International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02983
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

IQR: Identification Made Easy

Dhruv Singh, Ayush Dubey, Gracy Verma, Shital Pazare
B.Tech AI&ML
Thakur College Of Engineering and Technology
dmsworlds@gmail.com
gracyverma962@gmail.com
Mumbai, Maharashtra, India
aadubey1106@gmail.com
shital.pazare@tcetmumbai.in

ABSTRACT

In the modern day, QR codes retain immense value as versatile tools with widespread applications. Their efficiency in facilitating contactless transactions, serving marketing and advertising needs, and enabling secure authentication processes has solidified their place in various industries. QR codes are commonly used for electronic tickets, boarding passes, and accessing product information. The COVID-19 pandemic further accentuated their importance in contact tracing and touchless interactions. As an integral part of mobile technology, QR codes continue to bridge the gap between physical and digital realms, offering quick and convenient access to a wealth of information and services. Their ease of use, coupled with the ubiquity of smartphones, ensures their ongoing relevance in an increasingly connected and tech-driven world.

This research paper explores the development and implementation of an innovative attendance system using facial recognition technology in the context of higher education. The aim is to streamline the integration of identity information , improve accuracy, and enhance the overall user. experience. By integrating QR technology into the identification system, people can not only ensure precise attendance records but also contribute to the development of a more efficient and secure learning environment. This paper discusses the design, technical aspects, user experience, and potential benefits of such a system, offering insights into the future of student information access.

QR codes have become an essential tool in various industries due to their versatility and efficiency in facilitating contactless transactions, marketing and advertising needs, and enabling secure authentication processes. They are commonly used for electronic tickets, boarding passes, and accessing product information. The search results include links to research papers, articles, and tutorials related to QR code-based attendance systems, facial recognition technology, and QR code generators.

KEYWORDS

QR, Identification, Security, OpenCV, AWS, MySQL, PayPal

1. INTRODUCTION

At the vanguard of a digital revolution, Identity QR (IQR) is revolutionizing the very nature of how people engage with and handle their personal data. This cutting-edge application, also referred to as Identity QR, surpasses basic functionality, functioning as an advanced and all- encompassing solution that surpasses the traditional limits of data management. Within the vast domain of IQR, users find a central hub that enables them to effortlessly integrate different aspects of their data. From basic contact information to the complexities of social media profiles, IQR offers a comprehensive approach to personal information integration. This all-inclusive feature not only streamlines the user experience but also increases the possibility of comprehensive representation.

In the vast domain of IQR, users find a single point of contact that enables them to easily combine different aspects of their data. From basic contact information to the nuances of social media profiles, IQR offers a comprehensive method of integrating personal information. This feature makes the user experience easier and increases the possibility of having a complete online persona.

The main selling point of IQR is its capacity to create personalized QR codes. These codes function as dynamic containers, holding a user's preferred data in a way that is both easily shared and updated. Since information is always changing in today's world, IQR makes sure that users can change and share their information safely while maintaining a careful balance between dynamism and data protection.

Privacy is a major concern in the digital age, and IQR takes this concern seriously. The company is committed to protecting user data, and one of its main priorities is privacy. By putting privacy first, IQR makes sure that only people who are authorized can access the integrated information, which builds user confidence and trust in the platform that they use to manage their sensitive information.

IQR's cross-platform compatibility solidifies its position as a must-have tool for a variety of situations. Whether a user needs to navigate networking events, apply for jobs, interact with others, or

build their professional brand, they can access IQR on multiple devices with ease. This cross-device fluidity increases the application's adaptability and establishes it as a go-to resource for people juggling the complex aspects of their personal and professional lives.

At the vanguard of a digital revolution, Identity QR (IQR) is revolutionizing the very nature of how people engage with and handle their personal data. This cutting-edge application, also referred to as Identity QR, surpasses basic functionality, functioning as an advanced and all-encompassing solution that surpasses the traditional limits of data management. Within the vast domain of IQR, users find a central hub that enables them to effortlessly integrate different aspects of their data. From basic contact information to the complexities of social media profiles, IQR offers a comprehensive approach to personal information integration. This all-inclusive feature not only streamlines the user experience but also increases the possibility of comprehensive representation.

