e-JURNAL PENYELIDIKAN DAN INOVASI
ISLAMIC INNOVATION CENTER FOR TECHNOLOGY, UIS
https://ejpi.uis.edu.my/
e-ISSN 2289-7909

VOL. 13 NO. 1 (APRIL, 2026): page 300-315
DOI: https://doi.org/10.53840/ejpi.v13i1.398

Received: March 15, 2026 Accepted: April 25, 2026 Published: April 30, 2026

A Systematic Literature Review on QRCode–Based Systems for Academic Credential Verification

Khirulnizam Abd Rahman, Syed Arbaz Ahmed, Che Wan Shamsul Che Wan Ahmad,
Nur Muizz Mohamed Salleh, Rafiza Kasbun
Universiti Islam Selangor, Malaysia
khirulnizam@uis.edu.my, syed_arbaz@hotmail.com

Syahrul Nizam Junaini
Universiti Malaysia Sarawak
snjunaini@unimas.my

ABSTRACT

The increasing need for secure and efficient academic credential verification has driven the adoption of digital solutions, particularly QR code–based systems, to address credential fraud and inefficiencies in manual verification processes. This study presents a Systematic Literature Review (SLR) on QR code–based systems for academic credential verification, conducted in accordance with PRISMA guidelines. Relevant studies were systematically identified through structured searches of major academic databases, followed by screening and eligibility assessment based on predefined inclusion and exclusion criteria. The final set of selected studies was analyzed and synthesized to examine system architectures, verification mechanisms, application domains, and security considerations of QR code–enabled credential verification systems in educational contexts. The review reveals that QR code technology is predominantly utilized for certificate authentication, transcript verification, attendance tracking, and digital credential issuance. However, limitations persist regarding data integrity assurance, interoperability across platforms, privacy protection, and resistance to tampering. Furthermore, the lack of standardized frameworks and inconsistent implementation practices across institutions were identified as key challenges. This review highlights existing research gaps and outlines future research directions toward developing more robust, secure and standardized QR code–based academic credential verification systems to support trustworthy and scalable digital education ecosystems.

Keywords: QR Code; Academic Credentials; Verification; Systematic literature review; Digital Solution

INTRODUCTION

In recent years, the integration of technology in academic credential verification has gained significant attention, particularly with the advent of Quick Response (QR) code-based systems. These systems offer

a modern approach to streamline the verification process, enhancing efficiency and security. As educational institutions and employers seek reliable methods to authenticate academic credentials, QR codes present a viable solution by enabling instant access to verified information through mobile devices (Yahya et al., 2017).

The use of QR codes for credential verification not only simplifies the process but also addresses issues related to forgery and misrepresentation of academic achievements (Kumar, 2024). By embedding encrypted data within QR codes, institutions can provide a secure means of sharing academic records, which can be easily scanned and validated by third parties (Naser et al., 2020). This technology aligns with the growing demand for transparency and trust in educational qualifications, as highlighted by several studies (Noorhizama et al., 2023).

Moreover, QR code-based systems facilitate a more user-friendly experience for both graduates and employers, as they eliminate the need for lengthy verification processes and reduce administrative burdens (Singhal & Pavithr, 2015). The adaptability of QR codes across various platforms further enhances their appeal, making them suitable for diverse contexts from job applications to international credential verification (Ahmed & Jang, 2018).

As the landscape of higher education continues to evolve, the implementation of QR code technology in academic credential verification is poised to transform traditional practices and methods. This systematic literature review (SLR) aims to explore the effectiveness, challenges, and future prospects of QR code-based systems in this domain, drawing insights from existing research to provide a comprehensive understanding of their impact on academic integrity and verification processes. Specifically, the review addresses 4 questions: (1) How are QR code technologies utilized in systems designed for academic credential verification? (2) What types of system architectures are used in QR code based academic credential verification systems? (3) What security and privacy challenges are associated with these systems? (4) What limitations and research gaps exist in current implementations of QR code? The review applies the Kitchenham and Petersen method for conducting SLRs and reports the study selection process using the PRISMA 2020 guidelines. This study summarizes existing research to show how QR code–based systems are used and utilize for academic credential verification while pointing out gaps, obstacles, and areas for further development.

METHODOLOGY

This study follows the systematic literature review (SLR) methodology proposed by Kitchenham and Petersen et al. (2015), which is widely applied in information systems and technology adoption research. The methodology consists of three main phases: planning the review, conducting the review, and reporting the results. To ensure transparency in study selection and screening, the review also applies the PRISMA 2020 reporting guidelines (Page et al., 2021).

Research Objectives

The following research objectives (ROs) were developed to guide the review:

I. **RO1:** To identify and analyze how QR code technologies are applied in academic credential verification systems within educational institutions.
II. **RO2:** To examine the different system architectures adopted in the development of QR code based academic credential verification platforms.
III. **RO3:** To investigate the security and privacy issues associated with the implementation of QR code enabled credential verification systems.
IV. **RO4:** To determine the existing limitations and research gaps in current QR code based academic credential verification implementations for future system enhancement.

Research Question

The aim or purpose of this study is to conduct a systematic literature review (SLR) of research on QR Code based systems for academic credential verification. Research objectives were translated into specific research questions as shown below:

I. **RQ1**: How are QR code technologies utilized in systems designed for academic credential verification?
II. **RQ2**: What types of system architectures are used in QR code based academic credential verification systems?
III. **RQ3**: What security and privacy challenges are associated with these systems?
IV. **RQ4:** What are the limitations and research gaps that exist in current implementations of QR code?

