Labs (T3)
Dynamic QR	Time/Session-based	Medium–High	Medium	Labs (T3), Transportation (T10)
Encrypted QR	AES/RSA	High	Medium	Healthcare (T11), Public Facilities (T4), High Security (T5)
Multi-Factor QR	QR + OTP/Bio	Very High	High	Offices (T2), Finance (T8), High Security (T5)
IoT-Integrated QR	Context-aware	Variable	High	Smart Homes (T6), Industrial IoT (T7), Smart Buildings (T9)

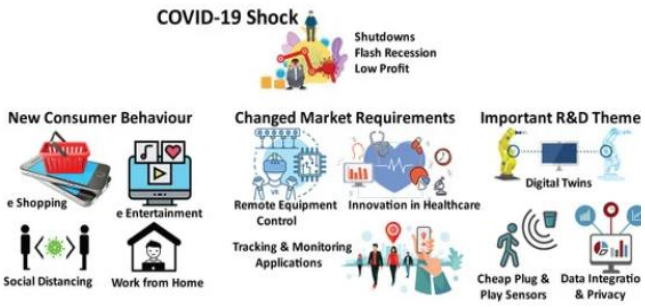

Fig. 11. Overview of application environments for QR code-based access control systems, including smart homes, healthcare, industrial settings, and high-security facilities [63].

A. Technological Innovations

Recent developments in QR-ACS have focused on improving the security of data encoded within QR codes through the use of cryptographic techniques. Many proposed systems employ encryption algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) to protect sensitive information from unauthorized access or manipulation. Previous studies note that QR codes have increasingly been adopted for security-related applications when combined with encryption mechanisms that support data confidentiality and integrity [64].

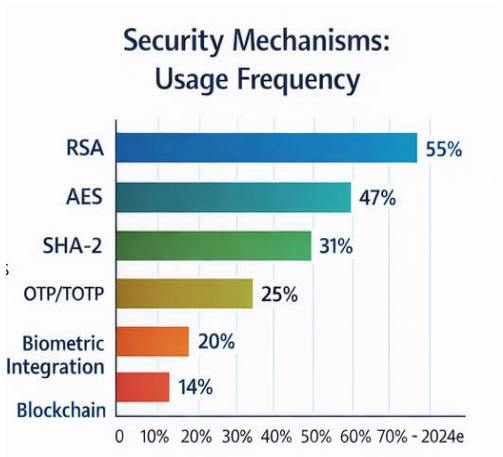

Fig. 12. Security mechanism usage frequency in QR-ACS.

In addition, the integration of cloud-based technologies has enabled more flexible management of QR codes. Cloud platforms allow QR codes to be updated dynamically and managed centrally, reducing the need for physical interaction and supporting scalable deployment in distributed environments [65]. The relative adoption frequency of security mechanisms is illustrated in Fig. 12. The figure compares the relative frequency of security mechanisms integrated within QR-ACS implementations. As shown, RSA and AES encryption dominate the literature, reflecting their widespread adoption for protecting QR-encoded credentials. Hash-based mechanisms such as SHA-2 are moderately represented, primarily in login authentication contexts. Multi-factor authentication techniques, including OTP/TOTP and biometric integration, appear less frequently but demonstrate increasing adoption in recent years. Blockchain-based logging mechanisms remain emerging but show promise for enhancing transparency and tamper resistance. This distribution suggests that encryption remains foundational, while decentralized and biometric security layers are still developing.

B. Biometric Integration

Another area of development in QR-ACS involves the combination of QR code authentication with biometric verification methods, such as facial recognition and fingerprint scanning. In these systems, QR codes are typically used as an initial authentication step, followed by biometric verification to confirm user identity. Studies suggest that combining encrypted QR data with biometric information can provide an additional layer of security compared to traditional single-factor access control methods [66].

This approach has been explored particularly in environments that require higher security levels, where layered authentication mechanisms can help reduce the risk of unauthorized access.

C. IoT and Smart Environments

In smart homes and smart buildings, QR-ACS are often integrated with Internet of Things (IoT) infrastructures to support more adaptive access control solutions. These systems can interact with sensors, actuators, and monitoring devices to adjust access permissions based on contextual factors such as time, location, or environmental conditions. Existing research indicates that IoT-enabled QR-based access control frameworks can enhance system responsiveness and support real-time monitoring when combined with encrypted communication and authentication mechanisms [67].

