JOURNAL OF INFORMATION SYSTEMS AND TECHNOLOGY

Journal of Information Systems and Technology
ISSN 3110-4096 (online)
https://athallahpublishing.com/index.php/jaip/index

OPEN ACCESS

Vol. 2, No. 1, 2026

DOI: 10.64845/jistech.v1i2

Development of a Web-Based TOEFL E-Certificate System with QR Code Verification and AES–SHA-256 Security Framework

Zainal Arifin
Universitas Gunadarma, Indonesia
Corresponding Author: zainalarf@gmail.com

A B S T R A C T

The rapid advancement of digital technologies has accelerated the adoption of electronic certification systems in higher education institutions, including TOEFL certificate management. However, issues related to document authenticity, data security, and verification reliability remain significant challenges. This study aims to develop a secure web-based TOEFL electronic certificate (e-certificate) system that integrates QR code verification with cryptographic techniques, specifically the Advanced Encryption Standard (AES) and Secure Hash Algorithm 256 (SHA-256). The proposed system enables efficient certificate generation, storage, and validation while ensuring data integrity and protection against unauthorized access and forgery. QR codes are utilized to provide instant and user-friendly verification, linking each certificate to a secure database. AES encryption is applied to safeguard sensitive data, while SHA-256 hashing ensures the integrity and authenticity of certificate information. The system is developed using a structured software development approach and evaluated through functional testing and user acceptance testing. The results indicate that the proposed system significantly enhances security, reliability, and efficiency compared to conventional certificate management methods. Furthermore, it provides a scalable and practical solution for academic institutions seeking to implement secure digital certification systems.

Keywords: Web-Based System, TOEFL E-Certificate, QR Code Verification, AES–SHA-256 Security

Received:	Revised:	Accepted:	Available online:
01.12.2025	01.02.2026	01.04.2026	26.06.2026

INTRODUCTION

The rapid advancement of digital technology has significantly transformed various sectors, including education, administration, and certification systems. Higher education institutions are increasingly adopting digital solutions to improve efficiency, accessibility, and security in managing academic records. One notable transformation is the shift from conventional paper-based certificates to electronic certificates (e-certificates), particularly in standardized testing environments such as the Test of English as a Foreign Language (TOEFL). This transition is driven by the need for faster processing, easier distribution, and improved document management in a digital era (Hassanin et al., 2024).

Despite these advantages, the implementation of e-certificate systems introduces several critical challenges, especially in terms of security, authenticity, and verification. Traditional certificate systems are vulnerable to forgery, duplication, and unauthorized modification, which can undermine the credibility of issuing institutions. In the context of TOEFL certification, where certificates are often used for academic admissions and professional requirements, ensuring authenticity and trustworthiness becomes paramount. Therefore, a secure and reliable system for managing and verifying electronic certificates is urgently needed (Dehimi & Tolba, 2024).

Recent studies have highlighted the importance of integrating advanced security mechanisms into digital certification systems. Cryptographic techniques such as encryption and hashing have become essential tools for protecting sensitive information and maintaining data integrity. The Advanced Encryption Standard (AES) is widely recognized for its efficiency and robustness in securing data, while the Secure Hash Algorithm 256 (SHA-256) is commonly used to ensure data integrity and prevent tampering. These technologies provide a strong foundation for developing secure e-certificate systems that can resist various cyber threats (Zhao et al., 2024). In addition to cryptographic protection, verification mechanisms play a crucial role in ensuring the authenticity of digital certificates. One of the most effective and widely adopted methods is the use of Quick Response (QR) codes. QR codes enable fast and convenient verification by linking certificate data to a secure online database. Users can easily scan the code using mobile devices to access verification information, making the process efficient and user-friendly. This approach has been successfully implemented in various domains,

including digital identity systems and academic credential verification (Parcalabescu & Frank, 2023).