Search strategy/process

To conduct the systematic literature review, a comprehensive search process was implemented in leading academic databases, including Google Scholar, Semantic Scholar, and Scopus to identify relevant articles and studies since 2016. The T able 1 shows search strings used for each database library:

Table 1: Search String

Database Library	Search String
Google Scholar	("QR Code" OR "Quick Response Code") AND ("Academic Credential" OR "Educational Certificate" OR "Digital Diploma" OR "Transcript Verification") AND (Authentication OR Verification OR Validation) AND (Education OR University OR "Higher Education")
Semantic Scholar	"QR Code" AND ("Academic Certificate" OR "Academic Credential" OR Transcript) AND (Verification OR Authentication) AND Education
Scopus	TITLE-ABS-KEY (("QR Code" OR "Quick Response Code") AND ("Academic Credential" OR "Educational Certificate" OR "Digital Diploma" OR "Academic Transcript") AND ("Verification" OR "Authentication" OR "Validation") AND ("Education" OR "University" OR "Higher Education")) AND PUBYEAR > 2021 AND PUBYEAR < 2027

Inclusion and Exclusion Criteria

There were articles on the following subjects:

i. Journal, conference.
ii. Papers composed in the English language.
iii. Published in or 2016 and later.
iv. Papers come up from the search string.
v. Focus on consumers or households.
vi. Discuss the usage of QR Code based systems for academic credential verification.

Articles on the following topics were excluded:

i. Studies on industrial/organizational e-waste only.
ii. Purely technical use of QR Code without involvement of credential verification.
iii. Non-English language publications.
iv. Other literature reviews.
v. PowerPoint and presentation Slides.
vi. Logs or web pages.

Study Selection

The selection process followed four steps:

1. Removal of duplicates.
2. Title and abstract screening.

3. Full-text screening based on inclusion/exclusion criteria.
4. Final inclusion documented using the PRISMA 2020 flow diagram.

Data Collection

The data that is retrieved out of all papers includes:

I. Bibliographic information (author, year, country).
II. Application of QR Code Technology applied
III. Main findings
IV. Security and Privacy Features mentioned
V. Reported Challenges and Limitations

Quality Assessment

There are five questions for quality assessment (QA) as shown in table below:

Table 2: Quality Assessment Questions

QA No.	Quality Assessment Questions
QA1	**Clarity of Objectives** Does the study clearly state its research objectives or purpose related to QR code–based academic credential verification systems?
QA2	**Description of System Architecture** Does the study provide a clear description of the system architecture or framework used for QR code–based credential verification?
QA3	**Explanation of Verification Mechanism** Does the study explain how the QR code is used to verify the authenticity of academic credentials?
QA4	**Security and Privacy Considerations** Does the study address security or privacy aspects associated with the implementation of the QR code–based verification system?
QA5	**Challenges and Limitations** Does this study report any challenges or limitations during the design, development, or implementation of the QR code–based academic credential verification system?

Quality Assessment (QA) Procedure

Each study that included was later assessed using five quality criteria adapted from Kitchenham (2009) & Petersen (2008). A total score (0–5) was calculated for each study by summing across all five questions. Table 3 below shows the scoring procedures:

Table 3: Quality Assessment Scoring System

QA1 Does the study clearly state its research objectives or purpose related to QR code–based academic credential verification systems?
Y (Yes): The study clearly states its research objectives or purpose related to QR code–based academic credential verification systems
P (Partly): The study partially states its research objectives or purpose related to QR code–based academic credential verification systems
N (No): The study does not state its research objectives or purpose related to QR code–based academic credential verification systems

QA2. Does the study provide a clear description of the system architecture or framework used for QR code–based credential verification?

Y (Yes): The study provides a clear description of the system architecture or framework used for QR code–based credential verification.

P (Partly): The study provides partially clear description of the system architecture or framework used for QR code–based credential verification

N (No): The study does not provide a clear description of the system architecture or framework used for QR code–based credential verification

QA3. Does the study explain how the QR code is used to verify the authenticity of academic credentials?

Y (Yes): The study clearly explains how the QR code is used to verify the authenticity of academic credentials.

P (Partly): The study partially explains how the QR code is used to verify the authenticity of academic credentials.

N (No): The study does not explain how the QR code is used to verify the authenticity of academic credentials.

QA4. Does the study address security or privacy aspects associated with the implementation of the QR code–based verification system?

Y (Yes): The study clearly addresses security or privacy aspects associated with the implementation of the QR code–based verification system.

P (Partly): The study partially addresses security or privacy aspects associated with the implementation of the QR code–based verification system.

N (No): The study does not address security or privacy aspects associated with the implementation of the QR code–based verification system.

QA5. Does the study report any challenges or limitations during the design, development, or implementation of the QR code–based academic credential verification system?

Y (Yes): The study clearly reports any challenges or limitations encountered during the design, development, or implementation of the QR code–based academic credential verification system

P (Partly): The study partially reports any challenges or limitations encountered during the design, development, or implementation of the QR code–based academic credential verification system

N (No): The study does not report any challenges or limitations encountered during the design, development, or implementation of the QR code–based academic credential verification system

The scoring procedure are Y = 1, P = 0.5, N = 0

Analysis of Data

Data will be extracted, analysed, and presented in table format and in descriptive format to easily summarise the outcomes of the review process. The analysis of the data will be structured as follows:

I. **Overview of the review stages**
   A diagram will be developed to outline the findings of the four-stage review process. To describe the selection process, the PRISMA 2020 flow diagram will be added.

II. **Quality assessment results**
A table will present the quality scores (QA1–QA5) for individual studies to indicate whether each article satisfied the criteria. Based on the total scores that will be obtained, and only studies over the cut-off point will be analysed.

