Design and Development of a One-Time-Use Dynamic QR Code System with an Anti-Screenshot Mechanism in a Web-Based Event Guest Book Application to Enhance Attendance Verification Security

Gatut Yulisusianto[1)], Febrianto Yoga Ari Sandy[2)], Yohanes Dwi Cahyono[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: mr.gatut@gmail.com[1)], ankumuhammad1@gmail.com[2)],
indorana2012@gmail.com[3)]

Design and Development of a One-Time-Use Dynamic QR Code System with an Anti-Screenshot Mechanism in a Web-Based Event Guest Book Application to Enhance Attendance Verification Security

Abstract: *The increasing use of QR codes in daily life has created opportunities for cyber threats, such as the insertion of malicious URLs that are difficult for average users to recognize. This research aims to qualitatively analyze best practices in URL security detection extracted from QR codes, particularly focusing on artificial intelligence (AI) approaches and the integration of digital audit systems. A systematic literature review method was applied, drawing from internationally indexed publications and thematic observations about user behavior and threat detection technologies for phishing and malware. Findings indicate that AI-based detection systems effectively identify security threats earlier and more accurately, especially when combined with user education features and activity logging through the Wazuh/ELK Stack. However, human error due to limited digital security literacy remains a major challenge. The study concludes that integrating automated detection technologies, user education, and digital auditing is crucial to mitigating cyberattacks via QR codes. Development of adaptable tools for emerging threat patterns and behavior-based user education strategies are recommended to enhance the national cybersecurity ecosystem.*

Keywords: artificial intelligence, cybersecurity, digital audit, malicious URL, phishing detection, QR code.

Abstrak: *Meningkatnya pemanfaatan QR code dalam kehidupan sehari-hari telah membuka peluang bagi ancaman keamanan siber berupa penyisipan URL berbahaya yang sulit dikenali oleh pengguna awam. Penelitian ini bertujuan menganalisis secara kualitatif praktik-praktik terbaik deteksi keamanan URL hasil ekstraksi QR code, khususnya menggunakan pendekatan kecerdasan buatan (AI) dan integrasi sistem audit digital. Studi ini menggunakan metode telaah literatur sistematis terhadap publikasi internasional terindeks dan hasil observasi tematik terkait perilaku pengguna serta teknologi deteksi ancaman phishing dan malware. Temuan menunjukkan bahwa sistem deteksi berbasis AI terbukti*

mampu mengidentifikasi ancaman secara lebih dini dan akurat, terutama ketika dipadukan dengan fitur edukasi pengguna dan logging aktivitas menggunakan Wazuh/ELK Stack. Meskipun demikian, human-error akibat kurangnya literasi keamanan digital masih menjadi tantangan utama. Kesimpulan yang diperoleh menegaskan pentingnya integrasi teknologi deteksi otomatis, edukasi pengguna, dan audit digital untuk mengurangi risiko serangan siber melalui QR code. Disarankan pengembangan alat yang adaptif terhadap pola serangan terbaru serta pendekatan edukatif berbasis perilaku pengguna untuk memperkuat ekosistem keamanan siber nasional.

Kata kunci: audit digital, deteksi phishing, keamanan siber, kecerdasan buatan, QR code, URL berbahaya.

INTRODUCTION

The rapid advancement of information and communication technology (ICT) over the last two decades has fundamentally reshaped administrative processes and data governance across diverse institutional domains, including governmental, defense, and other strategic organizations. Digital transformation has evolved from a supplementary initiative into a core strategic imperative aimed at improving operational efficiency, data accuracy, traceability, and information security. Administrative subsystems that were traditionally manual are now being reengineered into integrated digital platforms capable of supporting real-time data processing and secure information exchange. One notable example of this transformation is the migration from paper-based guest registration systems to web-based digital guest book applications. Conventional manual guest books are inherently vulnerable to data loss, transcription errors, identity falsification, and inefficiencies in archival retrieval. In high-security environments, such as military installations or state strategic facilities visitor registration is not merely clerical documentation but an essential component of layered access control and institutional security monitoring. Consequently, a secure, technology-driven guest book system that balances procedural efficiency with robust authentication and verification mechanisms has become indispensable. QR Code technology presents a practical digital authentication medium due to its high data capacity, rapid encoding-decoding capability, and compatibility with widely available electronic devices (Prananingrum et al., 2025).

