Proceedings ASTRAtech International Conference
Vol. 1 October 2024, 75-82
https://doi.org/10.52453/aic.v1i0ctober.460

Certificate digitalization for information security in verification

Eko Abdul Goffar*, Riesta Pinky Nurul Arifah

Informatic Management Department, Politeknik Atra, Jakarta, Indonesia

* Corresponding author: eko.gofar@polytechnic.astra.ac.id

Abstract

The rapid advancement of technology has made information access more convenient, but this ease is often misused for fraudulent purposes, such as manipulating TOEFL certificates, graduation certificates, and other important documents. These forgeries are challenging to detect, raising doubts about the validity and authenticity of such documents. To address this issue, this paper aims to ensure the authenticity and validity of certificates by developing an e-certificate system integrated with a QR Code-based verification mechanism. This approach minimizes the risk of forgery and strengthens trust in document verification processes. The system is built using the System Development Life Cycle (SDLC) approach with the Extreme Programming methodology. This includes stages of planning, where a detailed activity plan is created; design, where the Physical Data Model (PDM) and user interfaces are developed; and implementation, where the designs are transformed into a functional program. These stages are iterated continuously to ensure the system meets user needs. The proposed system features an admin module for managing activities, creating certificates, and handling user data. Participants, on the other hand, can validate certificates by scanning QR Codes and downloading their verified certificates. By integrating these functionalities, the e-certificate system offers a reliable solution to verify document authenticity and protect the integrity of the information contained within. This innovation is expected to significantly reduce forgery incidents and enhance the security of important documents in various applications.

Keywords: extreme programming, e-certificate, qr code, system development life cycle

1. Introduction

In the era of modernization marked by the advancement of information technology, the development of information systems has reached an extraordinarily rapid level. Digital transformation has created various tools and applications that function to facilitate human activities in various fields, from education to business. Optimal utilization of information technology has the potential to provide significant benefits, including time efficiency, data accuracy, and ease of access. However, if this technology is used without proper consideration, negative impacts can arise. One of the serious problems related to the use of information technology is the high rate of plagiarism and falsification of information. This poses a complex challenge, especially in assessing the authenticity of information and official documents. Certificates, as one form of important document in the world of education and professionals, are often the target of forgery. Common examples include graduation certificates, language test certificates such as TOEFL, and various other certificates issued by official institutions. Forgery

of certificates not only harms the individuals involved but can also disrupt the integrity of the education system and public trust in the institutions that issue these documents. In this context, the need for an effective verification mechanism is very urgent to prevent increasingly widespread misuse practices.

The digitalization of certificates has been widely recognized in academic research as a significant enhancement to information security within verification processes, addressing issues related to forgery and data integrity. Previous studies have demonstrated that the transition to e-certificates provides substantial security improvements, with each e-certificate being uniquely designed to prevent duplication or tampering, ensuring document authenticity throughout its lifecycle (Artha et al., 2022). This approach effectively protects certificates from unauthorized modifications, thereby preserving their reliability as verifiable documents. Furthermore, (Verma & Sharma, 2022) has emphasized that systems allowing institutions to dynamically generate various types of certificates, tailored to their needs, contribute to operational efficiency and reduce the workload associated with certificate design. By offering built-in templates for different certificate types such as participation, awards, or attendance, these systems automate the certificate issuance process, enabling certificates to be sent directly to participants via email while also generating delivery reports for tracking purposes. (Imbar et al., 2021) highlighted that the integration of smart attendance systems using RFID technology significantly enhances the efficiency of tracking student attendance in campus activities, while simultaneously ensuring the authenticity of the certificates issued. In addition, the use of digital signatures based on QR Code technology has been identified as a secure method for certificate verification. Recent studies have also explored the application of blockchain technology in digital certificate systems, which provides a robust solution to academic certificate forgery. By securely recording certificates in a transparent and immutable manner on the blockchain, the risk of unauthorized alterations is minimized, thereby enhancing the credibility of academic credentials (MONDAL et al., 2023). Further research into the security and privacy challenges associated with sixth generation (6G) mobile networks underscore the critical need for robust security frameworks to address vulnerabilities in increasingly hyper-connected environments (Nguyen et al., 2021). The implementation of effective verification mechanisms has been deemed essential to maintaining the integrity of official documents, particularly considering rising privacy concerns and the growing impact of regulatory frameworks on digital technologies (Quach et al., 2022). Given the escalating incidences of cybercrime and data breaches, the need for robust security frameworks and regulatory measures to protect sensitive information has been widely acknowledged in the literature, ensuring that users can engage with digital services securely (Indah et al., 2022; Kesuma et al., 2021). Collectively, the body of research supports the view that advancing certificate digitalization presents a comprehensive strategy for safeguarding information security in verification processes while reinforcing institutional trust (Pawar et al., 2022). The findings and strategies discussed in previous research emphasize the importance of utilizing advanced technologies to enhance the security and efficiency of certificate management systems. As digital transformation progresses across various sectors, the design and implementation of secure digital systems, including certificate issuance platforms, require thorough analysis and robust frameworks. In the forthcoming research, the system analysis and design process will follow the methodology of creating diagrams based on Unified Modeling Language (UML), referencing the fifth edition of System Analysis and Design by Alan Dennis, Barbara Haley Wixom, and Roberta M. Roth. This book provides a comprehensive guide to systematically mapping system diagrams, which will serve as the foundation for designing an effective digital verification system (Dennis et al., 2012).