III. **Thematic Analysis of QR Code–Based Verification Systems**
The selected studies from all the databases will be analysed using a thematic approach to identify the primary applications of QR code technology in academic credential verification systems, the types of system architectures implemented in the studies, and the verification mechanisms used in all the selected papers. The identified features will be grouped into relevant themes to make comparisons between different studies.

RESULT

Search results

The results of the four-stage review process (identification, screening, eligibility, and inclusion) are summarized. A PRISMA 2020 flow diagram is included to illustrate the study selection process as shown in Figure 1 below:

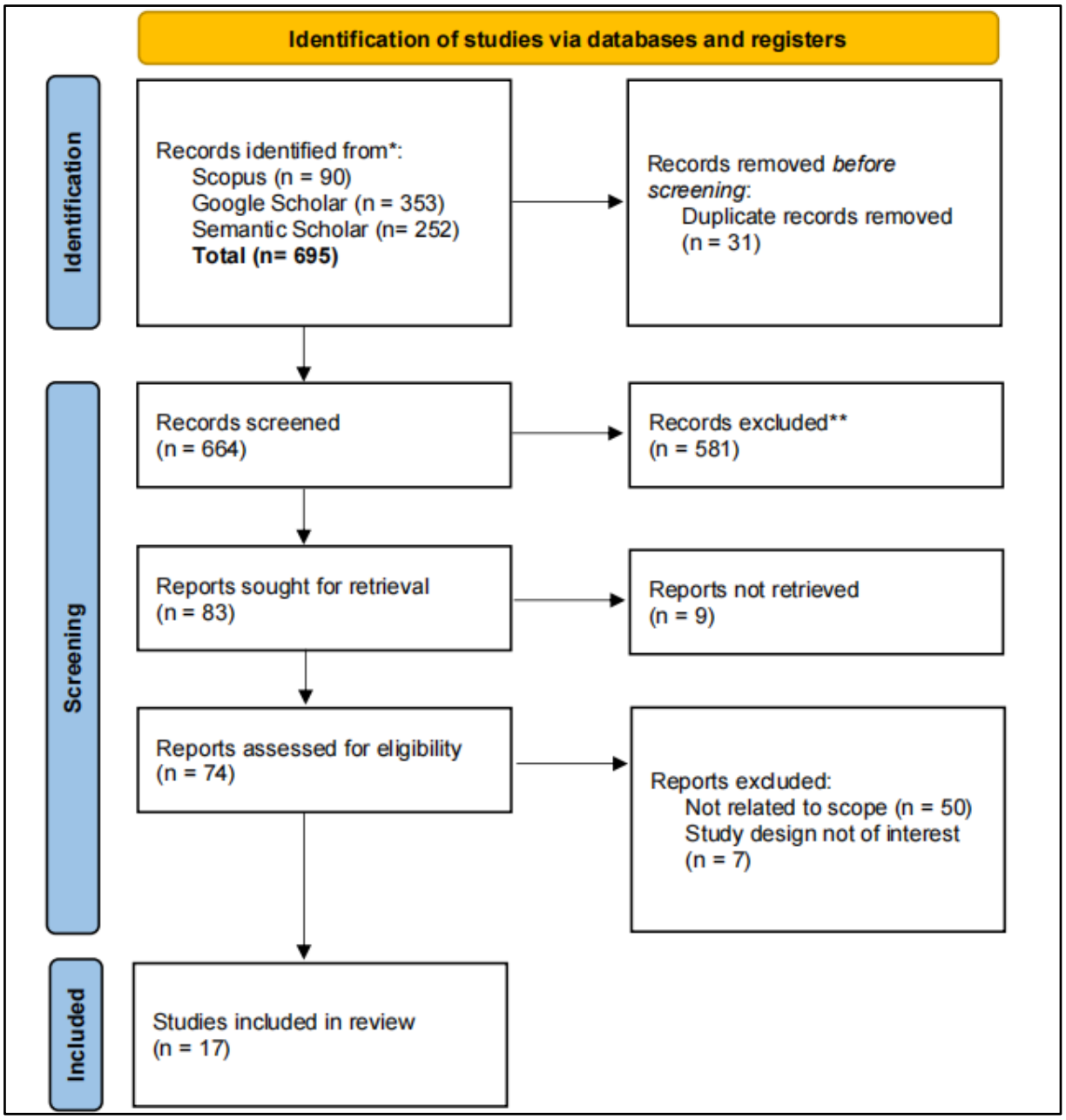

Figure 1 . Flow Diagram of the study (adapted from Page et al., 2020).

A collection of 17 relevant, related works has been assembled after searching with the strings mentioned and browsing online databases. Every paper has been organized into a table, which (as shown in Table 4) has the following details in its contents: (a) Title of study; (b) Author or authors/ citation; (c) Publication year; and (d) Country.

Table 4: Data Collection of Related Study

Paper ID.	Title	Author/Citation	Publication Year	Country
1.	Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications	(Gangwar, 2024)	2024	India
2.	Certificate Generation and Verification System Using	(Abdullahi, 2022)	2022	Nigeria

