https://doi.org/10.32815/jitika.1233

Volume 20, Issue 2, 2026

Jurnal Ilmiah Teknologi Informasi Asia

Journal Homepage: https://jurnal.asia.ac.id/index.php/jitika

Article

Implementation of role-based access control (RBAC) in a web-based mosque information system

Nurul Asrofi, Kasmawi *, Pretti Ristra

Information System Security, Department of Computer Science, Politeknik Negeri Bengkalis, 28711, Indonesia

***Abstract*—This study addresses the challenges of mosque administrative and financial management, which are still predominantly handled manually, resulting in inefficiency, limited transparency, and potential security risks. To address these issues, this research designs and implements a web-based mosque information system incorporating Role-Based Access Control (RBAC) to regulate user access based on predefined organizational roles. The system supports the management of mosque activities, financial transactions, announcements, and public information services. RBAC is applied to ensure that each user can only access system functionalities relevant to their responsibilities, including administrators, mosque management staff, treasurers, and public users. System evaluation includes functional testing, role-based access testing, a basic security assessment, and an initial performance evaluation using page-load time measurements. The performance evaluation shows that the most resource-intensive module achieves an average page load time of approximately 2.3 seconds, indicating acceptable performance for a small-scale community-based information system. The results suggest that the proposed system supports structured administrative workflows, improves access organization, and enhances transparency while maintaining controlled access to sensitive information. The proposed system provides a practical foundation for secure and accountable digital mosque management.**

***Keywords*—access management; data security; mosque information system; role-based access control; web application.**

1. Introduction

In the contemporary digital era, information technology has become a strategic instrument for enhancing efficiency, transparency, and accountability across various organizational sectors, including religious institutions such as mosques. Digital transformation enables structured data management, accurate reporting, and real-time information dissemination, which are essential for strengthening governance and maintaining public trust (Aspizain, 2025; Budhy et al., 2021). By adopting web-based information systems, mosques can modernize their administrative processes and align traditional religious management practices with the demands of modern information systems.

Mosques serve not only as places of worship but also as centers for social, educational, and community-oriented activities. These multifaceted roles require effective management of schedules, announcements, donations, and financial records. However, many mosques continue to rely on manual administrative methods or non-integrated tools, resulting in inefficiencies, data inconsistencies, delayed reporting, and limited access to historical information (Rahmawati, 2024; Sutrisno et al., 2022).

* Corresponding author.
E-mail Address: *kasmawi@polbeng.ac.id* (Kasmawi)

Author E-mail(s): NA (as21rofi@gmail.com), K (kasmawi@polbeng.ac.id), PR (prettirista@polbeng.ac.id)
Digital Object Identifier 10.32815/jitika.1233
Manuscript submitted 20 December 2025; revised 18 Januari 2026; accepted 20 Januari 2026.
ISSN: 2580-8397(O), 0852-730X(P).