For example, access to specific areas within a smart building may be regulated not only by user identity but also by predefined environmental or operational conditions.

D. Public and Commercial Applications

QR-ACS has also been adopted in a variety of public and commercial settings, including transportation systems, entertainment venues, and corporate facilities. In such environments, QR codes are commonly used to manage access efficiently, particularly in high-traffic scenarios. Prior studies reported that QR-based access control can support crowd management and streamline entry procedures by reducing reliance on physical tickets or access cards [67].

In public transportation systems, for instance, QR codes are frequently used to facilitate contactless entry and verification, contributing to improved operational efficiency during peak usage periods.

E. Healthcare and Institutional Use

In healthcare and institutional environments, QR-ACS are primarily employed to control access to restricted areas and sensitive information, such as patient records and clinical facilities. These systems can be configured to grant access only to authorized personnel while maintaining detailed access logs for auditing and compliance purposes. Research has shown that QR-based authentication mechanisms, particularly when combined with biometric verification, can support enhanced protection of patient data and restricted zones [68].

During health emergencies, including the COVID-19 pandemic, QR-based systems have also been utilized to manage patient flow and visitor access in a contactless manner, helping institutions maintain safety protocols while reducing physical interaction [65].

VI. Discussion

The review of QR Code-Based Access Control Systems (QR-ACS) provides several insights into both the strengths of these systems and the challenges that continue to affect their deployment, as in Table XIV. By examining studies across different application domains, this review highlights recurring technical, operational, and organizational issues that influence the effectiveness of QR-ACS, while also pointing to areas where further research may contribute to more robust implementations.

TABLE XIV. Security Strength Comparison

Mechanism	Duplication Resistance	Replay Protection	Scalability	Complexity
Static QR	Low	Low	High	Low
Encrypted QR	Medium	Medium	Medium	Medium
QR + OTP	High	High	Medium	Medium
QR + Biometric	Very High	High	Low-Medium	High
Blockchain QR	Very High	Very High	Medium	Very High

To enhance the practical applicability of the proposed taxonomy, a qualitative risk assessment matrix is introduced. The matrix evaluates key threats based on likelihood and impact, enabling prioritization of security measures, as Table XV. The analysis indicates that duplication and replay attacks represent the most critical risks in QR-ACS, particularly in static implementations, while biometric spoofing, although less frequent, poses severe consequences in high-security environments.

TABLE XV. Risk Assessment of QR-ACS Threats

Threat Type	Likelihood	Impact	Risk Level
QR Code Duplication	High	Medium	High
Replay Attacks	Medium	High	High
Biometric Spoofing	Low	Very High	High
Device Theft	Medium	Medium	Medium
Insider Misuse	Low	High	Medium

The findings indicate a clear trade-off between system security and deployment complexity. While multi-factor and blockchain-based QR-ACS provide higher resistance against attacks, they require significant infrastructural support and computational overhead. Conversely, lightweight QR systems offer scalability but remain vulnerable to duplication and replay attacks. This trade-off suggests that no single architecture is universally optimal; instead, system design should be guided by application-specific security requirements and operational constraints.

Moreover, the increasing integration of QR-ACS with IoT environments introduces new attack surfaces, particularly related to device-level vulnerabilities and network security. This highlights the need for cross-layer security frameworks that combine cryptographic protection, device authentication, and real-time monitoring.

VII. Challenges in Current QR-ACS

One of the most frequently discussed challenges in the literature relates to security vulnerabilities. Although many systems incorporate encryption techniques and, in some cases, biometric verification, QR-ACS can still be exposed to risks such as code duplication, spoofing, and unauthorized access. In particular, systems that rely on static QR codes may be more susceptible to misuse unless supported by dynamic generation and validation mechanisms.

Another limitation concerns the dependence on specific hardware, especially smartphones and dedicated scanning devices. While this reliance is feasible in many contexts, it can restrict deployment in environments where access to such technology is limited or economically impractical. To provide a structured understanding of these risks, Fig. 13 illustrates the threat landscape associated with QR-ACS implementations. Fig. 6 illustrates the threat landscape associated with QR Code-Based Access Control Systems (QR-ACS). The model categorizes vulnerabilities into code-level threats (e.g., duplication and replay attacks), authentication-layer threats (e.g., biometric spoofing and static QR reuse), and infrastructure-level risks (e.g., insider misuse and device theft). The figure highlights that static QR implementations are particularly vulnerable to duplication and replay-based exploitation, whereas systems integrating biometric verification and dynamic QR generation exhibit reduced exposure but introduce new attack surfaces related to biometric spoofing and device compromise. This layered threat perspective reinforces the need for multi-factor authentication and dynamic credential management in next-generation QR-ACS frameworks.