	Blockchain Technology and Quick Response Code			
3.	Certificate Management System using Blockchain and Steganography Techniques	(Ranjith & Davuluri, 2025)	2025	India
4.	Educational Document Verification through Blockchain: Literature Review	(Magar et al., 2024)	2024	India
5.	Hybrid Digital Certificate Management System with QR Code and IoT Integrated on Hyperledger Fabric Blockchain	(Kumar, 2024)	2024	India
6.	Preventing Forged and Fabricated Academic Credentials Using Cryptography and Qr Codes	(Shaik, 2021)	2021	USA
7.	ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh	(Farabi et al., 2025)	2025	Bangladesh
8.	University Of Cross River State Certificate Verification System with Embedded Unclonable Quick Response Code Digital Signature	(Essien & Tumenayu, 2022)	2022	Nigeria
9.	A Privacy-Centered Protocol for Enhancing Security and Authentication of Academic Certificates	(Saleh et al., 2023)	2023	Iraq
10.	Blockchain ensuring academic integrity with a degree verification prototype	(Cardenas-Quispe & Pacheco, 2025)	2025	Peru
11.	Verification of Ph.D. Certificate using QR Code on Blockchain Ethereum	(Noorhizama et al., 2023)	2023	Malaysia
12.	Document Certificate Authentication System Using Digitally Signed QR Code Tag	(Ahmed & Jang, 2018)	2018	South Korea
13.	A New Academic Certificate Authentication Using Leading Edge Technology	(Yahya et al., 2017)	2017	Malaysia
14.	QR code based two-factor authentication to verify paper-based documents	(Naser et al., 2020)	2020	Iraq
15.	Digital Certificate System for Verification of Educational Certificates Using Blockchain	(Chennur et al., 2021)	2021	India
16.	Embedding a Blockchain Technology Pattern into the QR Code for an Authentication Certificate	(Aini et al., 2020)	2020	Indonesia
17.	Exploring the Efficiency of QR-Code Technology in Developing Authentication System for Admitting Students into Examination Hall for Polytechnics in Nigeria	(Inyangetoh & Johnson, 2025)	2025	Nigeria

Quality Assessment of Related Papers

The 17 papers selected for this study were analysed and scored using the quality assessment questions that were previously stated. The results are shown in Table 5 below. Each study's quality scores indicate how well it satisfied the five evaluation criteria (QA1–QA5). A total score of 0–5 per paper was possible, with each criterion being scored as Yes (1 score), Partly (0.5 score), or No (0 score) as mentioned above in methodology section (Kitchenham, 2007; Petersen et al., 2008). Higher scores indicate and show stronger methodological rigor, clearer reporting, and better relevance to this review's research questions. For example, studies that scored 4.5–5 demonstrated excellent clarity of objectives, robust methodology , and transparent results. Papers in the 3–4 range were considered as being of average quality paper or research; they often satisfied the majority of the requirements but lacked an accurate methodological explanation or context description. Scores 3 and below reflected weaker studies with limited clarity or incomplete reporting, and these were interpreted more cautiously in the discussion section. This method make sures that the findings of this SLR are built primarily on evidence from higher-quality studies, while still capturing useful and important insights from lower-scoring ones where relevant.

Table 5; Systematic Review Studies

Paper ID.	Database	QA1	QA2	QA3	QA4	QA5	Total Score
1.	Google Scholar	1	1	1	1	1	**5**
2.	Google Scholar	1	1	1	0.5	1	**4.5**
3.	Google Scholar	1	0.5	1	0.5	1	**4**
4.	Google Scholar	1	1	1	1	1	**5**
5.	Google Scholar	1	1	1	1	0.5	**4.5**
6.	Google Scholar	1	1	1	1	1	**5**
7.	Google Scholar	0.5	1	1	1	1	**4.5**
8.	Google Scholar	1	1	1	1	1	**5**
9.	Scopus	1	1	1	1	0.5	**4.5**
10.	Scopus	1	1	1	1	1	**5**
11.	Scopus	1	1	1	1	1	**5**
12.	Scopus	1	1	1	1	1	**4.5**
13.	Scopus	1	1	1	1	1	**4**
14.	Scopus	1	1	1	1	1	**4**
15.	Semantic Scholar	1	1	1	1	0.5	**4.5**
16.	Semantic Scholar	1	1	1	1	0.5	**4.5**
17.	Semantic Scholar	1	1	1	1	1	**5**

Thematic Analysis of QR Code–Based Verification Systems

The included studies (17 papers) were analysed to determine the usage and utilization of QR code, system architecture, verification mechanism, and challenge/limitation the implementation of QR code-based systems. The analysed data is recorded in T able 6 9 as shown below.

For each thematic category, a corresponding graphical representation is provided to show the distribution of studies between the identified themes. These figures are shown to facilitate comparative analysis by highlighting the frequency of implementation approaches, verification techniques, QR code utilization methods, and also the commonly reported challenges and limitations in existing systems.

Table 6: QR code Utilization and Usage

QR Code Utilization and Usage	Description	Example Studies (Paper ID.)	Number of studies
Credential Authentication	QR code embedded into academic certificates such diplomas and degree to enable verification of document authenticity through institution or university systems	1, 2, 4, 6, 8, 9, 11, 12, 14, 15	10
Digital Credential Validation	QR code used to validate digitally issued academic credentials against stored records	3, 5, 7, 10, 13	5
Secure Document Access	QR code provides secure access to credential information via online verification portals	6, 8, 12, 14	4
Fraud Detection and Prevention	QR code as a mechanism to detect forged or tampered academic documents	4, 9, 11, 16	4
Automated Credential Retrieval	QR code used to retrieve academic credential records from databases during verification	13, 17	2