However, existing implementations of QR code-based verification systems often lack comprehensive security integration. Many systems rely solely on QR codes without incorporating strong encryption and hashing mechanisms, leaving them susceptible to manipulation and unauthorized access. Furthermore, some systems do not provide real-time validation or fail to ensure the integrity of stored data, resulting in potential security vulnerabilities. These limitations highlight the need for a more robust and integrated approach that combines verification mechanisms with advanced cryptographic techniques (Ghaleb et al., 2023). Another challenge lies in the scalability and usability of e-certificate systems. As the number of users and certificates increases, the system must be able to handle large volumes of data without compromising performance. Additionally, the system should provide an intuitive interface for administrators and users, ensuring ease of use while maintaining high security standards. Web-based systems offer a promising solution to these challenges by providing centralized access, real-time updates, and platform-independent usability (Moorthy & Moon, 2025).

From a methodological perspective, the development of a secure e-certificate system requires a structured and systematic approach. Software development models such as the Rational Unified Process (RUP) or other iterative frameworks are commonly used to ensure that system requirements are clearly defined and implemented effectively. These approaches facilitate the design, development, testing, and deployment of robust systems that meet both functional and non-functional requirements (Niu et al., 2021). In the context of Global Jakarta University, the current TOEFL certificate management system still faces several limitations, particularly in terms of manual verification and limited security features. The absence of an integrated digital verification system increases the risk of certificate forgery and delays in validation processes. Therefore, there is a pressing need to develop a web-based TOEFL e-certificate system that incorporates advanced security mechanisms and efficient verification methods.

This study proposes the development of a secure web-based TOEFL e-certificate system that integrates QR code verification with AES encryption and SHA-256 hashing. The proposed system aims to enhance

the security, reliability, and efficiency of certificate management and verification processes. By combining these technologies, the system ensures that certificate data is protected from unauthorized access while maintaining its integrity and authenticity. The novelty of this research lies in the integration of multiple security layers within a single system framework. Unlike previous studies that focus on either verification or encryption, this study combines QR code-based verification with robust cryptographic techniques to provide a comprehensive security solution. Additionally, the system is designed to be scalable and user-friendly, making it suitable for implementation in higher education institutions.

The objectives of this study are threefold. First, to design and develop a web-based TOEFL e-certificate system that supports secure certificate generation and management. Second, to implement QR code verification as a fast and reliable method for certificate validation. Third, to enhance data security and integrity using AES encryption and SHA-256 hashing. Through these objectives, the study aims to address existing gaps in digital certificate systems and provide a practical solution for real-world applications. The significance of this research extends beyond the academic domain. A secure and reliable e-certificate system can improve trust in digital credentials, reduce administrative workload, and enhance the overall efficiency of certification processes. Moreover, the integration of advanced security technologies contributes to the broader field of information systems by demonstrating the practical application of cryptography in real-world scenarios.

In conclusion, the transition to digital certification systems presents both opportunities and challenges. While e-certificates offer numerous advantages in terms of efficiency and accessibility, ensuring their security and authenticity remains a critical concern. By integrating QR code verification with AES and SHA-256 security mechanisms, this study provides a comprehensive approach to addressing these challenges. The proposed system not only enhances the reliability of TOEFL certification at Global Jakarta University but also offers a scalable and secure solution that can be adopted by other institutions in the future. In the Industrial Revolution 4.0 era, information and communication technology as developed rapidly, encouraging significant changes in various aspects of life. Conventional methods are gradually being replaced by more efficient digital approaches, such as QR Code technology, which has been widely applied in various fields including education. At Jakarta Global

University, the certificate issuance process is still carried out manually, leading to inefficiencies, delays, and vulnerability to forgery. This research proposes the development of a web-based TOEFL electronic certificate system integrated into the CEdEC web application, equipped with QR Code verification, AES encryption for confidentiality, and SHA-256 hashing for data integrity.

METHOD

This study adopts the Rapid Application Development (RAD) methodology to design and implement the proposed system. RAD is chosen due to its emphasis on rapid prototyping, iterative development, and active user involvement throughout the development lifecycle. This approach allows for faster system delivery while ensuring that the final product aligns with user requirements and expectations (Pressman & Maxim, 2021; Sommerville, 2022). The development process consists of four main stages: requirements planning, user design, construction, and implementation. Each stage plays a critical role in ensuring the successful development of the system and supports a structured yet flexible development cycle (Sommerville, 2022).