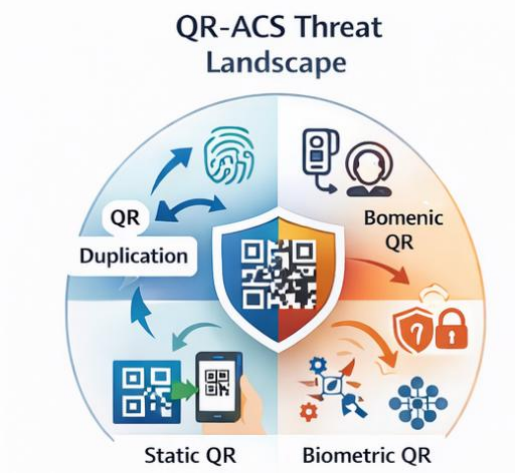

Fig. 13. QR-ACS threat model landscape.

Privacy considerations also emerge as a significant concern, especially in systems that integrate biometric data or personal identifiers. Ensuring compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), is essential for maintaining user trust and safeguarding sensitive information.

In addition, the lack of standardized protocols across different QR-ACS implementations often leads to interoperability challenges. As these systems are adopted in diverse sectors, inconsistencies in design and communication standards can hinder seamless integration with existing security infrastructures.

VIII. Future Research Directions

The findings of this review suggest several directions for future research. Enhancing security protocols remains a priority, particularly through the development of cryptographic techniques that can be efficiently embedded within QR-based systems. Emerging approaches, such as blockchain-based access logging, have also been discussed in the literature as potential solutions for improving transparency and traceability. Expanding accessibility represents another important research avenue. Future work may explore alternatives to smartphone-dependent systems, including low-cost scanning devices or hybrid authentication models that combine QR codes with other access control mechanisms.

To highlight areas requiring further investigation, Fig. 14 presents a structured research gap matrix. The figure presents a structured research gap matrix synthesizing the maturity of QR-ACS research across key dimensions. While encryption techniques are widely implemented across most domains, blockchain integration and large-scale real-world validation remain underexplored, particularly in public facilities and high-security environments. Scalability testing is inconsistently addressed, with many studies limited to prototype-level validation. The matrix highlights that although technical feasibility has been demonstrated, empirical deployment studies and interoperability frameworks are still insufficient. These gaps underscore the need for standardized evaluation methodologies and cross-domain benchmarking in future QR-ACS research.

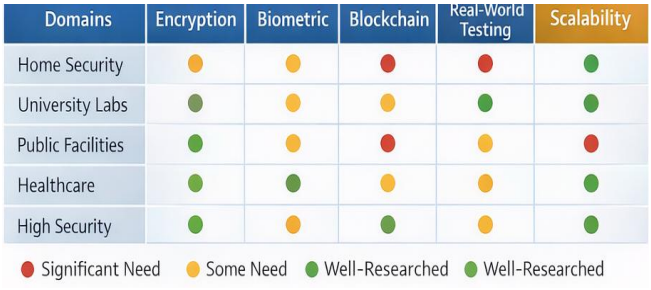

Fig. 14. Research gap matrix (2015–2024).

Dynamic QR code generation is also widely recognized as a promising approach to strengthening security. Techniques that enable real-time code generation and expiration could reduce the risk of unauthorized reuse, while adaptive methods based on usage patterns may further improve access control reliability.

Privacy-preserving frameworks require continued attention as well. Research focusing on data anonymization, secure storage, and regulatory compliance can contribute to the development of QR-ACS that balances security requirements with user privacy.

Finally, cross-industry standardization is essential for supporting large-scale deployment. Collaborative efforts among academic researchers, industry stakeholders, and regulatory authorities may facilitate the creation of interoperable standards that enhance scalability and adoption across different application domains.

IX. Conclusion

This systematic review has examined the evolution and current state of QR Code-Based Access Control Systems (QR-ACS), drawing on a wide range of studies that reflect their application across residential, institutional, commercial, and high-security environments. The reviewed literature indicates that QR-ACS offers flexible and cost-effective solutions for access control, particularly when combined with encryption techniques, biometric verification, and cloud-based management.