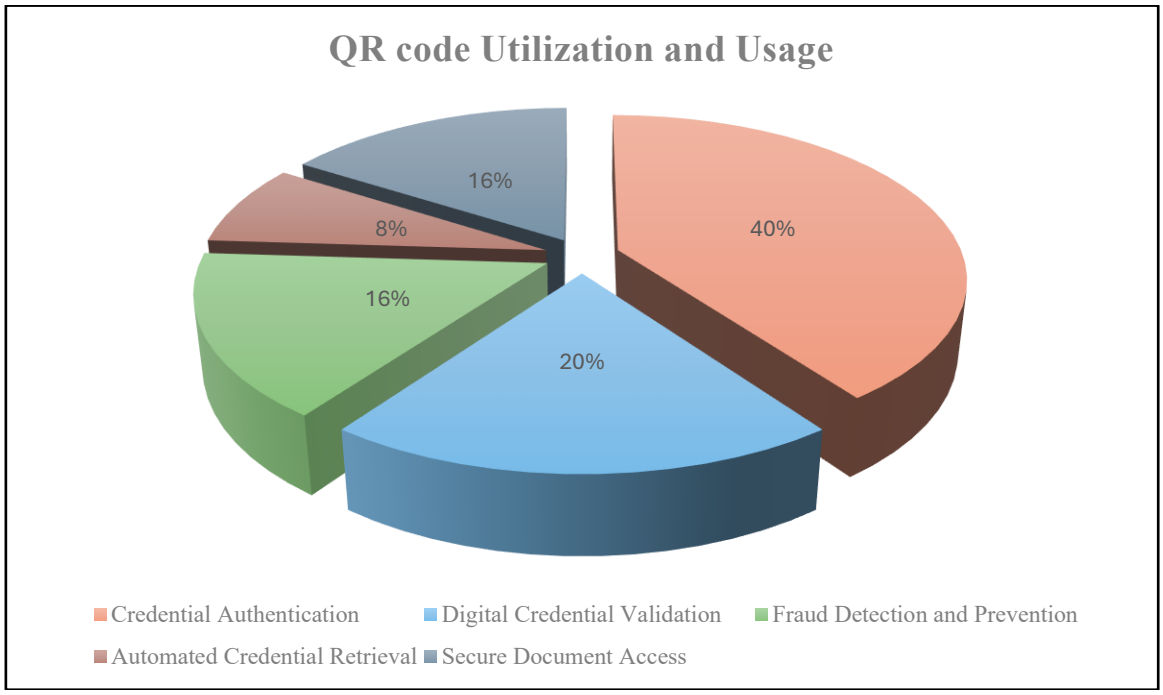

Figure 2: Graphical Representation of QR code Utilization and Usage

Table 7: System Architecture

System Architecture	Description	Example Studies (Paper ID.)	Number of studies
Blockchain-Based Architecture	QR code linked to blockchain ledger for immutable academic credential storage and verification	1, 2, 4, 5, 7, 10, 11, 15	8
Centralized Web-Based System	Credential data stored in institutional database and verified via web portal after QR scan	6, 8, 9, 12, 13, 14	6
Cloud-Integrated System	Credential verification supported through cloud host infrastructure	3, 16, 17	3

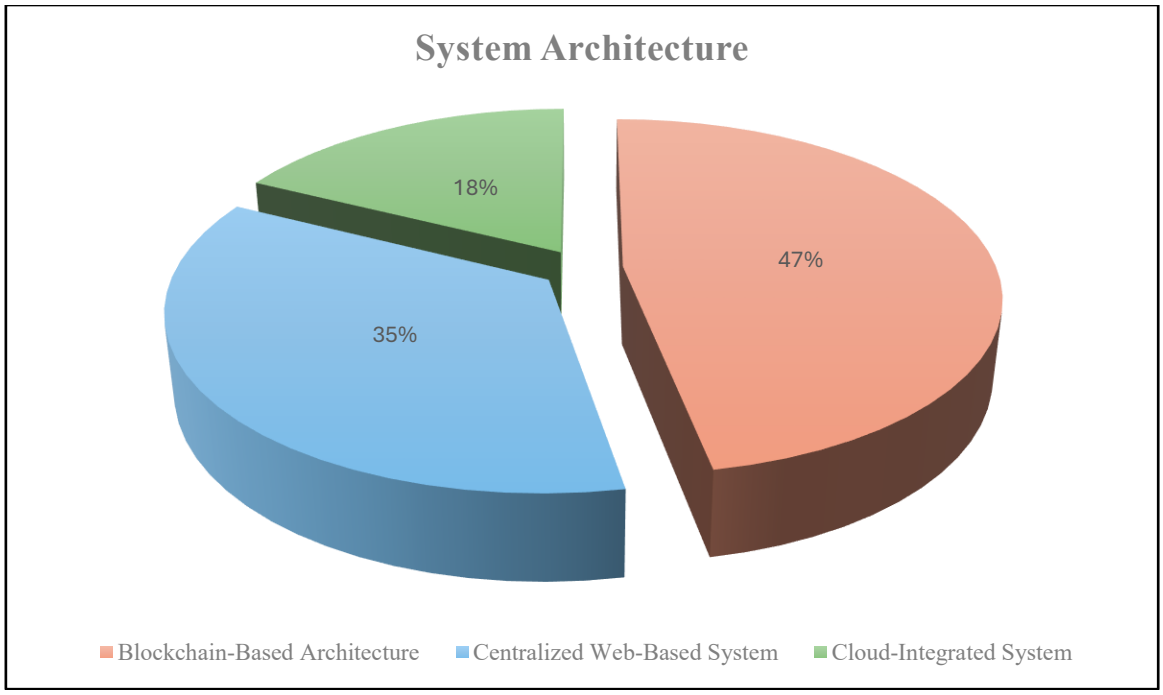

Figure 3: Graphical Representation of System Architecture

Table 8: Verification Mechanism

Verification Mechanism	Description	Example Studies (Paper ID.)	Number of studies
Hash-Based Credential Encoding	QR code generated from hashed academic credential data for validation	3, 5, 7, 10, 15	5
Encrypted URL Verification	QR redirects to secure institutional or universities verification page	6, 8, 12, 14	4
Digital Signature Authentication	Verification through embedded digital signature validation	2, 9, 11	3
Blockchain Ledger Reference	QR linked directly to immutable blockchain transaction record	1, 4, 16	3
Unique ID / Token-Based Lookup	QR contains unique identifier to retrieve credential record from database	13, 17	2