IQR's customizable features emphasize personalization while also adding a sophisticated touch. Users can customize their QR codes to meet specific needs or preferences, guaranteeing a unique representation of their identity. Whether it is showcasing contact details, career accomplishments, or pertinent social media profiles, IQR offers a flexible solution for people navigating the challenges of managing their personal information in the digital age.

The next frontier in personal information management is here: IQR, or Identity QR, with its highly customizable features, strong security protocols, and unwavering commitment to user control. Not only does it enable users to share and control their data with ease, but it also establishes a new benchmark for user-friendly, privacy-aware PIM platforms in an increasingly connected world. IQR is more than just an application; it is a monument to the development of digital identity management, revolutionizing the way people interact with and protect their personal data

2. LITERATURE REVIEW

2.1 RELATED WORKS

In recent times, the use of QR codes for attendance tracking is a technology-based approach that offers a convenient and efficient method for monitoring student attendance in educational settings. QR codes are generated for each class session, and students can scan the code using their smartphones to register their attendance. This system provides several advantages, such as the ability to easily monitor absences and tardiness, as well as the convenience of accessing attendance platforms through mobile devices. The use of QR codes for attendance management is being explored in various educational institutions, and research is being conducted to develop and enhance QR code-based attendance systems. The proposed systems aim to prevent attendance cheating and provide an efficient and automated alternative to traditional attendance tracking methods.

Since biometrics are concerned with the measurements of unique human physiological or behavioral characteristics, the technology has been used to verify the identity of users. It is becoming critical to be able to monitor the presence of the authenticated user throughout a session. Thus, another proposal discusses a prototype system that uses facial recognition technology to monitor authenticated users for students.[1]
The proposed software is to be installed on the instructor's mobile telephone. It enables it to query students' mobile telephones via Bluetooth connection and, through a transfer of students' mobile telephones Media Access Control (MAC) addresses to theinstructor's mobile telephone; the presence of the student can be confirmed.[2]
This research paper discusses the implementation of a student attendance system using QR codes in a mobile application. The system was tested on a group of students, and the results showed that the system is efficient and effective.[3]
The text presents QR codes, emphasizing their adaptability and simplicity of use. It examines their structure, describing elements like position patterns, alignment patterns, timing patterns, version information, and the quiet zone. The text highlights the capabilities of QR codes, including their capacity to handle various data types, store information effectively in a small area, and withstand distortion. The article then presents the idea of visual secret sharing technology as a way to improve QR code security. This technology works by splitting QR codes into multiple images (secrets), offering higher levels of security than conventional methods. The rationale for this approach is to safeguard private messages within QR codes, improve sharing effectiveness, and expand the storage capacity of traditional QR codes.[4] In recent years, QR codes have become commonplace in many facets of daily life. They are used for information storage, web links, traceability, identification, and authentication. Computer devices such as mobile phones and scanning guns can quickly identify QR codes due to their large storage capacity, strong anti-damage properties, and affordability. QR codes have a unique structure that includes geometrical correction, high-speed decoding, position tags, alignment patterns, timing patterns, and format information areas with error correction features. [5]
In this paper, we propose a standard multi-color QR code using textured patterns for text steganography, further enhancing security by using a visual secret sharing scheme. This innovation is expected to generate value in business applications. QR codes are popular because they are resilient during the copying process, universally readable, have a high encoding capacity with error correction, and can adapt to small sizes and geometrical distortion. Visual cryptography is a novel secret sharing technology that uses human visual perception to enhance the complexity of secret shared images for decryption.[6]
In the system by using smartphones students scan a QRcode which will be displayed by the teacher. When a student scans this QR code, automatically attendance will be marked according to the user id. It also discusses how the system verifies student identity

to eliminate false registrations.[7]

2.2 PROBLEM STATEMENT

Strong and effective identity systems are now essential in a time when worries about fraud, identity theft, and document forgeries are on the rise. Conventional techniques for document authentication, including barcodes and magnetic strips, frequently don't offer the simplicity and security needed for today's transactions. As a result, there is an urgent need for creative solutions that can expedite the verification process while guaranteeing the integrity and authenticity of official and personal papers.

