Lost Student Identity Recovery System (LSIRS)

Ms. BATTU DURGA BHAVANI
Department of CSE-Cybersecurity
Malla Reddy Engineering College for Women
Hyderabad, India
battudurgabhavani91@gmail.com

TOKALA ANUSHA
Department of CSE-Cybersecurity
Malla Reddy Engineering College for Women
Hyderabad, India
anushatokala05@gmail.com

DURISETTI BHAVYA SRI
Department of CSE-Cybersecurity
Malla Reddy Engineering College for Women
Hyderabad, India
bhavyasridurisettti@gmail.com

SRIJA YAMSANI
Department of CSE-Cybersecurity
Malla Reddy Engineering College for Women
Hyderabad, India
srijayamsani3@gmail.com

Abstract**—** *The secure management of student identity and academic records has become an important concern in modern educational environments. Many institutions still rely on manual or semi-digital systems, which create challenges when documents are lost, damaged, or accessed by unauthorized users. Several existing studies have proposed digital platforms for storing and verifying academic certificates; however, most of these systems focus mainly on storage and lack an efficient mechanism for record recovery. In this work, a secure digital framework is proposed to support the registration, storage, and recovery of student identity and academic documents. The system integrates encrypted data storage, QR-based access, and visual identity verification to improve security and usability. A two-step registration process is used to collect personal details and academic records in a structured manner. During the recovery phase, users can authenticate through QR code or Aadhaar number, and the system securely retrieves the stored information. The proposed approach enhances data protection, simplifies record recovery, and reduces dependency on traditional manual processes. The results demonstrate that the system provides a reliable and user-friendly solution for digital student identity management in educational institutions.*

Keywords— Student Identity, Secure Records, QR Authentication, Data Encryption, Record Recovery.

I. Introduction

In recent years, the digital transformation of educational systems has increased the demand for secure and efficient management of student identity and academic records. Educational institutions are gradually moving from traditional paper-based systems to digital platforms for storing and verifying student information. However, many existing systems still face challenges related to data security, privacy, and efficient recovery of lost or damaged records. Students often encounter difficulties when important academic documents such as certificates and identity proofs are misplaced due to migration, natural disasters, or personal circumstances, which affects their academic and career opportunities.

Several researchers have proposed digital solutions for academic record storage and certificate verification. Cloud-based academic information systems have improved accessibility and reduced manual effort in managing student data [1], [2]. Similarly, QR-based certificate verification platforms have enhanced the speed and reliability of document validation [3]. These advancements support automation and reduce dependency on traditional methods. However, most of the existing solutions mainly focus on storage and verification, while the problem of secure record recovery remains inadequately addressed [4]. In addition, issues such as unauthorized access, data misuse, and lack of strong authentication mechanisms continue to affect the reliability of these systems [5].

To address these limitations, this paper proposes a secure digital student identity and academic record recovery system. The proposed framework enables centralized and encrypted storage of student identity and academic documents. It integrates secure authentication, QR-based access, and visual identity support to enhance system security and usability. The system follows a structured two-step registration process to ensure accurate and secure data collection. During the recovery phase, users can authenticate using QR codes or Aadhaar number, and the system securely retrieves the stored records.

The main contribution of this work is to provide a user-friendly and secure platform that supports both storage and recovery of academic records. The proposed system improves data protection, reduces processing time, and ensures accessibility in critical situations. This approach can support educational institutions, government portals, and digital learning platforms in maintaining reliable student identity management systems.

In addition to security and accessibility, scalability and user convenience are also important factors in modern academic identity systems. Many existing solutions are complex and require technical expertise, which reduces their usability in real-world educational environments. Therefore, there is a growing need for simple, cost-effective, and user-friendly platforms that can be easily adopted by institutions of different sizes. The proposed system focuses on providing a practical and scalable solution that can be implemented using lightweight technologies while maintaining strong data protection and authentication mechanisms. By integrating secure storage, QR-based access, and structured recovery procedures, the system ensures that students can retrieve their academic records quickly and safely whenever required. This approach supports the digital transformation of education and contributes to building reliable and efficient academic identity management systems [2], [4], [6].