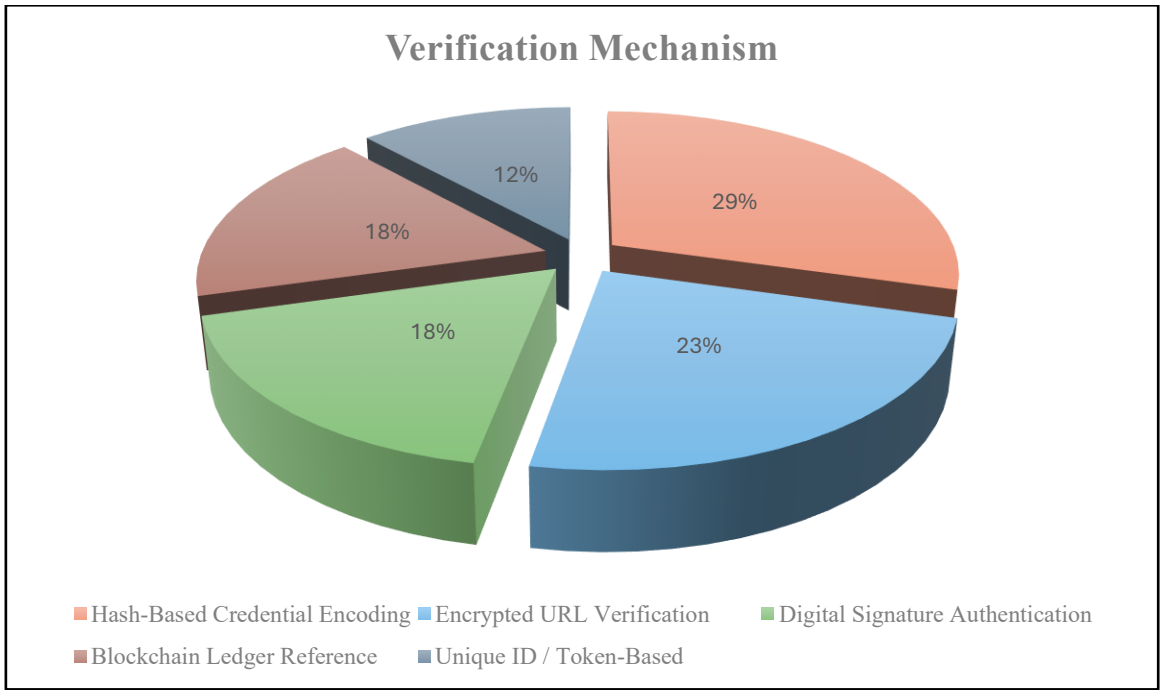

Figure 4: Verification Mechanism

Table 9: Challenges and Limitations

Challenge / Limitation	Description	Example of Studies	Number of studies
Data Tampering Risk	Vulnerability of static QR codes to duplication or unauthorized modification	6, 8, 12	3
Lack of Standardization	Absence of unified framework across institutions and universities	3, 9, 13	3
Interoperability Issues	Difficulty integrating systems across institutions or platforms	2, 14, 17	3
Privacy Concerns	Exposure of personal or academic data during verification	5, 11, 15	3
Scalability and Deployment Constraints	Limited discussion of large-scale implementation feasibility	1, 4, 7, 10, 16	5

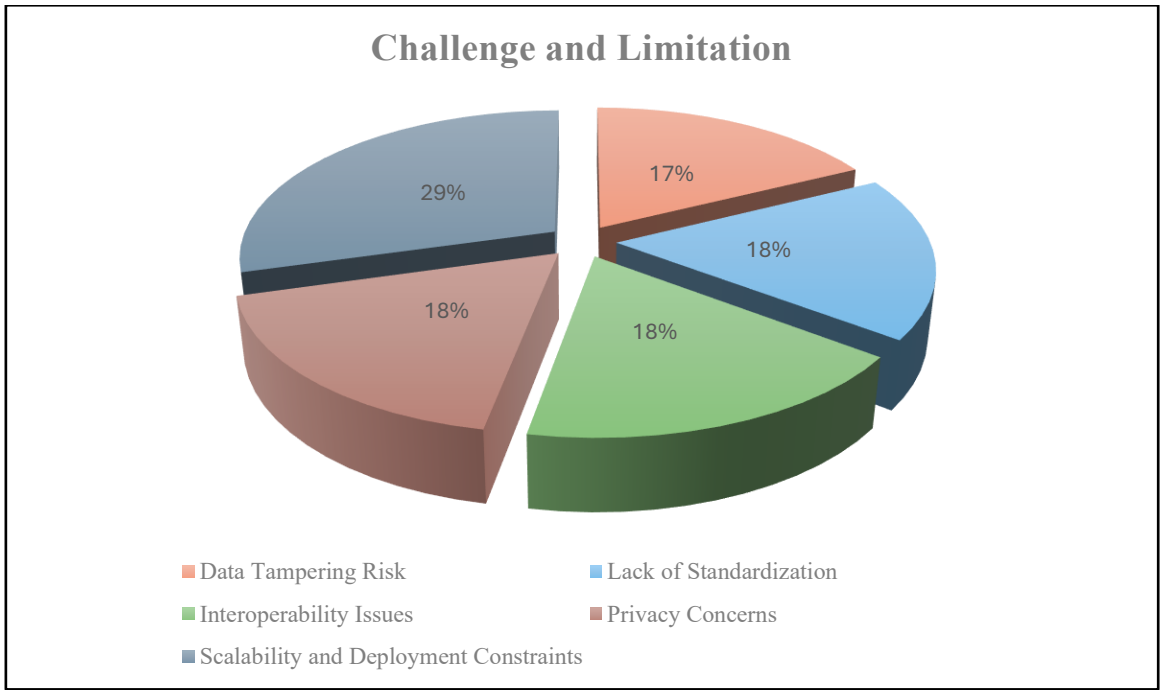

Figure 5: Challenge and Limitation

FINDINGS AND DISCUSSION

RQ1: How are QR code technologies utilized in systems designed for academic credential verification?