The application of Quick Response (QR) codes as an identifying mechanism is one possible solution to this problem. Comparing QR codes to traditional methods, there are a number of clear benefits: they can hold a lot of data in a small format; they work with a lot of devices; and they can be scanned and processed quickly. It might be able to improve security features and make verification processes easier for a variety of applications and sectors by adding QR codes to official and personal papers.

Nevertheless, there are a number of major logistical and technical obstacles to overcome before QR code identification systems may be successfully used. To guarantee the uniform creation and understanding of QR codes across various platforms and countries, it is imperative to establish standardized protocols and encoding procedures. To prevent unwanted access or alteration of sensitive data, issues with data privacy, encryption, and authentication procedures also need to be properly handled.

Additionally, as QR code identification technologies become more widely used, strong infrastructure and support networks that can handle high transaction volumes safely and effectively must be established. This means giving end users and service providers with sufficient training and support, as well as integrating QR code scanning capabilities into currently in use hardware and software systems.

Furthermore, the adoption and acknowledgement of QR code identification systems by pertinent parties, such as governmental organizations, financial institutions, and private businesses, is essential to their efficacy. Therefore, in order to guarantee the broad acceptance and effective application of QR code identification solutions, coordinated efforts are required to raise awareness, establish confidence, and encourage cooperation among important stakeholders.

This study intends to explore the viability, effectiveness, and ramifications of employing QR code technology for the identification of private and official documents in light of these difficulties and possibilities. This study looks at the operational, technological, and regulatory elements of QR code identification systems in an effort to offer insights and suggestions that might guide the creation, implementation, and uptake of safe and dependable identification solutions in the digital world.

3. IMPLEMENTATION

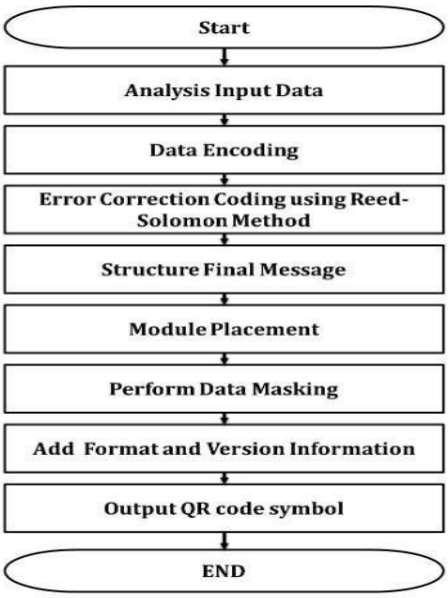
The proposed system has strong data anonymization methods in place to handle changing privacy laws and compliance requirements. Sensitive information is shielded from unwanted access or exposure by encryption or masking of personally identifiable information (PII). Tokenization and pseudonymization are two data anonymization strategies that maintain the integrated data's analytics value and usefulness while strengthening privacy protections.

Additionally, the system makes use of blockchain technology to improve traceability and data integrity. On the blockchain, every transaction is documented as an unchangeable block, generating a tamper-proof audit trail that stakeholders can independently confirm. By guaranteeing the validity and immutability of transaction records, this blockchain-based method improves confidence and transparency in data transfers.

Proactive threat information collecting and vulnerability management enable continuous monitoring and improvement of the security posture of the system. To prevent malicious activity or unauthorized access, intrusion detection systems and automated security scans are used to identify and eliminate any security risks instantly.

All things considered, the system offers a complete and flexible answer for data integration, privacy protection, and safe information sharing. It enables businesses to fully utilize their data assets while protecting against risks and vulnerabilities by fusing state-of-the-art technologies with strict security protocols and user-centric design concepts.