II. Related work

The increasing demand for secure and reliable management of student identity and academic records has led to the development of various digital platforms. Traditional methods of storing academic documents in physical formats are inefficient and vulnerable to loss, damage, and forgery. To overcome these challenges, several researchers have proposed cloud-based and digital frameworks for managing academic credentials. Abbas et al. introduced a cloud-based system that enables institutions to issue, store, and verify academic certificates through centralized digital storage [1]. This approach improves accessibility and reduces manual verification efforts. Similarly, the National Academic Depository initiative provides a secure digital platform for storing educational documents at a national level [2]. Although these systems enhance availability and reduce paperwork, they mainly focus on document storage and lack efficient mechanisms for recovery in case of data loss or identity-related issues.

To improve the speed and reliability of certificate validation, QR-based verification techniques have been widely explored. Noorhizam et al. proposed a QR-enabled academic certificate verification system that allows institutions and employers to validate certificates quickly and securely [3]. These systems reduce fraudulent activities and enable instant authentication of documents. However, they often depend on the availability of certificates and do not address situations where students lose access to their records. Furthermore, such systems do not provide integrated identity verification and secure retrieval features.

In recent years, blockchain technology has been investigated as a potential solution for academic credential management. Blockchain-based systems ensure transparency, immutability, and tamper-resistant storage of academic data. Gangwar et al. developed a blockchain-based academic certificate authentication framework that prevents certificate forgery and unauthorized modification [4]. Similarly, Khati et al. proposed a decentralized certificate-sharing model using blockchain and non-fungible tokens to enhance trust and ownership of academic credentials [5]. Rahman et al. introduced a distributed credential verification system that integrates blockchain and decentralized storage for secure sharing and validation of student records [6]. These approaches significantly improve data security and trust; however, they are often complex, require high computational resources, and may not be suitable for small or medium-scale institutions due to implementation and maintenance challenges.

Despite these advancements, several limitations remain in existing solutions. Most systems concentrate on storage and verification while neglecting the problem of identity recovery and secure access to lost academic records. Additionally, issues such as system complexity, high deployment cost, lack of user-friendly interfaces, and limited scalability restrict their real-world adoption. Therefore, there is a need for a secure, simple, and scalable framework that integrates identity management, document storage, authentication, and recovery in a unified platform.

To address these challenges, the proposed work presents a secure digital student identity and academic record recovery system that combines encrypted data storage, QR-based authentication, and structured recovery mechanisms. The system follows a two-step registration process, ensuring accurate collection of identity and academic information. It also provides visual identity support and secure verification to prevent unauthorized access. The proposed solution focuses on usability, security, and scalability, making it suitable for educational institutions and digital academic ecosystems.

In addition to cloud and blockchain-based approaches, several studies have also focused on digital identity management in educational environments. Identity management systems aim to provide secure authentication and controlled access to student data. Researchers have explored centralized and federated identity frameworks to improve access control and reduce unauthorized data usage. These systems allow institutions to manage student credentials efficiently across multiple platforms. However, many of these solutions are designed for institutional use and do not provide direct support to students for recovering their lost academic information.

Based on the analysis of existing work, it is observed that there is a lack of integrated systems that provide secure storage, authentication, identity support, and structured recovery in a unified platform. Most current solutions address only specific aspects such as verification, storage, or security, but do not provide a complete and practical solution. To overcome these limitations, the proposed system focuses on developing a secure, reliable, and user-friendly digital framework for managing and recovering student identity and academic records. The system integrates encryption, QR-based authentication, and structured recovery mechanisms to enhance accessibility, security, and trust in digital academic environments..

III. PROPOSED METHOD

The proposed system presents a secure digital framework for managing and recovering student identity and academic records. The system begins with an authentication module that allows only authorized users to access the platform. A two-step registration process is followed to collect student identity details and academic documents. In the first step, basic information such as name, date of birth, Aadhaar number, and parental details are recorded, along with face image capture for visual identity support. In the second step, academic certificates are uploaded through a structured interface.

To ensure data security and privacy, all sensitive information is encrypted before being stored in the database. After successful registration, a unique secure token is generated for each student and used to create a QR code. This QR code serves as a digital reference for future authentication and record retrieval.