Despite the increasing adoption of QR Code-based digital guest book systems, prevailing implementations often demonstrate critical vulnerabilities in their security architecture. A significant proportion of existing systems rely on static QR Codes or reusable codes that lack temporal constraints and automatic invalidation features. Such configurations introduce exploitable weaknesses, including the possibility of unauthorized screenshot capture, redistribution of valid codes to unintended parties, and repeated use of codes intended for single-entry access. Moreover, many systems do not implement time-based validation protocols or dynamically generated authentication tokens that periodically expire. Prior studies have predominantly emphasized usability optimization and administrative simplification while giving limited attention to countermeasures against digital duplication, replay attacks, and access manipulation strategies. This imbalance highlights a clear research gap in the design of guest book systems that integrate efficiency with advanced digital security safeguards capable of mitigating

screenshot-based exploitation and code reuse vulnerabilities (Ramadhan et al., 2025).

Addressing this gap, the present study proposes the design and development of a dynamic QR Code-based digital guest book system incorporating multilayered security mechanisms. Unlike static implementations, the proposed system generates encrypted, time-bound dynamic QR Codes derived from unique system-generated tokens. Each QR Code is explicitly associated with visitor identity data, scheduled visit parameters, and validation status stored within a centralized relational database. The system enforces a strict one-time-use protocol, ensuring that every issued QR Code becomes automatically invalid following a successful check-in transaction. This mechanism prevents replay attacks and eliminates the risk of multiple unauthorized entries using duplicated codes. In addition, the architecture integrates anti-screenshot protection features, including controlled interface rendering, browser activity monitoring, and periodic token regeneration within defined temporal intervals. These measures collectively strengthen digital access governance by reducing the feasibility of screen capture exploitation and unauthorized redistribution. Therefore, the system is conceptualized not solely as a digitized registration tool but as a structured digital access control framework designed to withstand contemporary cyber-manipulation threats (Ningsih & Fatah, 2025).

The research methodology encompasses comprehensive system requirement analysis, web-based application architecture design, relational database modeling, and implementation of a dynamic QR Code generation algorithm utilizing automatically generated unique tokens. Real-time validation is achieved through continuous server synchronization, ensuring that the status of each scanned QR Code is instantaneously updated in the database to prevent reuse. The primary novelty of this research lies in the simultaneous integration of three critical security components, which dynamic QR Code generation, one-time-use validation enforcement, and anti-screenshot protection, within a unified and centralized platform. While these elements may exist independently in various authentication systems, their combined application within a digital guest book framework, particularly in high-security institutional contexts, remains limited. Through this integrated approach, the system functions as both a visitor documentation instrument and an adaptive access control mechanism capable of responding to digital manipulation attempts. The proposed innovation is expected to contribute to the formulation of enhanced security standards for QR Code-based administrative systems in strategic operational environments (Hafizhah et al., 2025).

Based on the identified background issues, research gap, and proposed technological innovation, this study explicitly encapsulates the research emphasis on secure system architecture design, implementation of dynamic and time-bound QR authentication, enforcement of single-use validation protocols, and mitigation of digital misuse risks. Overall, this research aims to develop a web-based event guest book application that strengthens attendance verification security while maintaining operational efficiency and adaptability in the face of evolving digital security threats.

The objective of this study is to design, develop, and evaluate a secure web-based digital guest book system that implements dynamic QR Code authentication with a one-time-use validation mechanism and integrated anti-

screenshot protection. Specifically, the research aims to (1) formulate a secure system architecture capable of generating encrypted, time-limited QR Codes based on unique dynamic tokens; (2) implement real-time server-side validation to ensure automatic code invalidation after a single successful check-in; (3) integrate preventive mechanisms against screenshot-based duplication and unauthorized reuse; and (4) assess the system's effectiveness in enhancing attendance verification security compared to conventional static QR Code implementations. Through these objectives, the study seeks to contribute a technically robust and security-oriented solution adaptable to high-security institutional and event management environments.

RESEARCH METHOD

This research was conducted at the Network Practicum Classroom, Academic Building 2nd Floor, Cyber Security Engineering Study Program, Poltekad Kodiklatad Batu, East Java. The location was selected based on the availability of adequate minimum infrastructure to support the implementation of a web-based one-time-use dynamic QR Code system with an anti-screenshot mechanism. The environment represents a realistic operational setting similar to battalion-level military units, which typically do not possess dedicated information system development laboratories but require secure, practical, and cost-efficient attendance verification solutions for official events. The available infrastructure includes a stable 50 Mbps institutional internet connection, an 8-port managed Gigabit Ethernet switch integrated into the structured cabling system, sufficient electrical facilities to support server and peripheral deployment, and limited administrative access to network configuration through coordination with the institutional IT division for temporary VLAN segmentation during the research period. The study was carried out from November 2025 to July 2026, covering proposal preparation, system development, data collection, testing, documentation, and final evaluation stages.