3.1 QR Code Encoding



1. Analyze Input Data:

- The program verifies the kind of data being entered, such as text, URLs, and contact details.
- Before encoding, different data formats could need distinct pre-processing procedures. For instance, URLs might have to be condensed in order to fit inside the QR code.
- Based on the data type, the program also chooses the proper character encoding scheme (such as UTF-8).

2. Data Encoding:

- Using the selected encoding technique, the input data is transformed into a stream of bits.
- The type, length, and encoding strategy of the data will determine how many bits are needed.

3. Using the Reed-Solomon Method for Error Correction Coding:

- Reed-Solomon error repair is used to append new data to the encoded data.
- Even if parts of the modules are broken or obstructed, the QR code can still be deciphered because of this redundant data. The desired level of error correction determines how much error correction code is inserted (a higher level entails greater redundancy and better error correction, but also larger QR code).

4. Organization Concluding Remark:

- Data mode indicators and length indicators, among other service information, are appended to the data stream.
- According to the QR code version, the data and error correcting codewords are separated into data blocks.

5. Module Placement:

- For the selected QR code version, the data blocks
- are inserted between empty modules in a predetermined pattern. The ability to detect and repair errors is enhanced by this interleaving.
- To help with the decoding process, additional special patterns are introduced, such as timing patterns and alignment markers.

6. Carry out Data Masking:

- To enhance the contrast and scannability of the QR code, a bitwise XOR operation is applied to the data modules and chosen mask patterns.
- There are various mask patterns available; the data content and error correction level are used to determine which mask pattern is optimal.

7. Add Format and Version Information:

- Additions of format information bits are made to show the data mask pattern and error correction level
- .The one-module-wide spaces of white space that exist between each encoding region and finder pattern are known as separators.
-
- Sequential Structures: There are two different types of timing patterns: vertical and horizontal.
- They are made up of modules that switch between light and dark. Between the separators in the sixth row of the QR code is where the horizontal timing pattern is located.
- The QR code's sixth column, which lies between the separators, contains the vertical timing pattern. The symbol density, module coordinates, and version information area can all be found using these patterns.
-
- Alignment Patterns: A single dark module sits in the center of an alignment pattern made up of three by three light modules, five by five dark modules, and so on. Alignment patterns are required for QR codes greater than version 2, and the quantity of alignment patterns varies based on the version of the symbol.

- Encoding Region: Data, error correction codes, version information, and format information are all contained in the encoding region. A single module array needs to be set aside for format information in close proximity to the top-left, top-right,

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02983
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

bottom-left, and version information finder patterns. Additionally, a 6-by-3 block needs to be set aside above the bottom-left finger pattern, and a 3-by-6 block needs to be set aside to the left of the top-right finder pattern.
Quiet Zone: This 4-module-wide, blank space is used to make sure that the data from the QR code is not confused by nearby text or markings.

Version information bits—which define the version of the QR code and determine its capacity—are added.

8.Output QR Code Symbol:

An image file or other format containing black and white modules organized in a square grid is the final QR code symbol that is generated.Version information bits are added to specify the QR code version (which determines its capacity).

8. Output QR Code Symbol:

- The final QR code symbol is generated as an image file or other format.
- The image typically consists of black and white modules arranged in a square grid.

3.2 Structure of QR Code:

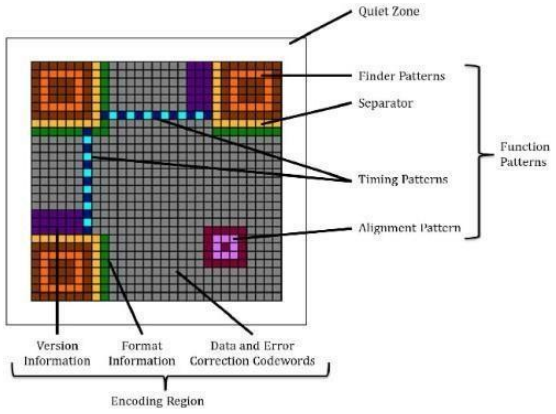


Fig. 3 Structure of a QR Code symbol

Every QR Code symbol must be constructed from square modules placed in a regular square array, include encoding areas and function patterns, and have a quiet zone border surrounding it on all four sides [4] [5].
In order to guarantee that QR code scanners can accurately recognize and orient the code for decoding, function patterns are the shapes that need to be positioned in particular locations of the QR code.
Function patterns come in four different varieties: timing, separator, alignment, and finder patterns. Data representing version information, format information, data, and error correcting codewords are contained in the encoding region.