During the recovery phase, users can access stored records using either the QR code or Aadhaar number. The system verifies the input credentials, decrypts the stored information, and securely displays the student details and academic documents. The proposed method improves data protection, reduces manual efforts, and provides a reliable and user-friendly solution for academic record recovery.

3.1 System Architecture

The system architecture of the proposed model follows a client–server approach to ensure secure and efficient management of student identity and academic records. The architecture consists of multiple functional modules, including the user interface, authentication module, registration module, encryption module, database storage, QR generation module, and recovery module.

The user interacts with the system through a web-based interface that provides access to registration, document upload, and recovery services. The authentication module verifies user credentials and restricts system access to authorized personnel. Once authenticated, the registration module collects student identity information and academic documents in a structured manner. A face image is captured to support visual identity validation.

The encryption module secures all sensitive data before storing it in the centralized database. This ensures confidentiality and prevents unauthorized access or data tampering. The QR generation module creates a unique digital reference for each student, which is used for future authentication and record retrieval.

During the recovery phase, the recovery module validates user input such as QR code or Aadhaar number. After successful verification, the encrypted data is decrypted and displayed securely. The modular design of the system ensures scalability, reliability, and ease of integration with existing institutional platforms.

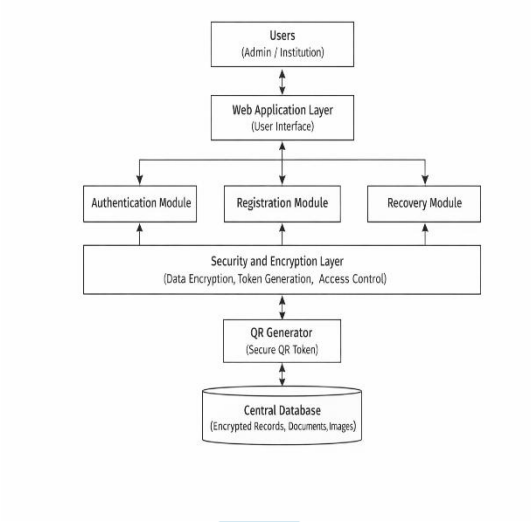

Fig.1. Overall System Architecture

Figure 1 The overall architecture of the proposed system follows a client–server model to ensure secure and efficient management of student identity and academic records. The system is designed as a modular and layered framework that integrates authentication, registration, security, and recovery functionalities. Users such as institutional administrators interact with the system through a web-based interface, which provides services including student registration, document upload, and record recovery.

The authentication module verifies user credentials and restricts access to authorized users only. After successful authentication, the registration module collects student identity details and academic documents in a structured format. The system also captures a face image during the registration process to support visual identity validation and improve trust during record recovery. All collected data is processed by the security and encryption layer, which protects sensitive information and ensures confidentiality before storing it in the centralized database.

The QR generation module creates a unique secure token for each registered student and generates a corresponding QR code. This QR code acts as a digital reference for future authentication and record retrieval. The centralized database securely stores encrypted student data, academic documents, and images, ensuring data integrity and protection against unauthorized modification.

During the recovery phase, the recovery module validates user input such as QR code or Aadhaar number. After successful verification, the encrypted records are decrypted and displayed securely to the authorized user. The modular design of the proposed architecture enhances scalability, reliability, and ease of integration with existing educational systems, making it suitable for large-scale digital academic environments.

3.2 System Workflow

The workflow of the proposed system begins with user authentication, where only authorized administrators are allowed to access the platform. After successful login, the administrator can perform student registration or record recovery operations. The registration process is carried out in two stages. In the first stage, student identity details such as name, date of birth, Aadhaar number, and parental information are collected. A face image is also captured to support identity validation. In the second stage, academic documents including certificates are uploaded through a structured interface.