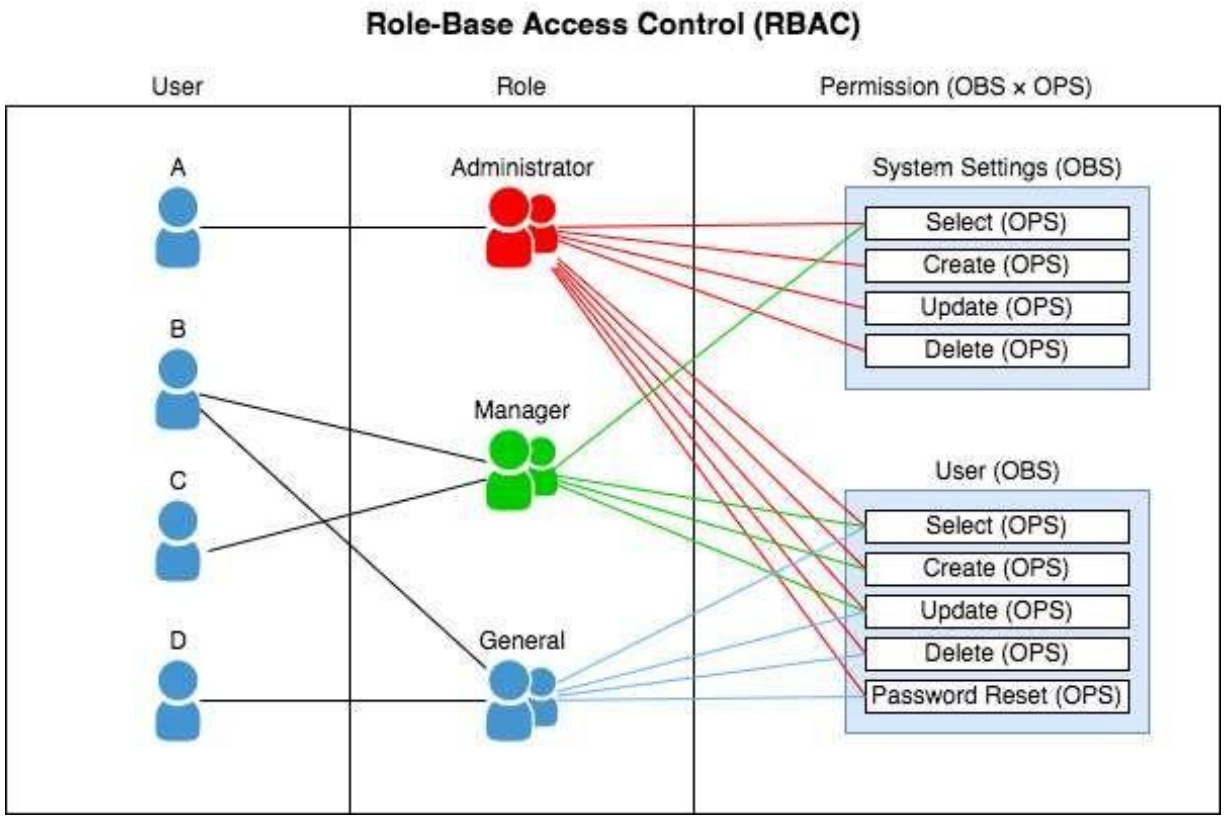

Fig. 1. Role-Based Access Control (RBAC) Conceptual Design

Such conditions hinder operational performance and reduce the effectiveness of mosque management in serving congregational needs.

Transparency in financial management is a fundamental principle for sustaining public trust in religious institutions. Conventional reporting methods, such as periodic announcements or static bulletin boards, are insufficient to provide real-time financial visibility and may lead to misunderstandings among congregants and donors (Rizki & Ekawati, 2023). Previous studies indicate that web-based financial and administrative systems significantly improve transparency and service delivery by enabling continuous access to financial reports and activity information (Haryono & Sujarwo, 2023; Kirom et al., 2024). Consequently, digital platforms have emerged as viable solutions for enhancing openness and accountability in mosque governance.

Beyond efficiency and transparency, information security has become a critical concern in the implementation of digital systems. Systems that lack structured access control mechanisms are vulnerable to unauthorized access, data manipulation, and misuse of sensitive information. In broader organizational contexts, Identity and Access Management (IAM) frameworks play a crucial role in protecting digital assets through authentication, authorization, and user lifecycle management (Premsai, 2024a; Vitla, 2023). Robust access management not only mitigates security risks but also supports regulatory compliance and operational effectiveness (Grandhi, 2025; Kaleru, 2025b).

Role-Based Access Control (RBAC) represents a widely adopted authorization model within IAM frameworks, in which system access is granted based on predefined user roles and responsibilities. RBAC ensures that users can only access functionalities relevant to their duties, thereby minimizing privilege escalation and reducing the risk of data breaches (Rosidin et al., 2025). In community-based systems such as mosque information platforms, RBAC provides a practical approach to balancing transparency with data protection, ensuring that sensitive financial and administrative information remains secure while still accessible to authorized stakeholders.

Several prior studies have examined the implementation of web-based mosque information systems to improve administrative efficiency and transparency. (Siregar et al., 2023) demonstrated that digital mosque management systems can streamline financial and activity management processes, although security and access control were not the primary focus. Similarly, (Ardian et al., 2024) found that digital financial systems enhance transparency but still face challenges related to authorization and access governance. These findings suggest that while digitalization offers substantial benefits, inadequate access control remains a critical limitation that must be addressed.