At the same time, the findings highlight several persistent challenges that must be addressed to ensure reliable and secure deployment. These challenges include security vulnerabilities, privacy concerns, hardware dependency, and interoperability limitations. Addressing such issues is critical for improving the robustness of QR-ACS and supporting their integration into complex security infrastructures.

Future research plays a key role in advancing this field. Continued efforts are needed to develop stronger security mechanisms, explore more inclusive and accessible system designs, and establish standardized frameworks that promote interoperability and scalability. Equally important is the need to incorporate privacy-preserving approaches that align with international data protection regulations and user expectations.

Overall, QR Code-Based Access Control Systems demonstrate significant potential to influence the future of access management in increasingly digital environments. With sustained research, careful system design, and cooperation between academia, industry, and regulatory bodies, QR-ACS can evolve into more secure, efficient, and user-centered access control solutions.

References

[1] M. Adedoyin and F. Olukoya, Development of a Smart Lock System using QR Code Technology. AJERD. doi: 10.53982/ajerd.

[2] G. Tejaswai et al., "Development of an IoT-Based QR Code Access Control and Payment System using Arduino and ESP8266"," Journal of Science and Technology, vol. 9, no. 06, pp. 20–32, 2024, doi: 10.46243/jst.2024.v9.i06.pp20-32.

[3] G. Petrea, C. Vlad, C. Aramă, M. Crăciun, and B. Ionescu, "QR code based access control system for hotels," Analele Universităţii" Dunărea de Jos" din Galaţi. Fascicula II, Matematică, fizică, mecanică teoretică/Annals of the" Dunarea de Jos" University of Galati. Fascicle II, Mathematics, Physics, Theoretical Mechanics, vol. 43, pp. 121–126, 2020.

[4] J. B. Awotunde, A. E. Adeniyi, A. L. Imoize, Y. Mejdoub, and Z. Abdualazizu, "A Mobile Visitor Management System Using a QR Code and PIN for Access Control," in International Conference on Connected Objects and Artificial Intelligence, Springer, 2024, pp. 192–198.

[5] S. Kaushik, "Steganography with Visual Secret Sharing Scheme," International Journal of Advanced Computer Science and Applications, vol. 2, Nov. 2011.

[6] M. Hara, "Development and popularization of QR code—Code development pursuing reading performance and market forming by open strategy—," National Institute of Advanced Industrial Science and Technology, 2019.

[7] P. C. Huang, C. C. Chang, Y. H. Li, and Y. Liu, "Efficient access control system based on aesthetic QR code," Pers. Ubiquitous Comput., vol. 22, no. 1, pp. 81–91, Feb. 2018, doi: 10.1007/s00779-017-1089-y.

[8] A. Jain, A. Panwar, Mohd. Azam, and R. Khanam, "Smart door access control system based on QR code," International Journal of Informatics and Communication Technology (IJ-ICT), vol. 12, no. 2, p. 171, Aug. 2023, doi: 10.11591/ijict.v12i2.pp171-179.

[9] R. Khatri, T. Shaikh, N. Gundecha, O. Kathe, K. Tiwari, and B. Tech, "QR Code Based Access Control System," 2023. Accessed: Nov. 17, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:259905457.

[10] T. L. Norman, Electronic access control. Elsevier, 2011.

[11] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "The evolution of RFID security," IEEE Pervasive Comput., vol. 5, pp. 62–69, 2006.

[12] E. Edwards and P. Orukpe, "Development of a RFID Based Library Management System and User Access Control," Nigerian Journal of Technology, vol. 33, no. 4, p. 574, Sep. 2014, doi: 10.4314/njt.v33i4.19.

[13] J. Yang, Y. Zhang, and C. J. M. Lanting, "Exploring the Impact of QR Codes in Authentication Protection: A Study Based on PMT and TPB," Wirel. Pers. Commun., vol. 96, no. 4, pp. 5315–5334, Oct. 2017, doi: 10.1007/s11277-016-3743-5.

[14] G. de Seta, "QR code: The global making of an infrastructural gateway," Global Media and China, vol. 8, no. 3, pp. 362–380, Sep. 2023, doi: 10.1177/20594364231183618.

[15] S. Kumar and M. L. Nirmal, "Advanced Visual Cryptography Secret Sharing Schemes Based on QR Codes: A Survey," Dogo Rangsang Research Journal, vol. 11, no. 01, 2021.