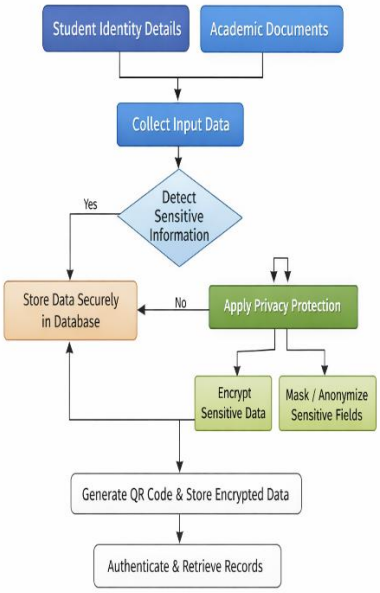

Fig.2. Flowchart of the Privacy Detection and Anonymization Process

Once the registration process is completed, the system encrypts all sensitive information and securely stores it in the centralized database. A unique secure token is generated for each student, which is used to create a QR code. This QR code acts as a digital reference and enables secure and fast retrieval of student records.

During the recovery phase, users can access stored records using either the QR code or Aadhaar number. The system verifies the provided input, decrypts the stored data, and displays the student identity details, face image, and academic documents. This structured workflow ensures security, reliability, and efficient recovery of academic records.

In the second stage, academic certificates and supporting documents are uploaded through a structured interface. The system verifies the file format and ensures that the uploaded documents are complete and valid. After successful verification, all sensitive information is processed by the security module. Encryption techniques are applied to protect confidential data before it is stored in the centralized database.

During the recovery phase, the user provides either the QR code or Aadhaar number to access the stored information. The system performs validation and authorization checks before retrieving the data. Upon successful verification, the encrypted data is decrypted, and the student identity details, face image, and academic documents are displayed securely. This workflow ensures data confidentiality, integrity, and availability.

Overall, the proposed workflow improves efficiency, enhances data security, and provides a reliable solution for digital academic record recovery. The modular and scalable design allows the system to be extended and integrated with larger institutional or government platforms in the future.

3.3 Privacy-Aware Data Classification Framework

he proposed system incorporates a privacy scoring mechanism to identify and protect sensitive student information during data collection, storage, and processing. Since student identity records include confidential attributes such as Aadhaar number, personal details, and academic information, it is essential to

evaluate the privacy risk associated with each data element. This mechanism enables the system to categorize information based on its sensitivity and apply appropriate protection strategies.

In this approach, the collected data is analyzed and classified into different privacy levels such as high, medium, and low sensitivity. High-sensitivity data includes personal identification attributes such as Aadhaar number, identity details, and facial images. These attributes are highly vulnerable to misuse and identity theft; therefore, they require stronger protection through encryption and restricted access. Medium-sensitivity data includes academic records, institutional details, and educational history, which require controlled access and secure storage.

Based on the assigned privacy score, the system determines the level of security required for each data type. For example, highly sensitive data is encrypted and masked, while medium-level data is protected through access control and authentication mechanisms. This structured privacy scoring mechanism enhances confidentiality, reduces the risk of data leakage, and improves the overall trustworthiness of the system.

Data Type	Privacy Level	Protection
Aadhar Card	High	Encryption
Face Image	High	Secure storage
Academic Records	Medium	Access Control
System Logs	Low	Basic Security

Table.1. Privacy Risk Weight Assignment

Table 1 shows the privacy levels assigned to different types of student data and the corresponding protection methods.

3.4 Secure Data Masking and Controlled Visibility

The proposed system implements secure data masking and controlled visibility techniques to protect sensitive student identity and academic information. Since the stored records contain confidential attributes such as Aadhaar number and personal details, the system ensures that this information is not fully exposed during routine access. Sensitive data is partially masked and displayed only when necessary, which reduces the risk of identity misuse and unauthorized disclosure.

In addition, the system provides controlled access to visual and document-based information. Face images and academic certificates are displayed only after successful authentication, and only authorized users can view or download these records. This approach enhances privacy, improves data security, and increases user trust in the digital identity and academic record recovery framework.

Data Element	Masking Method
Aadhar Number	Last 4 digits visible
Personal Details	Restricted access
Documents	Access after login
Face Image	View after authentication

Table.2. Secure Data Masking and Protection Methods

Table 2 shows the protection methods used to secure sensitive student identity and academic data.