This study employed a Research and Development (R&D) approach as the primary methodological framework. The R&D method was chosen because the objective of the study is not merely to analyze theoretical constructs but to design, develop, validate, and refine a functional technological product. The process began with a preliminary study and needs analysis to identify weaknesses in conventional manual guest registration systems and static QR Code implementations. Data collection techniques included observation of existing attendance procedures, interviews with event organizers, and literature review related to QR Code authentication, web-based system development, and digital access security models. The results of this stage served as the foundation for defining both functional requirements, such as dynamic token generation, one-time-use validation, and real-time attendance recording and non-functional requirements, including system security, response time, scalability, and usability.

The system development process followed the Waterfall software development methodology due to the clearly defined system requirements and the structured operational environment. The stages consisted of requirements analysis, system design, implementation, testing, deployment, and evaluation. During the design phase, system modeling was conducted using Unified Modeling Language (UML), including Use Case Diagrams to define actor interactions, Sequence Diagrams to illustrate object interaction flows, Activity Diagrams to model operational workflows, and Entity

Relationship Diagrams (ERD) to structure the relational database architecture. The system was implemented using the Laravel framework (PHP-based), MySQL database management system, and frontend technologies including HTML, CSS, and JavaScript. The architecture applied a client–server model in which all validation processes were executed server-side to prevent client-side manipulation.

A dynamic QR Code generation algorithm was implemented using encrypted unique tokens automatically produced by the server. Each token was associated with participant identity, event session, timestamp, and validation status. The system enforced time-based validation, limiting QR Code activity within a specific duration (e.g., 60 seconds), and automatically invalidating tokens after successful scanning under the one-time-use principle. Additional security layers included session binding and device verification mechanisms to prevent screenshot reuse across different devices or outside the permitted time window. In situations where participants were unable to present a valid QR Code due to technical constraints, a structured fallback mechanism was provided, allowing manual identity verification through database search while maintaining audit logs marked as “manual check-in.”

System testing was conducted using both black-box and white-box testing techniques. Black-box testing evaluated functional compliance from the user perspective, ensuring that each feature operated according to specified requirements. White-box testing examined internal logic, code structure, and algorithmic correctness, particularly in token validation and expiration handling. User Acceptance Testing (UAT) was also performed to assess usability and operational feasibility in real event scenarios. Performance metrics included QR scanning response time, database synchronization speed, token invalidation accuracy, and resistance to reuse attempts. Comparative analysis was conducted between the developed system and conventional static QR Code systems to measure improvements in security robustness and operational efficiency.

The overall research process was iterative, allowing revision and refinement whenever system deficiencies were identified during testing and evaluation phases. By integrating development, validation, and comparative security analysis, this methodology ensures that the resulting system is not merely a functional application but a validated security model for attendance verification. The final output of this research is a deployable web-based dynamic QR Code verification system accompanied by empirical performance data and a replicable security framework suitable for strategic institutional environments.

RESEARCH RESULTS

The research resulted in the successful design and implementation of a web-based digital guest book system that utilizes a one-time-use dynamic QR Code authentication mechanism integrated with an anti-screenshot protection feature. The system was developed using the Laravel framework with a MySQL database and implemented within a client–server architecture in which all authentication and validation processes are executed on the server side. The developed application consists of three primary modules: the visitor registration module, the dynamic QR Code generation module, and the attendance verification module. Each module operates in an integrated manner to ensure secure attendance recording and prevent unauthorized access.

The visitor registration module allows participants to register their identity and event participation information through a web interface. The system automatically

generates a unique encrypted token associated with each participant's identity, event session, and timestamp. This token is then encoded into a dynamic QR Code that becomes the participant's digital access credential. The generated QR Code is valid only within a limited time window, typically 60 seconds, and is refreshed periodically to prevent unauthorized duplication or redistribution.

The QR Code verification module is accessed by event administrators through a scanning interface. When a QR Code is scanned, the system immediately sends the token data to the server for validation. The server performs multiple verification steps including token authenticity verification, expiration time validation, identity matching, and verification of whether the code has already been used. If the token is valid and unused, the system records the participant's attendance and automatically invalidates the token to enforce the one-time-use policy.

System testing was conducted through black-box testing, white-box testing, and User Acceptance Testing (UAT). Black-box testing confirmed that all functional components such as QR generation, scanning, token validation, and attendance recording operated correctly according to system specifications. White-box testing verified the correctness of internal logic, particularly within the token generation algorithm and expiration handling procedures. The testing results showed that the average response time for QR Code verification was approximately 0.8 seconds under a stable network environment, indicating efficient server-side processing.