In the requirements planning phase, the system requirements are identified through direct interaction with users, including observation and interviews with CEdEC staff. This stage focuses on analyzing existing problems in the certificate issuance process and defining system requirements that address these challenges. The analysis ensures that the developed system meets both functional and non-functional requirements. Two primary actors are identified in the system: the admin, who is responsible for managing certificate data, and the user, who is responsible for registration and certificate verification. User-centered requirement analysis is essential to ensure system usability and effectiveness in real-world applications (Hassanin et al., 2024).

The user design phase involves close collaboration between developers and users to design the system. This stage includes the creation of system models and interface prototypes to visualize how the system will operate. Unified Modeling Language (UML) is used to represent system functionality and workflows through diagrams such as use case diagrams, activity diagrams, class diagrams, and sequence

diagrams. Additionally, prototype designs are developed using Axure RP software, allowing users to provide feedback and suggest improvements. This iterative process ensures that the system design aligns with user expectations and operational needs, which is a key principle in modern software engineering practices (Dehimi & Tolba, 2024). During the construction phase, the system is developed based on the approved design. The implementation utilizes the Laravel framework as the core development platform, supported by PHP for server-side programming and MySQL for database management. Front-end components are developed using HTML and CSS, along with supporting libraries to enhance user interface and user experience. At this stage, the integration of QR Code generation, AES encryption, and SHA-256 hashing is carried out to ensure system security and functionality. The use of cryptographic techniques such as AES and SHA-256 is widely recognized for enhancing data confidentiality and integrity in web-based systems (Zhao et al., 2024).

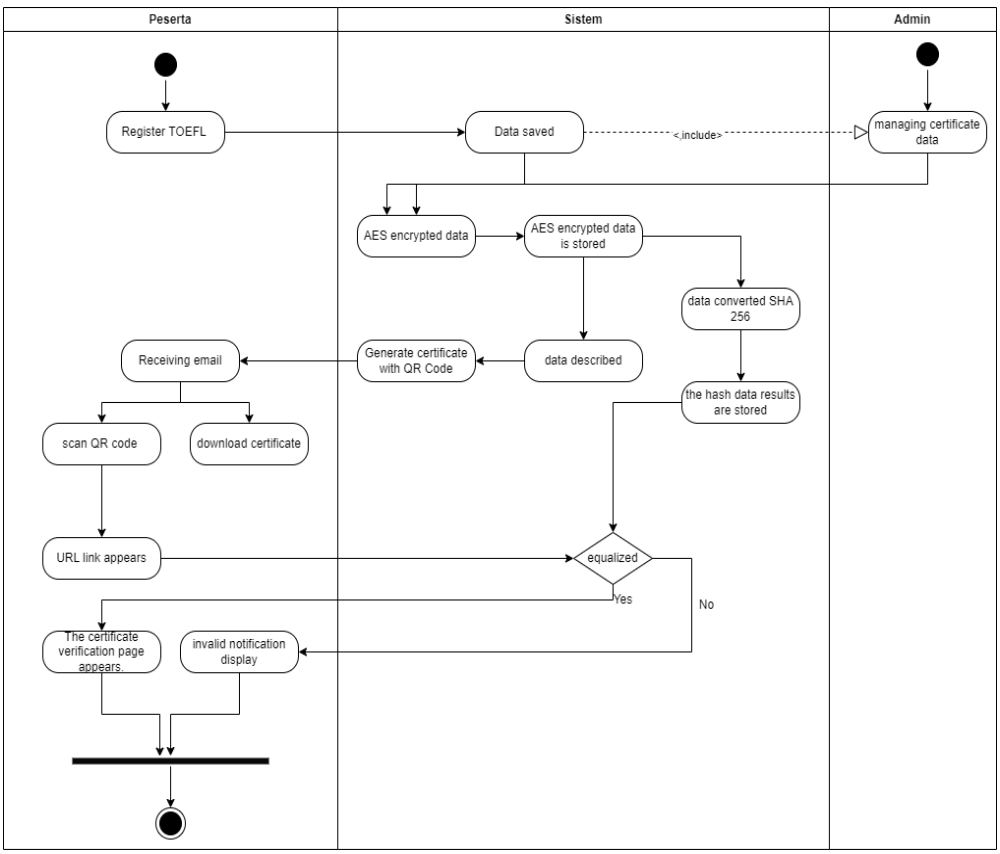

Figure 1. Activity Diagram Generate and Verify Electronic Certificates with Security