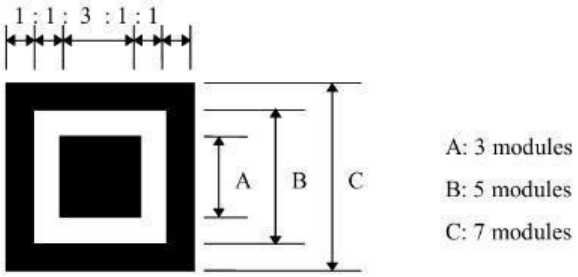


Fig. 4 Finder Pattern

The unique position-detection patterns known as finder patterns are found in each symbol's upper left, upper right, and lower left corners.
It is made up of three modules: a solid dark square measuring three by three in the center, an inner light square measuring five by five, and an outer dark square measuring seven by seven. As illustrated in fig. 4, the module width ratios in each position detection pattern are 1:1:3:1:1.

In order for QR code scanners to discover the finder patterns and properly orient the QR code for decoding, the finder pattern is made to be a pattern that is unlikely to appear inside the other portions of the QR code.

- Separators: These are the spaces of white space, one module in width, that exist between each encoding region and finder pattern.

Timing Patterns: Two timing patterns exist: the horizontal pattern and the vertical pattern.They are made up of modules that switch between light and dark. Between the separators in the sixth row of the QR code is where the horizontal timing pattern is located. The QR code's sixth column, which lies between the separators, contains the vertical timing pattern. The symbol density, module coordinates, and version information area can all be found using these patterns.

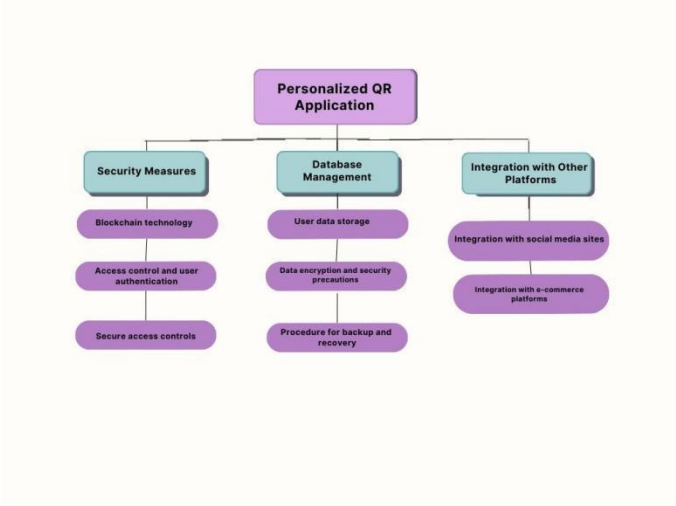
- Alignment Patterns: A single dark module sits in the center of an alignment pattern made up of three by three light modules, five by five dark modules, and so on. Alignment patterns are required for QR codes greater than version 2, and the quantity of alignment patterns varies based on the version of the symbol.

Encoding Region: This area includes data, error correction codes, format information, and version information. A one-module array needs to be set aside for format information in close proximity to the top-left, top-right, bottom-left fender pattern, and version information. Additionally, a 6-by-3 block needs to be set aside above the bottom-left finger pattern, and a 3-by-6 block needs to be set aside to the left of the top-right finder pattern.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02983
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

- Quiet Zone: This is a 4-module-wide space with no data, and it is employed to guarantee that the data from the QR code is not misdirected by the surrounding text or markings.
-

3.3 Flow of QR Application



1. Security Measures

- Blockchain technology: This section discusses the safe storage of user data using blockchain technology. Distributed ledger technology, or blockchain, offers a transparent and safe means of storing data. This application has the potential to record user personal data, including contact details, preferences, and name.
- Access control and user authentication: This section describes how to authenticate a user and provide them access to the program. A login and password or a more advanced technique like two-factor authentication could be used for this.
- Secure access controls: The method of limiting access to the application and its contents is discussed in this block. This can include things like role-based access control (RBAC), which assigns individuals varying degrees of access according to their roles.