Along with the development of technology, innovative solutions such as the use of QR Codes for information verification are starting to be widely considered. QR Code, which stands for Quick Response Code, is a type of matrix code that can store information in a format that is easy to read by digital devices, such as smartphones. By including a QR Code on a certificate, the owner and

third parties have easy access to check the authenticity of the certificate. When the QR Code is scanned, the system can be directed to a database containing related information, allowing for real-time verification.

This paper aims to explain the steps in building a system that utilizes QR Codes to improve information security on certificates. In this discussion, the system design, implementation methods, and potential benefits that can be generated from the application of this technology will be discussed. In addition, this discussion will also touch on challenges that may be faced in the implementation process, such as data privacy issues and information system security. With the implementation of a QR Code-based verification system, it is expected to reduce counterfeiting practices and increase transparency in certificate management. This system not only provides technical solutions but is also expected to restore public trust in the authenticity of documents issued by educational institutions and professional organizations.

Through this paper, the author aims to contribute significantly to the understanding of certificate digitalization and the critical role of technological innovation in ensuring the integrity and authenticity of information. By addressing the challenges of document forgery and enhancing verification processes, this research emphasizes the transformative potential of digital solutions in safeguarding data security. In a broader context, the implementation of QR Code-based verification systems is envisioned as a pivotal step towards achieving a more secure, transparent, and efficient digital transformation across various sectors.

2. Methodology

The methodology that will be used here is to build the System Development Life Cycle (SDLC) with the extreme programming methodology. The stages can be seen in Figure 1.

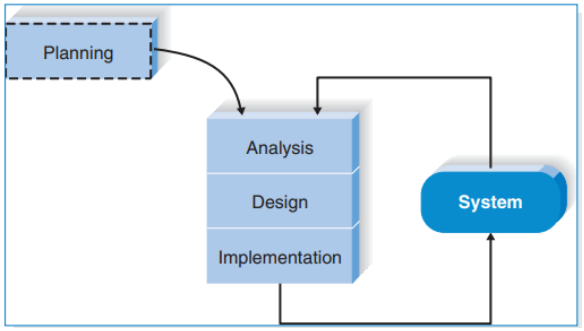

Figure 1. Extreme programming phases

a. Planning

At this stage, the researcher creates activities in the process of building an e-certificate system. The process carried out includes analyzing conditions, creating designs, building systems, and conducting testing. The activities carried out for 3 months can be seen in Table 1.

Table 1. Planning activities

No	Activity	Jul-24				Aug-24				Sep-24			
		1	2	3	4	1	2	3	4	1	2	3	4
1	Condition Analysis												
2	Task Division												
3	Creating Access Roles												
4	Building Design (Database & User Interface)												
5	Building System												
6	Testing												
7	Evaluation												

In the table above, it can be seen that the activity plan is carried out starting from conducting analysis to conducting evaluation of the system to be built. Based on the table, it can also be seen that the process of designing and building the system always goes hand in hand with system testing according to the extreme programming method used.

b. Analysis

At the analysis stage in system development, it is important to determine the division of access roles to be implemented. This division is directly related to the needs of system development, so that each user can have access and responsibilities according to their function. In this context, there are two types of access roles identified, namely admin and participant.

The admin role has the primary responsibility for managing certificates in the system. This task includes various activities, such as adding, editing, and deleting certificates, as well as ensuring that all data related to the certificate is accurate and up to date. The admin is also tasked with overseeing the verification process and ensuring that the system is functioning properly.