The reviewed studies demonstrate that QR code technology is predominantly employed as an enabling interface that links academic credentials to digitally stored verification records. Rather than functioning as a standalone security mechanism, QR codes serve as access points that facilitate real-time authentication by connecting physical or digital documents to institutional databases or verification platforms (Abdullahi, 2022; Ahmed & Jang, 2018; Essien & Tumenayu, 2022; Gangwar, 2024; Naser et al., 2020; Shaik, 2021). This approach reduces reliance on manual validation processes and enhances the efficiency of credential verification workflows.

In several implementations, QR codes are also integrated into digital credential issuance systems to support automated validation procedures, allowing academic documents to be authenticated against stored institutional records (Cardenas-Quispe & Pacheco, 2025; Farabi et al., 2025; Kumar, 2024; Ranjith & Davuluri, 2025; Yahya et al., 2017). Additionally, the utilization of QR codes in fraud detection mechanisms has been reported, whereby discrepancies between the scanned code and the stored credential data can be used to identify tampered or falsified academic documents (Aini et al., 2020; Magar et al., 2024; Noorhizama et al., 2023; Saleh et al., 2023). These findings suggest that QR codes are primarily applied as verification facilitators that bridge credential documents with backend authentication systems.

RQ2: What types of system architectures are used in QR code–based academic credential verification systems?

The findings indicate a growing trend toward the integration of decentralized technologies, particularly blockchain-based architectures, to enhance the integrity and transparency of academic credential verification systems (Abdullahi, 2022; Cardenas-Quispe & Pacheco, 2025; Chennur et al., 2021; Farabi et al., 2025; Gangwar, 2024; Kumar, 2024; Magar et al., 2024; Noorhizama et al., 2023). In such implementations, QR codes are commonly used to reference immutable credential records stored within distributed ledger environments, thereby minimizing the risk of unauthorized data manipulation.

Despite this trend, centralized web-based systems remain widely implemented due to their relative simplicity and ease of deployment within institutional infrastructures (Ahmed & Jang, 2018; Essien & Tumenayu, 2022; Naser et al., 2020; Saleh et al., 2023; Shaik, 2021; Yahya et al., 2017). These systems typically rely on institutional databases to store credential information, with QR codes serving as identifiers for accessing verification portals. Furthermore, cloud-integrated architectures have been explored to support remote credential storage and facilitate scalable access during the verification process (Aini et al., 2020; Inyangetoh & Johnson, 2025; Ranjith & Davuluri, 2025). In general, these architectural variations and differences reflect and show different priorities in balancing security, accessibility, and implementation feasibility.

RQ3: What security and privacy challenges are associated with these systems?
Several studies highlight security vulnerabilities associated with the use of QR codes, particularly in systems that employ static or unencrypted code structures (Ahmed & Jang, 2018; Essien & Tumenayu, 2022; Shaik, 2021). In such cases, QR codes may be susceptible to unauthorized duplication or modification, thereby compromising the authenticity of the associated academic credentials. This limitation underscores the importance of integrating additional cryptographic mechanisms to strengthen verification reliability.

Privacy-related concerns have also been reported, particularly in relation to the exposure of sensitive academic or personal information during the credential verification process (Chennur et al., 2021; Kumar, 2024; Noorhizama et al., 2023). The accessibility of credential data through publicly scannable QR codes may introduce risks if adequate access control or encryption measures are not implemented. Moreover, interoperability challenges were identified in systems attempting to integrate credential verification platforms across institutional or technological boundaries (Abdullahi, 2022; Inyangetoh & Johnson, 2025; Naser et al., 2020). These challenges may impede the development of universally accepted verification frameworks in academic environments.

RQ4: What are the limitations and research gaps that exist in current implementations and usage of QR code?
The reviewed studies reveal several limitations in the current implementation of QR code–based credential verification systems. A recurring issue is the absence of standardized implementation frameworks, which may lead to inconsistencies in system design and limit the interoperability of verification platforms across institutions (Ranjith & Davuluri, 2025; Saleh et al., 2023; Yahya et al., 2017). The lack of standardization creates challenges for the widespread adoption of QR-enabled credential verification systems in multi-institutional settings.

Additionally, scalability and deployment constraints have been identified as potential barriers to large-scale implementation, particularly in systems that remain at the prototype or conceptual stage (Aini et al., 2020; Cardenas-Quispe & Pacheco, 2025; Farabi et al., 2025; Gangwar, 2024; Magar et al., 2024). These findings suggest that while QR code–based verification systems demonstrate considerable potential for improving credential authentication processes, further research is required to address practical implementation challenges and support the development of robust, scalable solutions for academic environments.