2. Database Management

- User data storage: The information contained in this block is kept in a database. This data may consist of the user's name, contact details, preferences, and QR codes, among other things.
- Data encryption and security precautions: The steps done to safeguard user information in the database are discussed in this block. Access controls and encryption may be part of this.
- Procedure for backup and recovery: This section discusses the procedure for protecting user data

and retrieving it in the event of an emergency. In order to prevent user data loss, this is crucial.

3. Integration with Other Platforms

- Integration with social media sites: This section describes how the program can be integrated with Twitter, Facebook, and Instagram, among other social media networks. Users might be able to create QR codes for their posts or profiles using this.
- Integration with e-commerce platforms: This section describes how the application can be integrated with e-commerce sites like Magento, WooCommerce, and Shopify. Users might be able to create QR codes for goods or promotions with this.

4. QR Code Generation

- Enter the required data: The procedure of entering the data to be encoded into the QR code is covered in this block. This could be binary data, like an image or video, or text, such a URL or contact details.
- Create the QR Code: This section discusses the actual procedure of creating the QR code. In order to do this, the input data must be formatted so that a QR code reader can scan it.
- Store the QR Code: This section describes how to store the QR code on a server or in a database. This gives users the option to retrieve the QR code at a later time and enables the program to monitor its usage.

5. Data Encryption

- Use of Advanced Encryption Standard (AES) for data encryption: The data encoded in the QR code is encrypted using the AES encryption method, as stated in this block. The National Institute of Standards and Technology (NIST) has validated AES as a popular and safe encryption method.
- PublicKey Infrastructure (PKI) integration for safe key management: This paragraph discusses managing the encryption keys that are needed to both encrypt and decode data using public key infrastructure (PKI). PKI offers a safe method for distributing, storing, and using encryption keys.

6. User Authentication

- Permit users to verify their identity by having them scan a customized QR code with their smartphone: This section discusses the procedure for verifying a user's identification with a QR code. When a user scans a QR code, the application uses the data included in the code to confirm the user's identity.
- Put two-factor authentication into practice: This section discusses adding an extra security layer through the usage of two-

factor authentication. In order to log in, users using two-factor authentication must enter two pieces of information, such as their username, password, and one-time passcode.

3.1 RESULT AND DISCUSSION

The planned Identity QR (IQR) system is being implemented, which shows how revolutionary it may be in terms of personal data management and identification procedures. The technology provides a comprehensive solution for integrating and safeguarding sensitive data across several platforms and devices by utilizing advanced security mechanisms and QR technology.

Efficiency and Convenience: The exchange and updating of personal data is made easier by the incorporation of QR technology. Users may create customized QR codes with the information they want to share, making it easy and quick to share data in a variety of settings, including professional contacts, networking events, and job applications. Its simplicity of use promotes effective communication in both personal and professional contexts and increases user convenience.

Privacy and Security: In the digital era, privacy and security are crucial. The IQR system takes these worries seriously by enforcing strict access limits and strong encryption techniques. By putting user privacy first, the system builds users' confidence and trust by making sure that their private data is shielded from exposure or illegal access. The system's security posture is strengthened by the application of blockchain technology and data anonymization techniques, which further improve data integrity and traceability.

Cross-Platform Compatibility: The cross-platform compatibility of the IQR system extends its utility across multiple devices and environments, catering to the diverse needs of users in today's interconnected world. Whether accessing the system on smartphones, tablets, or desktop computers, users can seamlessly manage their personal information and maintain control over their digital identity. This adaptability enhances the system's versatility and accessibility, empowering users to navigate the complexities of modern information management with ease.