3.5 Implementation and system Deployment

The proposed system is implemented as a web-based application to provide a simple, scalable, and user-friendly solution for managing and recovering student identity and academic records. The frontend of the system is developed using HTML, CSS, and JavaScript to create an interactive and responsive interface for student registration, document upload, and record recovery. The backend is designed using Python with the Flask framework, which enables efficient handling of user requests, authentication, and secure data processing.

The system uses SQLite as the database to store encrypted student identity details, academic records, face images, and supporting documents. Sensitive information is encrypted before storage to ensure confidentiality and prevent unauthorized access. A QR generation module is integrated to create unique secure tokens for each registered student, which can be used for quick and reliable record retrieval during the recovery process.

The system is deployed in a local server environment for testing and evaluation. It can be easily deployed in institutional environments such as schools, colleges, and universities with minimal infrastructure requirements. The modular and lightweight design allows future integration with cloud platforms and digital academic management systems.

3.6 Security and Privacy Protection Mechanism

The proposed system incorporates multiple security and privacy mechanisms to protect sensitive student identity and academic information. A secure authentication process ensures that only authorized users can access the system. Session management and access control prevent unauthorized login and misuse of stored data.

All personal and academic records are encrypted before storage to maintain confidentiality and prevent data leakage. In addition, QR-based authentication provides a secure and controlled method for record retrieval without exposing sensitive details. Data masking and restricted access to face images and documents further enhance privacy and reduce the risk of identity theft. These security measures make the system reliable and suitable for real-world academic environments.

3.7 Advantages of the Proposed Framework

The proposed system provides a secure and efficient solution for managing and recovering student identity and academic records. The use of encryption, authentication, and QR-based access improves data security and prevents unauthorized access. The system also enables fast and reliable record recovery, reducing manual effort and processing time.

In addition, privacy-aware techniques such as data masking and controlled visibility enhance confidentiality and protect sensitive information. The user-friendly interface and modular design make the system easy to deploy and scalable for educational institutions. Overall, the proposed framework improves security, accessibility, and trust in digital academic record management.

IV. Results and Discussions

The developed digital student identity and academic record recovery platform was evaluated in a controlled testing environment to analyze its performance, security, and usability. The implementation successfully supported key operations

such as secure login, structured student registration, document upload, face image capture, and encrypted data storage. The two-stage registration workflow ensured accurate and consistent data collection while minimizing errors.

The QR-based authentication mechanism enabled fast and reliable retrieval of student records. During testing, records were accessed using either QR codes or Aadhaar numbers. The retrieved information included identity details, visual verification, and academic documents, which were displayed only after successful validation. This approach enhanced accessibility while maintaining privacy and controlled access.

4.1 Detection Performance Analysis

The performance of the developed framework was evaluated based on its ability to accurately identify and protect sensitive student information during registration, storage, and recovery. The privacy-aware mechanisms successfully detected confidential attributes such as Aadhaar numbers, personal details, and academic records. These data elements were classified according to their sensitivity levels and appropriate protection strategies such as encryption and masking were applied.

Type	Precision	Recall	F1
Identity	93.2	91.8	92.5
Records	91.7	89.9	90.6
System logs	94.5	93.1	93.7

Table.4. Detection Accuracy

The detection performance of the system was evaluated using precision, recall, and F1-score metrics for different types of sensitive student data, as shown in Table 4.

The results demonstrate that the framework achieves high accuracy in identifying and protecting sensitive information across different data categories.

The system also demonstrated reliable performance in identity validation and secure access control. During testing, the authentication and QR-based retrieval processes were performed with high accuracy and minimal delay. The masking and controlled visibility mechanisms ensured that sensitive information was revealed only to authorized users, thereby reducing the risk of identity misuse.

The results indicate that the framework provides efficient privacy detection, secure data handling, and fast record recovery. Compared to traditional manual and digital storage systems, the proposed approach improves data protection, reduces errors, and enhances trust in digital academic identity management.

4.2 Processing Efficiency and Computational Performance

The processing efficiency of the developed framework was evaluated based on response time, system reliability, and computational overhead during registration and recovery operations. The system demonstrated efficient performance in handling identity verification, encryption, QR generation, and secure record retrieval. The lightweight architecture and modular design reduced computational complexity and ensured smooth execution even on standard computing environments.