Figure 2 shows the process flow for creating and verifying a digital certificate integrated with QR Code security. The process begins when a participant registers for the TOEFL. Once registration is complete, participant data is automatically stored in the system. The administrator is then responsible for managing the certificate data. The system then processes the stored data through two parallel security channels. First, the data is encrypted using the AES algorithm and stored, then used to generate a certificate and QR Code. This encrypted data can then be decrypted for verification purposes. Second, the data is converted into a hash value using the SHA-256 method, and the resulting hash is stored separately as a data integrity verification step.

Algoritma kriptografi AES (*Advanced Encryption Standart*)

The 128-bit AES encryption trial process was carried out with the plain text TOEFLJGUCEdECdpk and the cipher key KampusJGUCEdEC25. The plain text and cipher key were converted to hexadecimal form, then an XOR operation was performed in the initial round stage [3] like FIGURE 3.

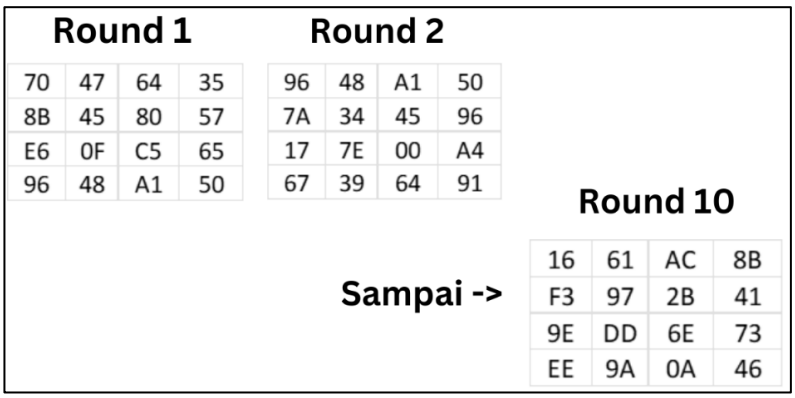

Figure 2. Key Generation Stage

Next, the key generation was carried out for 10 rounds through four iterative steps (SubBytes, ShiftRow, MixColumn, AddRoundKey), resulting in a final output of 177675589BEA6945379358EB1B22E28E (hexadecimal).

Algoritma kriptografi SHA-256 (*Secure Hash Calculation*)

After obtaining the encryption key from the AES process, the next step is to generate a hash using the SHA-256 algorithm. For the message

"**JGU**", it is first converted to binary, padded with a '1' bit followed by '0' bits until the length meets the 448-bit requirement, and appended with its original length in 64-bit binary.

The message is then divided into sixteen 32-bit words, and an initial hash value (H0–H7) is set according to SHA-256 standards. Using the defined message schedule and constants, the SHA-256 computation is performed through iterative rounds of bitwise operations.

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

Also prepare the SHA-256 coefficients specified in the SHA-2 standard. Now that everything needed for SHA-256 computation is ready, it's time to perform SHA-256 computation using the following formula:

$$T_1 = h + h + \sum_{1}^{(256)}(e) + Ch(e,f,g)K_1^{(256)} + W_t$$

$$T_1 = \sum_{0}^{(256)}(a) + Maj(a,b,c)$$

$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T_1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T_1 + T_2$$

The final iteration result is added to the initial hash values, producing the 256-bit message digest:

ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f200

15ad. In this phase, after the design stage has been approved by the users, the author begins coding to transform the system design into a planned application, taking user feedback into account. At this stage, the developed system undergoes 13 test scenarios using the Black Box Testing method to reduce the risk of system defects before being used by

end users. The testing is conducted using the Equivalence Partitioning technique.

RESULTS AND DISCUSSION

The developed system includes several main features: TOEFL registration form, admin panel for managing test data, score input form, certificate generation, and QR Code verification page. The AES encryption successfully secured confidential participant data, and SHA-256 hashing ensured the integrity of stored certificates. Black Box testing was carried out on 13 functional scenarios, all of which passed successfully (100% success rate), indicating the system's functionality and stability. QR Code verification allowed real-time validation of certificate authenticity by scanning the code and retrieving encrypted and hashed data for integrity checking.