On the other hand, the participant role has a more limited but still crucial function. Participants can download certificates that have been issued and also verify the authenticity of the certificate. In other words, participants have access to ensure that the certificates they receive are valid and recognized by the relevant parties. With this clear division of roles, it is hoped that each user can contribute according to their responsibilities, as well as increase efficiency and security in certificate management. The following can be seen in Table 2.

Table 2. Admin and participant features in the QR code-based e-certificate system

Role	Feature	Description
Admin	Manage Activities	Admin can plan and manage activities related to certificate issuance.
	Create Certificates	Admin has the capability to create electronic certificates.
	Manage User Information	Admin can add, update, or delete user data registered in the system.
Participant	Validate Certificates with QR Code	Participants can validate the authenticity of certificates by scanning the QR Code provided.
	Download Certificates	Participants can download verified certificates through the system.
	Feature	Description

c. Design

At this stage, the main focus is on creating a system design, which includes two important aspects: the database and the user interface. This design is based on the results of the previous analysis, which has determined the division of access between two main roles, namely admin and participant.

The database design serves to determine the data storage structure required in the system. This includes selecting data types, setting relationships between tables, and storing certificate and user information. Meanwhile, the user interface design focuses on how users will interact with the system. The interface designed must be intuitive and user-friendly, so that both admin and participants can easily access the functions they need.

The results of this design process are very important, because they will be a guide for the next implementation stage. In the implementation stage, the design that has been made will be realized into an operational system, so that all planned features can be implemented effectively. Thus, the design stage becomes a crucial foundation for the success of the overall system development. The following can be seen in Figure 2.

Figure 2. Rich picture of the system

d. Implementation

Based on the design that has been made, the next stage is the development of an e-certificate system that will function according to the main roles that have been determined, namely admin and participants. The development process of this system is not linear, but rather iterative, where each step will be carried out repeatedly. This aims to ensure that the system developed can meet all previously identified needs. The role of the admin in this system allows them to manage certificates more effectively, while participants have access to obtain certificates and verify them. One important feature of this system is the ability to verify certificate data through QR Code technology. By using QR Code, users can scan to check the authenticity of the certificate quickly and efficiently. This development process will continue until the resulting e-certificate system functions according to the expectations and needs that have been determined. Thus, the success of the system will depend on the extent to which each element of the system can be integrated and operate well, providing an optimal experience for all users. The following can be seen in Figure 3.

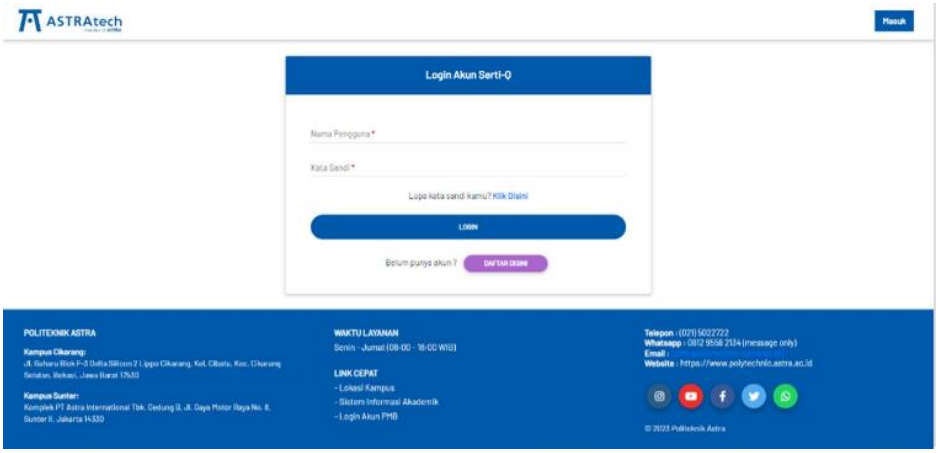

Figure 3. Implementation of the QR code-based e-certificate verification system

3. Results and Discussion

Based on the results of the analysis and design that has been built, there are several results from the development process. The first result is the database design in the form of a Physical Data Model (PDM). The following can be seen in Figure 4.