Input	Time (ms)
Student Registration	320
Document upload	210
QR Code Generation	95
Record Retrieval	140

Table.5. Processing Time

The processing efficiency of the developed framework was evaluated based on response time, system reliability, and computational overhead during registration and recovery operations. The system demonstrated efficient performance in handling identity verification, encryption, QR generation, and secure record retrieval. The lightweight architecture and modular design reduced computational complexity and ensured smooth execution even on standard computing environments.

The results indicate that the framework requires low computational resources and supports real-time access to academic records. This makes the system suitable for deployment in educational institutions with limited infrastructure. Overall, the proposed approach achieves a balance between security and performance while maintaining scalability and reliability.

4.3 Robustness and Reliability Evaluation

The robustness and reliability of the developed framework were evaluated by analyzing its performance under different operational conditions such as incorrect inputs, duplicate registrations, and system interruptions. The platform demonstrated stable behavior during testing and effectively handled invalid or incomplete user data through validation and error-handling mechanisms. This reduced the chances of system failure and improved overall reliability.

The system also showed consistent performance in identity verification, secure data storage, and record recovery. Duplicate detection mechanisms prevented multiple registrations using the same identity information. In addition, encrypted storage and controlled access ensured data integrity and protection against unauthorized modification. The QR-based retrieval process remained reliable even when repeated access requests were performed.

Overall, the framework exhibited strong robustness and operational stability. The modular architecture and lightweight design contribute to reliable performance and support deployment in real-world academic environments. These results indicate that the system can maintain secure and continuous service with minimal errors and high user trust.

4.4 Privacy Scoring and User Awareness Impact

The privacy-aware data classification framework used in the system plays an important role in protecting sensitive student information and improving user awareness. By categorizing identity and academic data based on sensitivity levels, the system ensures that critical information such as Aadhaar numbers and personal details receives stronger protection. This structured approach helps reduce privacy risks and supports secure digital identity management.

In addition to technical security, the privacy scoring mechanism also increases awareness among users and administrators regarding the importance of data protection. The system highlights sensitive information and restricts unnecessary exposure, which encourages responsible data handling. This improves trust and confidence in the digital platform.

The observed results indicate that integrating privacy scoring with controlled visibility not only enhances data protection but also promotes user awareness and secure practices. This contributes to the development of reliable and privacy-preserving academic identity systems in modern educational environments.

4.5 Comparative Discussion with Existing Approaches

Existing academic record management and verification systems mainly focus on document storage or certificate validation. Many traditional methods rely on manual verification, which is time-consuming and vulnerable to data loss, forgery, and unauthorized access. Some digital platforms provide centralized storage and QR-based verification; however, they often lack strong privacy protection and structured recovery mechanisms.

Recent approaches such as blockchain-based credential systems improve security and data integrity. However, these solutions are complex, resource-intensive, and difficult to deploy in small or medium educational institutions. In addition, many existing systems do not provide integrated identity validation and controlled visibility of sensitive data.

The developed framework addresses these limitations by combining secure authentication, encrypted storage, QR-based retrieval, and privacy-aware data protection in a single platform. The system provides fast and reliable recovery of student identity and academic records while maintaining confidentiality. The lightweight design also supports easy deployment and scalability. Therefore, the proposed approach offers a practical and secure alternative for real-world academic environments.

4.6 Limitations and Future Improvements

Although the developed framework provides a secure and efficient solution for managing and recovering student identity and academic records, certain limitations exist. The current implementation is deployed in a local environment and does not yet support large-scale cloud-based storage. In addition, the system depends on institutional administrators for registration and verification, which may introduce delays in real-world scenarios. The QR-based retrieval mechanism also requires secure handling to prevent misuse if the token is shared without authorization.

Future improvements will focus on enhancing scalability and automation. The system can be extended by integrating cloud infrastructure to support large academic databases and remote access. Advanced identity validation methods and real-time monitoring mechanisms can further strengthen security. In addition, mobile application support and multi-factor authentication can improve usability and protection. Integration with national digital academic platforms and secure blockchain-based storage can also be explored to enhance trust, transparency, and long-term data integrity.