[16] A. AWASTHI and A. PANDEY, "Steganography with Visual Secret Sharing Scheme Based QR Code Application: A Survey," Dogo Rangsang Research Journal, vol. 10, no. 07, Jul. 2020.

[17] U. Emenike, "Design and Implementation of a Business Networking App Using or Code," 2016, doi: 10.13140/RG.2.2.34012.60802.

[18] H. Gupta, S. Avasthi, and D. a, "ScanKaro: An QR Code-Based Menu Application for Restaurants," in Artificial Intelligence and Communication Technologies, Soft Computing Research Society, 2023, pp. 945–951. doi: 10.52458/978-81-955020-5-9-90.

[19] M. Kamal Hossain, S. Software Engineer, and M. Mynuddin, "International Journal of Modern Embedded System (IJMES) Design and Implementation of Smart Home Security System Prodip Biswas 2 nd," 2014. [Online]. Available: http://ijmes.info

[20] S. Dharme, "Door Lock Security System Using Recent Technology," Int. J. Res. Appl. Sci. Eng. Technol., vol. 10, no. 1, pp. 684–686, Jan. 2022, doi: 10.22214/ijraset.2022.39812.

[21] N. Susmitha, P. Sindhuja, R. M. Krishna, and B. Mamatha, "HOME SECURITY AND AUTOMATION SYSTEMBASED ON AI," Complexity International Journal (CIJ), vol. 25, pp. 5–6, 2021, [Online]. Available: http://cij.org.in/Currentvolumissue2502.aspx1593

[22] K. T. Reddy, "Intelligent Door Lock System with Face Recognition," Int. J. Res. Appl. Sci. Eng. Technol., vol. 8, no. 5, pp. 364–371, May 2020, doi: 10.22214/ijraset.2020.5060

[23] N. Ghodekar, K. Wagh, R. Kale, S. Kadekar, M. Vijay, and N. Kukre, "Door Lock Control using Wireless Biometric," International Research Journal of Engineering and Technology, 2020, [Online]. Available: www.irjet.net

[24] S. Lakshminarayanan et al., "Home Security System Based on Finger Print and Face Recognition," International Research Journal of Engineering and Technology, 2020.

[25] S. Marrapu, S. Satyanarayana, V. ArunKumar, and J. D. S. K. Teja, "Smart home based security system for door access control using smart phone," International Journal of Engineering and Technology(UAE), vol. 7, no. 1, pp. 249–251, 2018, doi: 10.14419/ijet.v7i1.9247.

[26] P. Y. Lin, W. S. Lan, Y. H. Chen, and W. C. Wu, "A Confidential QR Code Approach with Higher Information Privacy," Entropy, vol. 24, no. 2, Feb. 2022, doi: 10.3390/e24020284.

[27] M. F. Jamal and N. Rahim, "Fingerprint and Qr Code Based Authentication System at Pusat Servis Komputer JB," Applied Information Technology And Computer Science, vol. 4, no. 1, pp. 205–223, 2023, doi: 10.30880/aitcs.2023.04.01.013.

[28] P. Satanasaowapak, W. Kawseewai, S. Promlee, and A. Vilamat, "Residential access control system using QR code and the IoT," International Journal of Electrical and Computer Engineering, vol. 11, no. 4, pp. 3267–3274, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3267-3274.

[29] V. Susukailo and Y. Lakh, Access control system based on encryption in QR-Code technology. IEEE, 2018. doi: 10.1109/IDAACS-SWS.2018.8525779.

[30] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, Development of Web-Based Smart Security Door Using QR Code System. IEEE, 2020.

[31] I. Ishrat, W. M. Ali, S. Ghani, S. Sami, M. Waqas, and F. Aftab, "SMART DOOR LOCK SYSTEM WITH AUTOMATION AND SECURITY," Sci.Int.(Lahore), vol. 29, no. 1, pp. 73–76, 2017.

[32] H. Alsalem et al., "Laboratory Access Implementing QR Code Authentication Using OTP," International Journal on Cybernetics & Informatics, vol. 12, no. 5, pp. 121–141, Aug. 2023, doi: 10.5121/ijci.2023.120511.

[33] H. Park, T. Kim, G. Kim, W. Jang, K. Lee, and S. Y. Lee, "Improvement of QR Code Access Control System Based on Lamport Hash Chain," in Advances in Intelligent Systems and Computing, Springer Verlag, 2020, pp. 824–833. doi: 10.1007/978-3-030-22263-5_79.