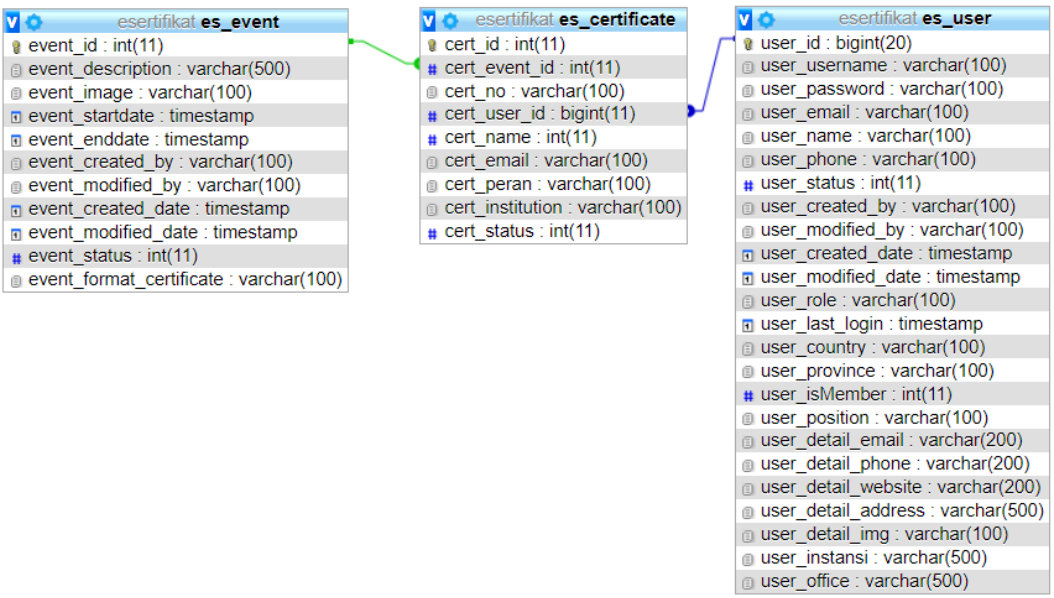

Figure 4. Physical data model

From the image above, es_event is used to store information about activities that can be used to differentiate the certificate from the activity. Then there is es_user which is used to store user information including admin and participants. The table can also be used to store user profile information. Furthermore, es_certificate is used to store certificate information according to the participant's name and the related activity. The certificate will work by storing a signed certificate template as a master certificate for one activity. The master certificate will be used for the activity for all related participants and the certificate will be automatically generated including the certificate number and QR Code in it which will be scanned and the information verified. The second result of this research is the design or prototype result of the user interface of the certificate digitalization. The following can be seen in Figure 5.

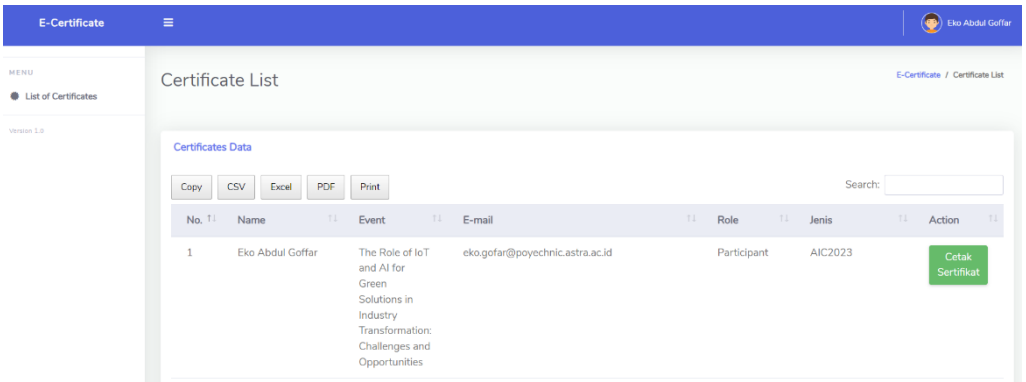

Figure 5. Certificate list

The image above shows the certificate page on the participant side. So that participants can see the list of certificates obtained in all events attended at the Astra Polytechnic by using their account to access the e-certificate system. The following can be seen in Figure 6.