CONCLUSION

In conclusion, the systematic literature review (SLR) on QR code-based systems for academic credential verification underscores and verifies that the transformative potential of this technology in enhancing the efficiency, security, and user experience of verification processes is increasing day by day By serving as an essential medium that interlinks both physical and digital records with institutional databases, QR codes assume a pivotal function in streamlining and improving the mechanisms of real-time authentication, thereby substantially diminishing and mitigating various challenges typically associated with forgery and misrepresentation of academic credentials. The review highlights the different types of architectural approaches employed in these systems, ranging from centralized databases to decentralized

blockchain technologies, each with its own set of advantages and challenges. Furthermore, the research identifies critical security and privacy concerns that must be addressed to ensure the integrity and confidentiality of academic credentials. Despite the highly promising capabilities and functionalities offered by QR code systems, there exist notable limitations that include, but are not limited to, the absence of standardized frameworks and significant scalability issues, which continue to pose substantial obstacles to the widespread adoption and implementation of these systems across various educational institutions. As the landscape of higher education and universities continue to evolve, it becomes increasingly imperative that further research is conducted with the aim of refining these systems, addressing the existing gaps in their implementation, and ultimately developing robust and scalable solutions that steadfastly uphold the principles of academic integrity and foster trust in the verification of academic credentials.

ACKNOWLEDGEMENT

This work was supported by Universiti Islam Selangor (UIS) under the GPIU Research Grant Scheme.

REFERENCES

Abdullahi, M. U. (2022). Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code. *IOSR Journal of Computer Engineering (IOSR-JCE)*.

Ahmed, H. A., & Jang, J. W. (2018). Document Certificate Authentication System Using Digitally Signed QR Code Tag. *Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication*, 1–5. https://doi.org/10.1145/3164541.3164586

Aini, Q., Rahardja, U., Tangkaw, M. R., Santoso, N. P. L., & Khoirunisa, A. (2020). Embedding a Blockchain Technology Pattern Into the QR Code for an Authentication Certificate. *Jurnal Online Informatika*, 239–244. https://doi.org/10.15575/join.v5i2.583

Cardenas-Quispe, M. A., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. *Scientific Reports*, *15*(1), 9281. https://doi.org/10.1038/s41598-025-93913-6

Chennur, J., Mulla, M., Joy, J., Gosavi, K., & Gayke, P. S. (2021). *Digital Certificate System for Verification of Educational Certificates Using Blockchain*. *9*(6).

Essien, U. E., & Tumenayu, O. O. (2022). UNIVERSITY OF CROSS RIVER STATE CERTIFICATE VERIFICATION SYSTEM WITH EMBEDDED UNCLONABLE QUICK RESPONSE CODE DIGITAL SIGNATURE. *JOURNAL OF CONTEMPORARY RESEARCH (JOCRES)*, *1*.

Farabi, A., Khandaker, I., Ahsan, J., Shanto, I. K., Jahan, N., & Khan, M. J. (2025). *ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh* (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2508.05334

Gangwar, S. (2024). Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications. *International Journal of Computer Applications*, *186*.

Inyangetoh, J. A., & Johnson, E. A. (2025). Exploring the Efficiency of QR-Code Technology in Developing Authentication System for Admitting Students into Examination Hall for Polytechnics in Nigeria. *International Journal of Network and Communication Research*, *9*(1), 1–14. https://doi.org/10.37745/ijncr.16/vol9n1114

Kitchenham, B. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*. https://www.researchgate.net/publication/302924724

Kumar, D. N. (2024). Hybrid Digital Certificate Management System with QR Code and IoT Integrated on Hyperledger Fabric Blockchain. *International Journal of Maritime Engineering*. https://doi.org/10.5750/ijme.v1i1.1392

Magar, Kanke, & Kayte. (2024). Educational Document Verification through Blockchain: Literature Review. *International Journal of Scientific Research in Science and Technology*. https://doi.org/doi%2520:%2520https://doi.org/10.32628

Naser, M. A. U., Jasim, E. T., & Al-Mashhadi, H. M. (2020). QR code based two-factor authentication to verify paper-based documents. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *18*(4), 1834. https://doi.org/10.12928/telkomnika.v18i4.14339

Noorhizama, N. K., Abdullah, Z., Kasim, S., A Hamid, I. R., & Mat Isa, M. A. (2023). Verification of Ph.D. Certificate using QR Code on Blockchain Ethereum. *JOIV : International Journal on Informatics Visualization*, *7*(3), 716. https://doi.org/10.30630/joiv.7.3.1584

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … McKenzie, J. E. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ*, n160. https://doi.org/10.1136/bmj.n160

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008, June). *Systematic Mapping Studies in Software Engineering*. 12th International Conference on Evaluation and Assessment in Software Engineering (EASE). https://doi.org/10.14236/ewic/EASE2008.8

Ranjith, M. J., & Davuluri, S. S. (2025). Certificate Management System using Blockchain and Steganography Techniques. *International Conference on Innovative Computing & Communication (ICICC)*. http://dx.doi.org/10.2139/ssrn.5771262

Saleh, O. S., Ghazali, O., & Idris, N. B. (2023). A Privacy-Centered Protocol for Enhancing Security and Authentication of Academic Certificates. *International Journal of Advanced Computer Science and Applications*, *14*(2). https://doi.org/10.14569/IJACSA.2023.0140253

Shaik, C. (2021). *PREVENTING FORGED AND FABRICATED ACADEMIC CREDENTIALS USING CRYPTOGRAPHY AND QR CODES.*

Singhal, A., & S. Pavithr, R. (2015). Degree Certificate Authentication using QR Code and Smartphone. *International Journal of Computer Applications*, *120*(16), 38–43. https://doi.org/10.5120/21315-4303

Yahya, Z., Kamarzaman, N. S., Azizan, N., Jusoh, Z., Isa, R., Shafazand, M. Y., Salleh, N. S. A., & Mokhtaruddin, S. Z. S. (2017). A New Academic Certificate Authentication Using Leading Edge Technology. *Proceedings of the 2017 International Conference on E-Commerce, E-Business and E-Government*, 82–85. https://doi.org/10.1145/3108421.3108428