Furthermore, poorly managed or unrestricted access to digital systems poses ethical and security risks, including data misuse, privacy violations, and erosion of stakeholder trust (Mutambik et al., 2023; Piasecki et al., 2021). Studies on open access and digital governance emphasize the importance of balancing openness with controlled access through clear policies and secure infrastructures (Alsamaualy et al., 2024; Ross-Hellauer et al., 2022). In the context of mosque

Table 1. Comparison of Access Control Models

Model	Access Control Basis	Advantages	Limitations	Suitability for Mosque Information System
ACL	User-specific permissions	Simple for small systems	Poor scalability, difficult maintenance	Low
ABAC	Attributes and policies	Highly flexible and dynamic	High complexity and policy overhead	Medium
RBAC	Organizational roles	Scalable, manageable, role-oriented	Limited flexibility for dynamic roles	High

information systems, unrestricted access may compromise sensitive financial and personal data, underscoring the need for structured access controls.

Based on these considerations, this study aims to design and implement a web-based mosque information system

incorporating Role-Based Access Control (RBAC). The proposed system aims to support administrative processes through structured access management, enhance transparency in financial reporting, and improve data security by regulating user access based on clearly defined roles. This research contributes to the development of secure, accountable, and sustainable digital management practices for mosque administration, aligning religious institutional governance with contemporary information security principles.

2. Methods

2.1. Role-based access control (RBAC) implementation

Role-Based Access Control (RBAC) is implemented as the system's core access control mechanism. RBAC manages user permissions based on predefined roles, ensuring that users can only access system functions relevant to their responsibilities. This approach reduces the risk of unauthorized access and mitigates potential insider threats by enforcing the principle of least privilege (Marquis, 2024).

In this system, users are classified into administrator, mosque management staff, treasurer, and public users. Each role is associated with specific permissions that define allowable actions within the system. Administrators manage user accounts and roles; mosque management staff handle activity-related data; treasurers manage financial transactions and reports; while public users are restricted to viewing published information only.

In access control design, several authorization models can be considered, including Access Control Lists (ACL), Attribute-Based Access Control (ABAC), and Role-Based Access Control (RBAC). ACL assigns permissions directly to individual users, which can become difficult to manage as the number of users and system resources increases (Vitla, 2023).

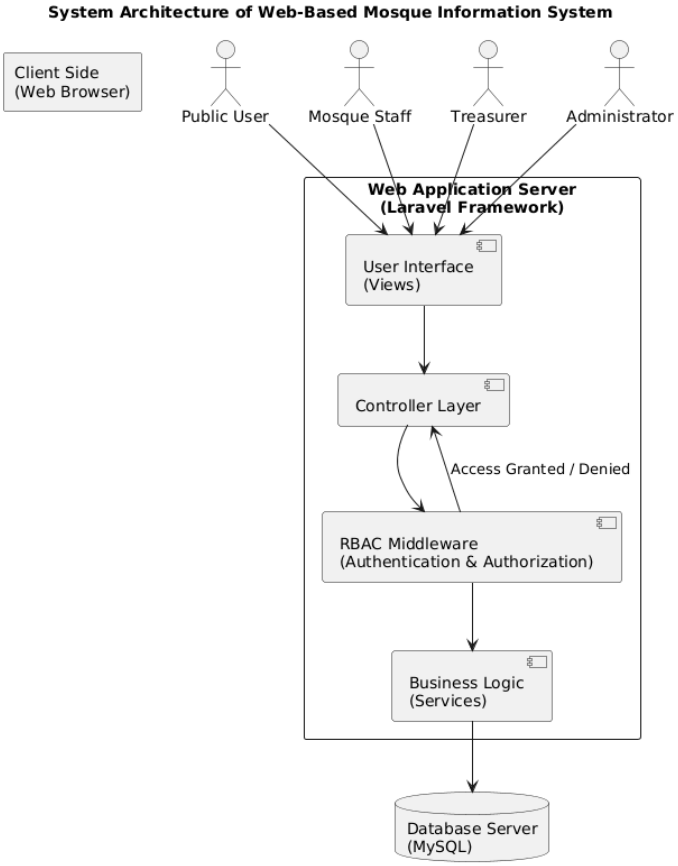

Fig 2. System Architecture of the Web-Based Mosque Information System

ABAC offers higher flexibility by evaluating multiple user and environmental attributes; however, it introduces greater policy complexity and administrative overhead, particularly for small and medium-sized organizations (Kaleru, 2025). RBAC, on the other hand, groups permissions according to organizational roles, simplifying access management and reducing administrative effort (Marquis, 2024).