Personalization & Customization: Users may customize their QR codes to meet their unique needs and preferences thanks to the IQR system's configurable capabilities. Users can display personal information such as contact data, professional achievements, or social network accounts in a way that is distinctive to them. A more relevant and customized user experience is produced as a result of the personalization, which also increases user engagement and gives users a sense of control over their online presence.

Future Repercussions: In terms of identity and personal data management, the IQR system establishes a new standard. Its creative method of fusing cutting-edge security measures with QR technology opens the door for more advancements in the field of digital identity management. The IQR system is still positioned to innovate and adapt as technology develops, guaranteeing its relevance and influence in a digital environment that is always shifting.

All things considered, the deployment of the Identity QR system is a noteworthy development in the area of identification and administration of personal data. Through the utilization of QR technology, privacy-enhancing protocols, and cross-platform interoperability, the system provides a comprehensive approach that enables users to efficiently maintain and safeguard their digital identities. The IQR system is leading the way in innovation, influencing the direction of identity identification and personal data management as the digital ecosystem develops.

5. CONCLUSION

In this study, we investigate the wide range of uses for QR code technology, looking at its advantages, various applications, and significant influence on marketing and the wider tech scene. Since its initial development for inventory tracking, QR codes have spread to a number of industries, including marketing, advertising, secure payment systems, and education. Notably, QR codes have become an essential identifying tool, especially when it comes to the verification of official and personal documents.

Thanks to its many benefits, QR codes have become increasingly popular in recent years. Users have been using them at an exponential rate. Its large data store capacity, quick scanning speed, integrated mistake correcting mechanisms, direct marketing functions, and intuitive user interface are only a few of these qualities. This rapid uptake highlights the adaptability and ease of use provided by QR code technology, establishing it as a standard solution in a variety of fields.

Moreover, QR codes have gained additional utility due to their incorporation for identity purposes. QR codes are currently used to improve the security and effectiveness of document verification procedures, both in private and public settings, going beyond their conventional use in inventory management. Stakeholders can reduce the risks of fraud and counterfeiting while expediting authentication operations by embedding relevant information into QR codes attached to documents.

Furthermore, because of their adaptability, QR codes may be easily integrated into current document management systems, promoting compatibility and interoperability across a range of platforms and devices. This compatibility supports the dependability and credibility of QR code-based identifying systems in addition to improving information accessibility.

Nevertheless, in addition to the numerous advantages of QR code technology for document identification, there are certain issues and factors to take into account that need careful thought. These include resolving regulatory frameworks limiting the use of QR codes in sensitive circumstances, guaranteeing data privacy and

security, and providing standardized standards for QR code development and interpretation.

Given these intricacies, the goal of this study is to present a thorough examination of the development of QR code technology, its growing significance in document identification, and its consequences for the public and private spheres. The goal of this research is to provide insights that guide the creation of reliable and secure identification systems in a world that is becoming more and more digitized by analyzing the potential and difficulties associated with the use of QR codes.

6. ACKNOWLEDGMENT

We are appreciative of our principal's vision and leadership, which drove us forward during this research endeavor with their inspiration and support. We also want to thank our vice principal and dean for all of their help and support throughout this attempt. In addition, we would like to sincerely thank all the people and organizations that helped us finish our study paper on the detection of cracks in nuclear power plants.We sincerely appreciate the research participants' helpful advice and cooperation throughout the data collection process. Our work was significantly improved by the ongoing advice, skill, and support from our mentors and advisors, for which we are incredibly grateful. Finally, we would like to thank the editors and reviewers for their insightful comments.