Security testing also demonstrated that attempts to reuse previously scanned QR Codes were automatically rejected by the system. Similarly, QR Codes captured through screenshots became invalid due to the short token expiration time and periodic regeneration mechanism. These results confirm that the implemented security architecture effectively mitigates risks associated with static QR Code systems. Overall, the developed system successfully fulfills the research objective of providing a secure digital attendance verification platform capable of preventing QR Code duplication, replay attacks, and unauthorized access attempts.

DISCUSSION

The results of this study demonstrate that integrating dynamic QR Code authentication with one-time-use validation significantly enhances the security of digital attendance verification systems. Unlike conventional static QR Code implementations, the proposed system generates temporary authentication tokens that are valid only within a short time window. This mechanism effectively prevents common exploitation techniques such as screenshot sharing, code duplication, and repeated access attempts.

The implementation of server-side token validation further strengthens system security. Because all verification processes are performed on the server rather than on the client device, the possibility of local manipulation or tampering with authentication data is greatly reduced. The centralized validation architecture also allows real-time synchronization between the scanning interface and the database, ensuring that once a QR Code is successfully scanned, its token status immediately changes to "used." This mechanism eliminates the possibility of replay attacks.

Another significant contribution of the system is the integration of anti-screenshot protection strategies. Although screenshot prevention cannot be fully guaranteed at the operating system level, the combination of rapid token expiration and periodic QR Code regeneration

significantly reduces the usefulness of captured QR images. Even if a user captures a screenshot of a QR Code, the token will expire before it can be reused. This design effectively addresses one of the major vulnerabilities found in static QR Code-based authentication systems.

The performance evaluation also indicates that the developed system maintains efficient operational performance. With an average response time below one second for QR verification, the system is suitable for real-world event environments where rapid attendee processing is required. This balance between security and efficiency is critical, particularly for large-scale events where long verification delays could disrupt operational flow.

Furthermore, the inclusion of a fallback manual verification mechanism ensures operational continuity in situations where technical constraints occur, such as device malfunction, internet connectivity issues, or damaged QR displays. By allowing administrators to manually verify participant identity through database search while maintaining audit logs, the system maintains both flexibility and accountability.

From a broader perspective, this research contributes to the development of secure digital access control systems that can be applied not only in event management but also in other institutional contexts such as campus access systems, conference management platforms, and restricted facility entry verification. The integration of dynamic authentication, time-based validation, and centralized monitoring provides a scalable security model for modern digital attendance systems.

CONCLUSION

This study successfully designed and developed a secure web-based digital guest book system implementing a one-time-use dynamic QR Code authentication mechanism integrated with an anti-screenshot protection approach. The developed system generates encrypted tokens that are dynamically converted into QR Codes with limited validity periods, ensuring that each code can only be used once for attendance verification.

The implementation of server-side validation, automatic token expiration, and real-time database synchronization effectively prevents common security vulnerabilities associated with static QR Code systems, including duplication, replay attacks, and unauthorized reuse. System testing results confirm that the application operates reliably, with fast verification response times and accurate token invalidation after successful use.

The integration of dynamic QR Code generation with time-based validation and anti-screenshot strategies significantly improves the security of attendance verification processes while maintaining operational efficiency. In addition, the system provides a structured fallback verification mechanism that ensures continuity of attendance recording under technical constraints.

Overall, the proposed system demonstrates that dynamic QR authentication combined with strict one-time-use enforcement can serve as an effective solution for enhancing digital attendance security in event management environments. Future research may focus on expanding the system with biometric verification, multi-factor authentication, and AI-based anomaly detection to further strengthen access control mechanisms in high-security institutional applications.

REFERENCES

Hafizhah, N., Hidayat, A. T., & Wijayanti, Y. (2025). Optimalisasi Pengembangan Sistem Presensi Karyawan Menggunakan Extreme Programming dan Teknologi QR Code. *Jurnal Janitra Informatika Dan*

Sistem Informasi, *5*(1), 1–13.

Ningsih, R. A., & Fatah, Z. (2025). Perancangan Sistem Informasi Buku Tamu Berbasis Tamu Berbasis Website Dengan Notifikasi Whatsapp di Kantor Bawaslu Situbondo. *Jurnal Mahasiswa Teknik Informatika*, *4*(2), 162–167.

Prananingrum, L., Wahab, S. R., Supriyanto, B. F., Jarudin, J., Ardiansyah, M., Wihardjo, E., Yuningsih, N., Ridwan, A., & Yusriadin, Y. (2025). *Pengantar Teknologi Informasi dan Komunikasi*. Yayasan Tri Edukasi Ilmiah.

Ramadhan, R. S., Wirdani, R. R., Delpina, H., & Nelwati, S. (2025). Pendidikan Di Era Teknologi Informasi Dan Komunikasi. *Jurnal Media Akademik (JMA)*, *3*(1).