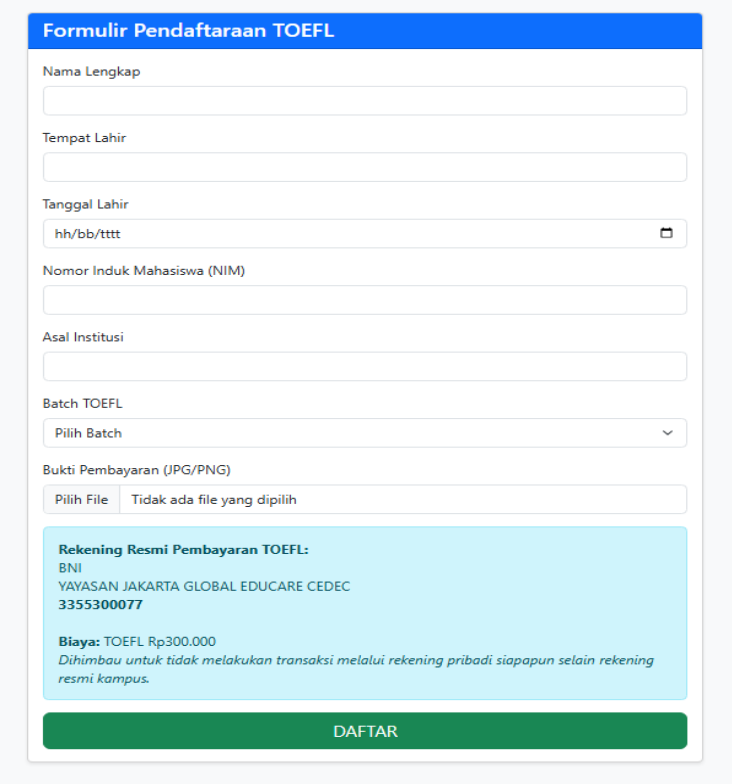

Figure 3. TOEFL Registration Form Page

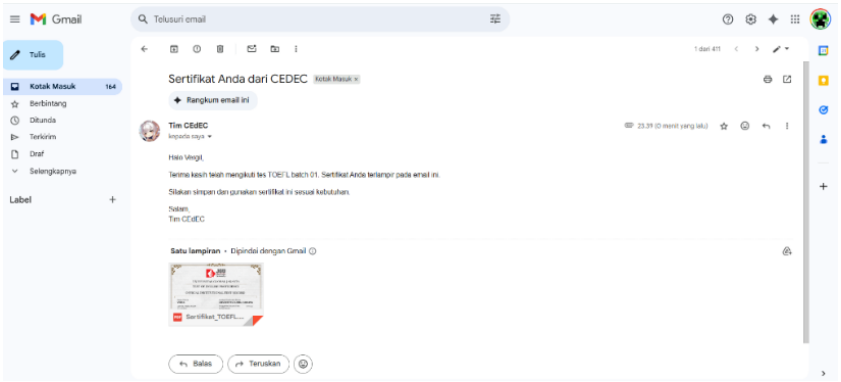

Figure 4 Enroll in The TOEFL Program

One of the core features is the TOEFL registration form, as shown in Figure 4, which serves as the initial interface for users to enroll in the TOEFL program at Universitas Global Jakarta. This form is designed to collect personal data and registration details, such as full name, place and date of birth, student ID number, institution of origin, TOEFL batch selection, and uploading proof of payment in JPG/PNG format. Once all data is filled in, users can click the REGISTER button to process the registration and navigate to the successful registration page.