7. REFERENCES

[1] A. Nuhi, A. Memeti, F. Imeri and B. Cico, "SmartAttendance System using QR Code," 2020 9thMediterranean Conference on EmbeddedComputing (MECO), 2020, pp. 1-4, doi:10.1109/MECO49872.2020.9134225. https://www.semanticscholar.org/paper/Smart-Attendance-System-using-QR-Code-Nuhi-Memeti/9aad95ea4b33d02cb7b8c2a9883953adda505f42

[2] Casunuran, J.J.S., Quiambao, C.R.C., Fordan, M.E.,Soriano, A.J., Beaño, M.G.P., Mandayo, E.A. andDomingo, B.B., 2020, November. Quick ResponseCode Attendance System with SMS LocationTracker. In 2020 IEEE REGION 10 CONFERENCE(TENCON) (pp. 373-378). IEEE. https://ijsrset.com/IJSRSET23103124

[3] S. Nalintipwong, T. Tasarika, C. Ruksomya, S.Vittayakorn and T. Numnonda, "Concurrent Self-Identification Applying QR Code to Record ClassAttendance (QRClass)," 2019 IEEE 9thInternational Conference on ElectronicsInformation and Emergency Communication(ICIEC), 2019, pp. 1-5, doi:10.1109/ICEIEC.2019.8784518 https://www.semanticscholar.org/paper/Concurrent-Self-Identification-Applyin g-QR-Code-to-Nalintipwong-Tasarika/242a2e21f1f3a3267fc47185448c1b4b3 6ecb6e9

[4] Tiwari, Sumit, and Pitney Bowes. "(PDF) An Introduction to QR Code Technology."ResearchGate, https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology

[5] "Use QR Code Generator for PDF." QR Code Generator, https://www.qr-code-generator.com/solutions/pdf-qr-code/

[6] "Personal QR Code: 6 Novel Ways to Share Information." QR Code Generator, https://www.qr-code-generator.com/qr-codes-for/personal-use/

[7] Hteik Htar Lwin, Aung Soe Khaing, Hla Myo Tun "Automatic Door Access System Using FaceRecognition" International Journal Of Scientific & Technology Research Volume 4, Issue 06, June2015. https://www.ijstr.org/paper-references.php?ref=IJSTR-0615-11966

[8] "QR code generator as a tool for document verification." ME-QR, https://me-qr.com/page/blog/verification-of-documents-with-qr-codes

[9] Wainwright, Corey. "How to Make a QR Code in 5 Easy Steps." HubSpot Blog, 27 December 2023, https://blog.hubspot.com/blog/tabid/6307/bid/29449/how-to-create-a-qr-code-in-4-quick-steps.aspx.

[10] "QR Codes | Infographics." Google for Developers, 16 November 2023, https://developers.google.com/chart/infographics/docs/qr_codes.

[11] "Flowchart of reading QR Codes | Download Scientific Diagram." ResearchGate, https://www.researchgate.net/figure/Flowchart-of-reading-QR-Codes-1_fig2_324534361.

[12] "Information capacity and versions of QR Code." QRcode.com, https://www.qrcode.com/en/about/version.html.

[13] Garg, Gautam. "QR Code Structure: Everything you need to know." Scanova, https://scanova.io/blog/qr-code-structure/.

[14] "Blockchain As Database For Maximum Security: 4 Steps." RedSwitches, 9 August 2023, https://www.redswitches.com/blog/blockchain-as-database/.

[15] YouTube: Home, 9 November 2017, https://www.analyticsvidhya.com/blog/2021/06/learn-how-to-implement-face-recognition-using-opencv-with-python.

[16] Tiwari, Sumit, and Pitney Bowes. "(PDF) An Introduction to QR Code Technology." ResearchGate, https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology.

[17] "(PDF) QR-code generator." ResearchGate, 25 February 2015, https://www.researchgate.net/publication/251987247_QR-code_generator.

Fernigrini, Lisandro. "How to Store Login Data in a Database." Vertabelo, 3 February 2022, https://vertabelo.com/blog/authentication-data-storage/.

[18] Kirvan, Paul. "What are some tips for storage of sensitive data?" TechTarget, 9 May 2022, https://www.techtarget.com/searchstorage/answer/What-are-some-tips-for-storage-of-sensitive-data.

[19] "Storage of personal data." SearchInform, 24 November 2020, https://searchinform.com/challenges/personal-data-protection/protection-of-personal-information/storage-of-personal-data/.

[20]