[34] L. Kakwete Musambo and J. Phiri, "Student Facial Authentication Model based on OpenCV's Object Detection Method and QR Code for Zambian Higher Institutions of Learning," 2018.

[35] E. A. Amusan, A. O. Popoola, and S. A. O. Ogirima, "Securing Logins in Electronic Examination Systems for Tertiary Institutions Using Quick Response Code (QR) Technology and Multiple Hashing Algorithms," Asian Journal of Research in Computer Science, pp. 23–34, Sep. 2021, doi: 10.9734/ajrcos/2021/v11i330264.

[36] S. Belguith, S. P. Gochhayat, M. Conti, and G. Russello, "Emergency access control management via attribute based encrypted QR codes," in 2018 IEEE Conference on Communications and Network Security, CNS 2018, Institute of Electrical and Electronics Engineers Inc., Aug. 2018. doi: 10.1109/CNS.2018.8433186.

[37] Y. Hong, "Design of Intelligent Access Control System Based on des Encrypted QR Code," in Proceedings of 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications, AEECA 2020, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 1005–1008. doi: 10.1109/AEECA49918.2020.9213475.

[38] X. Xiong, S. Zhang, S. Wang, and J. Crawford, "Intelligent Identity Authorization System Design Based on WSN and Cloud Platform," U.P.B. Sci. Bull., Series C, vol. 82, no. 3, p. 2020, 2020.

[39] Y. Yan, Z. Zou, H. Xie, Y. Gao, and L. Zheng, "An IoT-Based Anti-Counterfeiting System Using Visual Features on QR Code," IEEE Internet Things J., vol. 8, no. 8, pp. 6789–6799, Apr. 2021, doi: 10.1109/JIOT.2020.3035697.

[40] J. Y. Kim, Y. Hoon Jung, D. S. Yang, and M.-S. Jun, "Implementation of Integrated Authentication Service using Blockchain and One Time QR Code for Access Control in U-city Environment," International Journal of Advanced Research in Big Data Management System, vol. 3, no. 2, pp. 15–20, 2019, doi: 10.21742/ijarbms.2019.3.2.03.

[41] Z. H. Choudhury and M. M. A. Rabbani, "Biometric Passport for National Security Using Multibiometrics and Encrypted Biometric Data Encoded in the QR Code," Journal of Applied Security Research, vol. 15, no. 2, pp. 199–229, Apr. 2019, doi: 10.1080/19361610.2019.1630226.

[42] Y. Chung, S. Jung, J. Kim, J. Lee, and J. Cha, "LED-QR Authentication Technology for Access Control and Security," International journal of advanced smart convergence, vol. 4, no. 2, pp. 69–75, Nov. 2015, doi: 10.7236/ijasc.2015.4.2.69.

[43] A. Mohammed Ali and A. K. Farhan, "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document," IEEE Access, vol. 8, pp. 27448–27458, 2020, doi: 10.1109/ACCESS.2020.2971779.

[44] A. Palaniappan, L. P. Veilumuthu, and R. P. S. Louis, "Enhancing Security Through QR Code and Enriched Blowfish Cryptography for Sensitive Data," Springer, Cham, 2024.

[45] K. A. Hashim, H. H. Qasim, A. E. Hamzah, O. A. Hasan, and M. Al-Jadiri, "Door lock system based on internet of things and Bluetooth by

using Raspberry Pi," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 5, pp. 2753–2762, Oct. 2023, doi: 10.11591/eei.v12i5.5134.

[46] F. Yahya, F. A. Hazri, and M. S. M. Kassim, "Entrance monitoring and authentication IoT based system," in AIP Conference Proceedings, American Institute of Physics Inc., Nov. 2022. doi: 10.1063/5.0119671.

[47] A. Fadiga, M. Agarwal, and P. Kaushik, "Home security based on Internet of things Review paper," International Research Journal of Engineering and Technology, 2022.

[48] T. Adiono, S. Fuada, S. Feranti Anindya, I. G. Purwanda, and M. Y. Fathany, "IoT-Enabled Door Lock System," 2019.

[49] K. N. L, B. G. Kumar, D. V D, H. G. Kumar R, and A. Professor, "Home Automation System with Security using Raspberry-Pi," International Research Journal of Engineering and Technology, 2020.