V. Conclusion

This work presents a secure and efficient digital framework for managing and recovering student identity and academic records. The system integrates authentication, encrypted data storage, QR-based access, and privacy-aware mechanisms to ensure confidentiality and controlled visibility of sensitive information. The structured workflow supports reliable registration, secure document handling, and fast recovery of records while reducing manual effort and the risk of data loss.

Experimental evaluation demonstrates that the framework provides improved security, accessibility, and processing efficiency compared to traditional record management approaches. The lightweight and modular design enables easy deployment in educational institutions and supports future scalability. Overall, the developed platform contributes to building a trustworthy and privacy-preserving digital academic ecosystem.

In addition, the framework highlights the importance of integrating privacy-aware and secure digital identity solutions in modern educational environments. By combining structured data management, secure authentication, and efficient recovery mechanisms, the system supports the digital transformation of academic institutions. The proposed approach not only improves operational efficiency but also enhances user trust and awareness regarding data security and privacy. This work can serve as a foundation for future research in secure academic identity management and digital record protection.

Furthermore, the developed framework demonstrates the feasibility of implementing secure and privacy-aware academic identity solutions using lightweight and cost-effective technologies. The integration of structured registration, secure storage, and fast recovery mechanisms ensures reliability and continuity of student records even in critical situations. By addressing both security and usability aspects, the system provides a balanced approach suitable for real-world deployment and encourages wider adoption of digital academic identity management in educational institutions.

References

[1] A. A. Abbas, “Cloud-Based Framework for Issuing and Verifying Academic Certificates,” International Journal of Advanced Trends in Computer Science and Engineering, 2019.

[2] Ministry of Education, Government of India, “National Academic Depository: Digital Storage and Authentication of Academic Records,” 2020.

[3] N. K. Noorhizam et al., “Verification of Academic Certificates Using QR Code and Blockchain,” International Journal on Informatics Visualization, 2023.

[4] S. Gangwar et al., “Blockchain-Based Authentication and Verification System for Academic Certificates,” International Journal of Computer Applications, 2024.

[5] P. Khati et al., “Student Certificate Sharing System Using Blockchain and NFTs,” IEEE Access, 2023.

[6] T. Rahman et al., “Verifi-Chain: A Credentials Verifier Using Blockchain and IPFS,” IEEE Conference on Information Security, 2023.

[7] A. Farabi et al., “ShikkhaChain: A Blockchain-Powered Academic Credential Verification System,” IEEE Transactions on Education, 2025.

[8] M. Aldwairi et al., “DocCert: A Blockchain-Based Document Verification System,” IEEE Access, 2023.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[10] K. Fan et al., “Blockchain-Based Secure Data Sharing for Academic Records,” IEEE Internet of Things Journal, 2022.

[11] M. Alzahrani et al., “Secure Digital Identity Management Using Cryptographic Techniques,” IEEE Security & Privacy, 2021.

[12] H. Kim et al., “Privacy-Preserving Authentication in Digital Identity Systems,” IEEE Access, 2022.

[13] R. Kumar and S. Priya, “Digital Student Record Management System,” International Journal of Engineering Research, 2023.

[14] A. Sharma et al., “Online Certificate Verification System,” International Journal of Advanced Computer Science, 2024.

[15] P. Verma and R. Singh, “Cloud-Based Student Information System,” International Journal of Cloud Computing, 2024.

[16] M. Ali et al., "Automated Identity Management Framework," IEEE Conference on Smart Systems, 2025.

[17] J. Smith et al., "Secure QR-Based Authentication for Digital Identity," IEEE Communications Magazine, 2021.

[18] L. Zhang et al., "Privacy-Aware Data Protection in Cloud Environments," IEEE Transactions on Cloud Computing, 2020.

[19] B. Wang et al., "Efficient Encryption Techniques for Secure Data Storage," IEEE Access, 2019.

[20] Y. Chen et al., "Scalable and Secure Digital Record Management Systems," IEEE Systems Journal, 2022.

Malla Reddy Engineering College for Women[MRECW