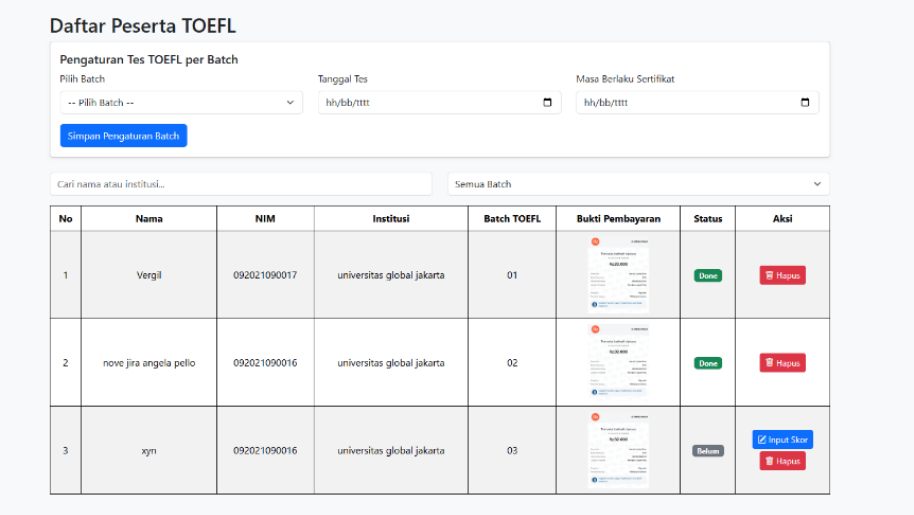

Figure 5. TOEFL Participant List Page

Figure 5. shows the implementation of the TOEFL participant data management feature, including the user interface and functional test results. This page displays the participant list and provides management features such as batch settings, score editing, and data deletion. Admins can view participant information, including name, student ID number,

institution, TOEFL batch, proof of payment, status, and action options, with confirmation via success notification.

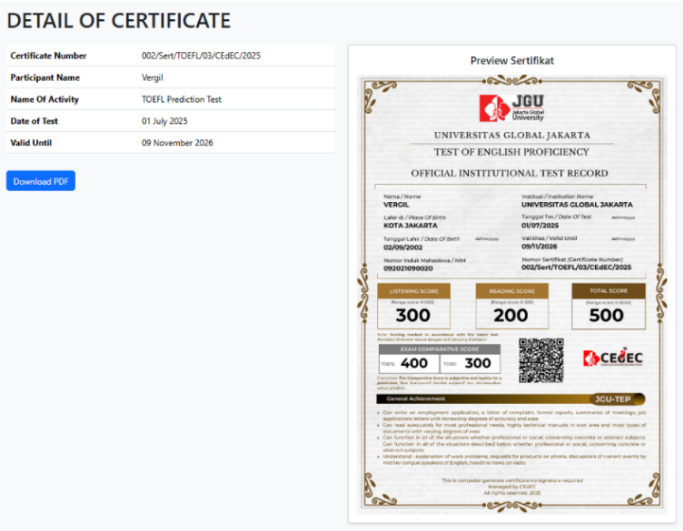

Figure 6. Email Receiving Page

Figure 6. is a page for users who have received an email, along with its contents in the form of a certificate in PDF format.

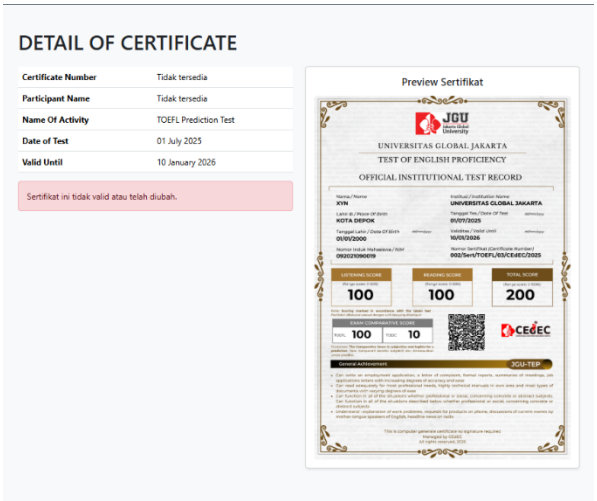

Figure 7. Certificate Verification Page

Figure 7, the system successfully displays the certificate verification page that matches the stored data, including Certificate Number, Participant Name, Activity Name, Test Date, Validity Date, and score on the certificate preview. The following table

compares the original data with the data that has been encrypted with AES into the database:

Tabel 1. Comparison Table of Original Data and Encrypted Data

Data Categories	Original Data	Encrypted Data
Name	Vergil	eyJpdiI6IjBsVlFjRGswcUZlS0YzbmJOK3lDa3c9PSIsInZhbHVlIjoiYTlxdTZleGJYUm53Z0piVUVZRmlWdz09IiwibWFjIjoiM2FkNDYwNmY3M2UwMzUxMGY4ZjBkYjhjMDM2YzVjZmYwNzgyYmM0N2EyMjk4MWMyNDUxOTZkM2M5YmYwNjRiNiIsInRhZyI6IiJ9
Place of birth	Kota Jakarta	eyJpdiI6IlhLL2ZBejlRdjlscTljKzFibnJKVnc9PSIsInZhbHVlIjoiVkpDU1ZPY2dNdUw1R2dyakVCckc5dz09IiwibWFjIjoiODQ2MTdkN2NhMDQyNjFjOTA2YTcyNjNkNDJmOGI4NTg2NDE5MzZjYjcxYjQ0NTZjNDdiMTliYjNmZjVmMGZhNyIsInRhZyI6IiJ9
Date of birth	02/09/2002	eyJpdiI6IkJiK2ViVXlNcGxMVXR3T3ZPWUV3aWc9PSIsInZhbHVlIjoiajVBcU1nd3hUUCs0TFJscE5sZGdBZz09IiwibWFjIjoiYzcwMGZmZDVjNjJiODMwMWFmZDU4MGUzOGUwYmJjMDFhNTEwOWY2MTAzOWFlYjI3NDg4MzhjNjU1ZmRlYTc0MiIsInRhZyI6IiJ9

When a certificate is created or renewed, the system calculates a hash of the encrypted data and stores it in the database. For verification, the encrypted data and date are retrieved, recalculated in the same order, and compared to the stored hash.Thehashvalue;726278bef44516ab7bda7bdddfab4e9255140b2b16e7b6440d9cd54960e0c3ae is the result of the encrypted data in Table 1.

Next, the system decrypts data such as the participant's name for display and verifies its integrity by regenerating a hash from the encrypted data and comparing it to the stored hash. If the hashes match, the certificate is declared valid and its validity status is displayed to the user. Otherwise, a mismatch indicates that the certificate data has been modified since the original hash was generated, as shown in.

After the QR code is scanned, the user is redirected to a URL, where the system extracts the UUID and retrieves the associated certificate data from the database, including the encrypted data and its hash value. If the UUID has been altered, the system displays the message shown. After the QR code is scanned, the user is redirected to a URL, where the system extracts the UUID and retrieves the associated certificate data from the database, including the encrypted data and its hash value. If the UUID has been altered, the system displays the message shown in Figure 9. This functionality, along with other system features, was evaluated through Black Box testing to ensure that each feature and display functioned as intended.

Testing was conducted using a Black Box Testing approach, focusing on input and output functionality without examining the program's internal structure. Equivalence Partitioning techniques were used to classify data sets into valid and invalid input classes to ensure the system handled various types of input appropriately.

$$Test\ Case\ Pass = \left(\frac{Test\ Case\ Passed}{Total\ Test\ Case}\right) x\ 100\% = 100\%$$

With the number of successful test cases being 13 out of a total of 13 scenarios, then:

$$Test\ Case\ Pass = \left(\frac{13}{13}\right) x\ 100\% = 100\%$$

These results indicate that the web-based TOEFL electronic certificate system has met good functionality standards with a system success rate of 100%, indicating that the system is in a stable condition and ready for use by users.

CONCLUSION

From the design and implementation of the TOEFL Electronic Certificate Creation Web Application with QR Code Technology for Verification, the developed system successfully provides the main features in the form of participant registration forms, score input by admins, digital certificate creation, automatic email sending, and certificate verification via QR Code. This system has integrated the AES-256 algorithm to maintain the confidentiality of personal data and the SHA-256 algorithm to ensure data integrity. Testing using the Black Box method with the Equivalence Partitioning technique in 13 scenarios shows that all features function as designed with a 100% success rate. Direct validation by the CEdEC admin of Global University Jakarta as the end user also confirms that the system is easy to use, meets operational needs, and improves the efficiency and security of the certificate creation and verification process.