[50] Atanas Plamenov Karaguiozov, "QReact A Generic Framework to Create and Use QR Codes and a Usage Case in the Field of Access Control under Android."

[51] A. M. Al-Ghaili, H. Kasim, M. Othman, and W. Hashim, "QR code based authentication method for IoT applications using three security layers," Telkomnika (Telecommunication Computing Electronics and Control), vol. 18, no. 4, pp. 2004–2011, 2020, doi: 10.12928/TELKOMNIKA.V18I4.14748.

[52] K. C. Liao and W. H. Lee, "A novel user authentication scheme based on QR-code," Journal of Networks, vol. 5, no. 8, pp. 937–941, 2010, doi: 10.4304/jnw.5.8.937-941.

[53] G. Ali, M. A. Dida, and A. E. Sam, "A secure and efficient multi‐factor authentication algorithm for mobile money applications," Future Internet, vol. 13, no. 12, Dec. 2021, doi: 10.3390/fi13120299.

[54] Y. Wahyu Agung Prasetyo, R. Rahim, M. A. Manuhutu, and S. Sujito, "QRIS and GOST: A Symbiotic Approach for Secure QR Code Transactions," SSRG International Journal of Electronics and Communication Engineering, vol. 10, no. 5, pp. 138–147, May 2023, doi: 10.14445/23488549/IJECE-V10I5P113.

[55] Y. Sil Lee, N. Hyun Kim, H. Lim, H. Jo, and H. Jae Lee, "Online Banking Authentication System using Mobile-OTP with QR-code," 2010.

[56] J. Sa-Ngiampak et al., "LockerSwarm: An IoT-based Smart Locker System with Access Sharing," 2019.

[57] B. Muthukumar, J. Albert Mayan, G. Nambiar, and D. Nair, "QR Code and Biometric Based Authentication System for Trains," in IOP Conference Series: Materials Science and Engineering, Institute of Physics Publishing, Oct. 2019. doi: 10.1088/1757-899X/590/1/012010.

[58] D. Conde-Lagoa, E. Costa-Montenegro, F. J. González-Castaño, and F. Gil-Castiñeira, Secure eTickets Based on QR-Codes with User-Encrypted Content. IEEE, 2010.

[59] A. M. S. Pangan, I. L. Lacuesta, R. C. Mabborang, and F. P. Ferrer, "Authenticating Data Transfer Using RSA-Generated QR Codes," pp. 18–38, 2022.

[60] M. E. Sankar, T. Sai Divya, and R. Gunasri, "Delegated Authorization Framework for the Services Using or Code Generation," 2020.

[61] B. Olaiya and O. Onyekachi, "A QR-Code-Based Identity Management System for Monitoring Hostel Residents," Mountain Top University, 2021.

[62] Y. Rahayu, L. Afif, and P. J. Soh, "Design and development of smart lock system based QR-Code for library's locker at Faculty of Engineering, Universitas Riau," SINERGI, vol. 26, no. 3, p. 379, Oct. 2022, doi: 10.22441/sinergi.2022.3.013.

[63] M. Umair, M. A. Cheema, O. Cheema, H. Li, and H. Lu, "Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT," Sensors, vol. 21, no. 11, p. 3838, Jun. 2021, doi: 10.3390/s21113838.

[64] K. Saranya, R. S. Reminaa, and S. Subhitsha, Modern applications of QR-Code for security. 2016.

[65] S. Suman Rajest Professor, R. Regin Assistant Professor, and S. R. Assistant Professor, "International Journal of Human Computing Studies (IJHCS) A QR Code-Based Real-Time Auditing System for Safe Online Data Storage," 2024. [Online]. Available: https://journals.researchparks.org/index.php/IJHCS

[66] Z. H. Choudhury and M. M. A. Rabbani, "Biometric passport for National Security Using Multibiometrics and encrypted biometric data encoded in the QR code," Journal of Applied Security Research, pp. 199–229, 2020.

[67] A. Y. Chaudhari, J. Kulkarni, U. Dube, A. Ghorpade, S. Sakore, and A. K. Gupta, A Biometric Authentication System By Embedding Biometrics in QR Codes. ieee, 2024.

[68] D. Reddy Rachapalli and H. Kumar Kalluri, "Disseminating the Authentication Process Based on Secure RGVSS Multi-Biometric Template Encryption through QR Code in Health Care Informatics," International Journal on Emerging Technologies, vol. 10, no. 3, pp. 370–378, 2019.