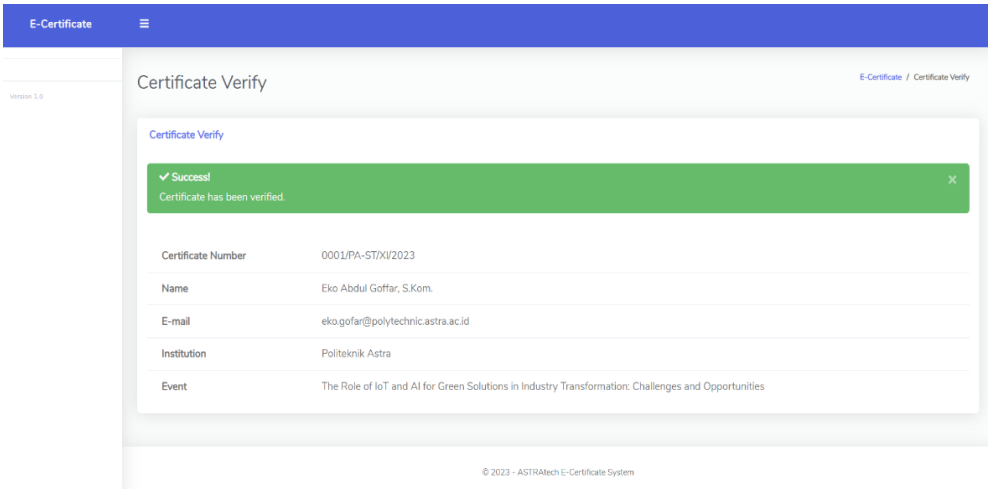

Figure 6. Certificate verify

The image above shows the result of moving the QR Code on the certificate and displays evidence that the certificate has been verified by the e-certificate system. With this, the document can be declared valid because it has been verified. The verification process is expected to be a solution to improve information security sin the validity of certificates in various activities.

4. Conclusion

Certificate verification through QR Code scanning offers a practical and efficient solution for ensuring the authenticity of certificates while verifying whether they are issued by authorized institutions. This technology simplifies the verification process, making it faster and reducing the risk of confusion or misunderstandings regarding document validity. By leveraging QR Code-based verification, the system aims to address the pressing issue of certificate forgery, thereby enhancing trust in the integrity of official documents.

The primary objective of this paper is to propose an effective solution to minimize plagiarism and document falsification. The implementation of this technology not only empowers users to confidently verify the certificates they receive but also strengthens the credibility of the institutions that issue these documents. This advancement is expected to foster a more transparent and accountable environment, contributing to reducing the negative impact of certificate forgery across various sectors.

Since the proposed application has not yet been implemented, future research will focus on the detailed design and development of the system. Key steps include creating comprehensive system architecture, implementing robust security measures to protect certificate data, and conducting usability testing to ensure the system meets user needs. Additionally, further exploration of complementary technologies, such as blockchain for added security and scalability, will be considered. By addressing these next steps, this research aims to move closer to realizing a reliable and impactful solution for digital certificate verification.

References

Artha, K. A. R., Zain, S. N., Alkautsar, A. A., & Widianto, M. H. (2022). Implementation of Smart Contracts for E-Certificate as Non-Fungible Token using Solana Network. 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), 1-6. https://doi.org/10.1109/ICITDA55840.2022.9971423

Dennis, A., Wixom, B., & Roth, R. (2012). System Analysis and Design, Fifth Edition. John Wiley & Sons. https://books.google.co.id/books?id=zCRQzQEACAAJ

Imbar, R. V, Sutedja, B. R., & Christianti, M. (2021). Smart Attendance Recording System using RFID and e-Certificate using QR Code-based Digital Signature. 2021 International Conference on ICT for Smart Society (ICISS), 1–5. https://doi.org/10.1109/ICISS53185.2021.9533199

Indah, F., Sidabutar, A., & Annisa, N. (2022). Jurnal Bidang Penelitian Informatika Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). Jurnal Bidang Penelitian Informatika, 1(1), 1–8. https://ejournal.kreatifcemerlang.id/index.php/jbpi

Kesuma, A. A. N. D. H., Budiartha, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik. Jurnal Preferensi Hukum, 2(2), 411–416. https://doi.org/10.22225/jph.2.2.3350.411-416

MONDAL, S., PANJA, A., & KARFORMA, S. (2023). An Efficient E-Certificate Management System in E-Learning Using Blockchain. Science and Culture, 89(March-April), 120–124. https://doi.org/10.36094/sc.v89.2023.an_efficient_e-certificate_management_system.mondal.120

Nguyen, V.-L., Lin, P.-C., Cheng, B.-C., Hwang, R.-H., & Lin, Y.-D. (2021). Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. IEEE Communications Surveys & Tutorials, 23(4), 2384–2428. https://doi.org/10.1109/COMST.2021.3108618

Pawar, M. K., Patil, P., Sawhney, R., Gumathanavar, P., Hegde, S., & Maremmagol, K. (2022). Performance Analysis of E-Certificate Generation and Verification using Blockchain and IPFS. 2022 International Conference on Inventive Computation Technologies (ICICT), 345–350. https://doi.org/10.1109/ICICT54344.2022.9850830

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Verma, A., & Sharma, B. (2022). Dynamic E-Certificate Designing with Automatic Mailing System using Python and SQLite3. Journal of Applied Information Science, 10(2), 26–30. https://ssrn.com/abstract=4249245