REFERENCES

Baltrusaitis, T., Ahuja, C., & Morency, L. P. (2019). Multimodal machine learning: A survey and taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(2), 423–443. https://doi.org/10.1109/TPAMI.2018.2798607

Dehimi, N. E. H., & Tolba, Z. (2024). Attention mechanisms in deep learning: Towards explainable artificial intelligence. *Proceedings of the International Conference on Pattern Analysis and Intelligent Systems*, 1–7. https://doi.org/10.1109/PAIS62026.2024.00006

Ghaffarian, S., Valente, J., Van Der Voort, M., & Tekinerdogan, B. (2021). Effect of attention mechanism in deep learning-based remote sensing image processing: A systematic literature review. *Remote Sensing*, 13(15), 2965. https://doi.org/10.3390/rs13152965

Ghaleb, E., Niehues, J., & Asteriadis, S. (2023). Joint modelling of audio-visual cues using attention mechanisms for emotion recognition. *Multimedia Tools and Applications*, 82(8), 11239–11264. https://doi.org/10.1007/s11042-022-13557-w

Hassanin, M., Anwar, S., Radwan, I., Khan, F. S., & Mian, A. (2024). Visual attention methods in deep learning: An in-depth survey. *Information Fusion*, 108, 102417. https://doi.org/10.1016/j.inffus.2024.102417

I. Gunawan, "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force," *TECHSI - Jurnal Teknik Informatika*, vol. 13, no. 1, p. 14, Apr. 2021, doi: 10.29103/techsi.v13i1.2395.

Kibria, M. R., Lafond, S., & Arslan, J. (2025). Decoding the multimodal maze: A systematic review on the adoption of explainability in multimodal attention-based models. *arXiv preprint*. https://doi.org/10.48550/arXiv.2508.04427

Mardiansyah, "Black Box Testing with Equivalence Partitioning and Boundary Value Analysis Methods (Study Case: Academic Information System of Mataram University)," in *Proceedings of the First Mandalika International Multi-Conference on Science and Engineering 2022, MIMSE 2022 (Informatics and Computer Science)*, Atlantis Press International BV, 2022, pp. 207–219. doi: 10.2991/978-94-6463-084-8_19.

Mocanu, B., Tapu, R., & Zaharia, T. (2023). Multimodal emotion recognition using cross-modal audio-video fusion with attention and deep metric learning. *Image and Vision Computing*, 133, 104624. https://doi.org/10.1016/j.imavis.2023.104624

Moorthy, S., & Moon, Y. K. (2025). Hybrid multi-attention network for audio–visual emotion recognition through multimodal feature fusion. *Mathematics*, 13(7), 1100. https://doi.org/10.3390/math13071100

Nagrani, A., Yang, S., Arnab, A., Jansen, A., Schmid, C., & Sun, C. (2021). Attention bottlenecks for multimodal fusion. *Advances in Neural Information Processing Systems*, 34, 14200–14213.

Niu, Z., Zhong, G., & Yu, H. (2021). A review on the attention mechanism of deep learning. *Neurocomputing*, 452, 48–62. https://doi.org/10.1016/j.neucom.2021.03.091

Parcalabescu, L., & Frank, A. (2023). MM-SHAP: A performance-agnostic metric for measuring multimodal contributions in vision and language models. *Proceedings of the ACL*, 4032–4059. https://doi.org/10.18653/v1/2023.acl-long.220

Pressman, R. S., & Maxim, B. R. (2021). *Software Engineering: A Practitioner's Approach* (9th ed.). McGraw-Hill.

Sommerville, I. (2022). *Software Engineering* (11th ed.). Pearson.

R. Khair, "Application of Rapid Application Development (RAD) in the E-Career System: A Startup Approach," *The Indonesian Journal of*

Computer Science, vol. 13, no. 6, Dec. 2024, doi: 10.33022/ijcs.v13i6.4450

Vamsidhar, D., Desai, P., Shahade, A. K., Patil, S., & Deshmukh, P. V. (2025). Hierarchical cross-modal attention and dual audio pathways for enhanced multimodal sentiment analysis. *Scientific Reports*, 15(1), 25440. https://doi.org/10.1038/s41598-025-25440-0

Zhao, F., Zhang, C., & Geng, B. (2024). Deep multimodal data fusion. *ACM Computing Surveys*, 56(9), 1–36. https://doi.org/10.1145/3631234