In community-based organizations such as mosques, organizational structures are typically role-based, with clearly defined roles for administrators, treasurers, and management staff. Therefore, RBAC aligns well with these organizational characteristics while maintaining manageable system complexity and effective authorization enforcement.

Based on the comparison, RBAC provides the most appropriate balance between security enforcement, administrative manageability, and organizational alignment for mosque information systems. While ABAC offers greater flexibility, its complexity is less suitable for small-scale community-based organizations. ACL, although simple, lacks scalability and structured access management. Therefore, RBAC was selected as the most suitable access control model for this study.

2.2. Framework and system implementation

a. The system was implemented using the Laravel PHP framework, which follows the Model–View–Controller

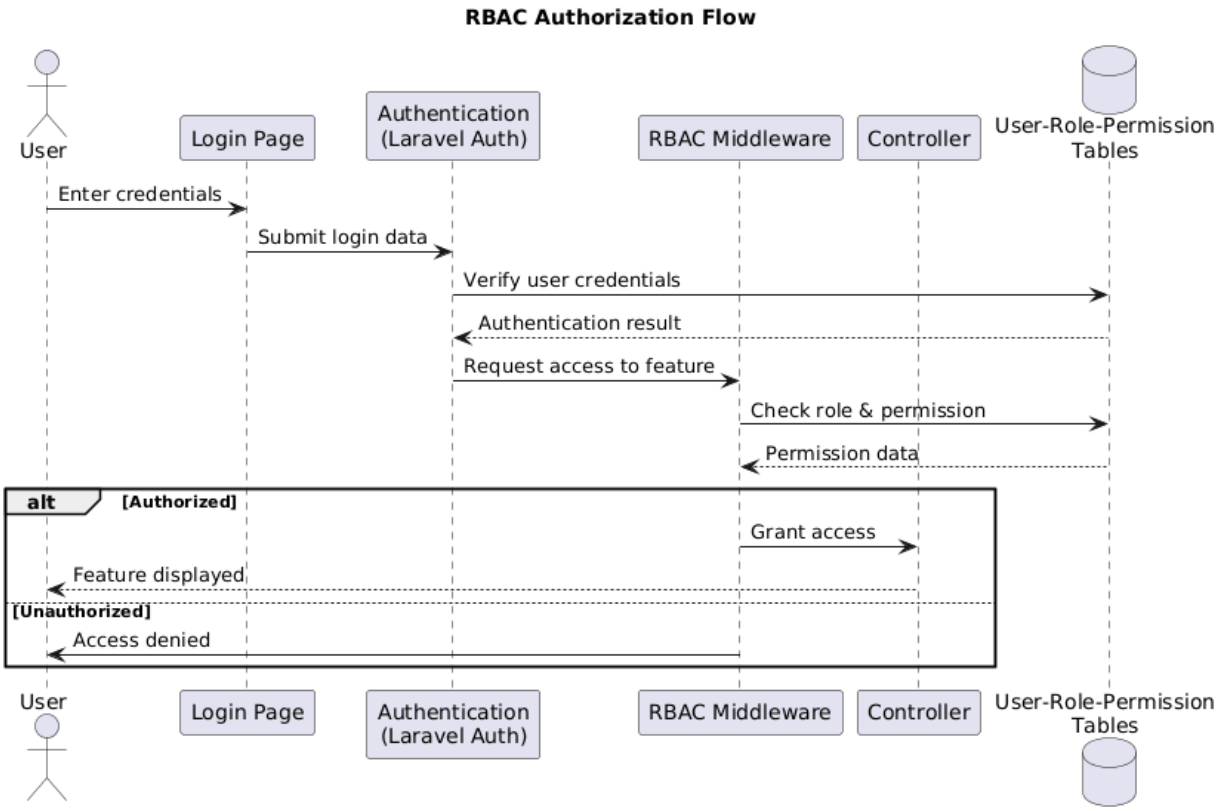

Fig. 3. RBAC Authorization Flow

Fig. 4. Landing Page

(MVC) architecture. Laravel was selected due to its support for structured development, built-in authentication and authorization features, and strong security mechanisms. The framework facilitates clean code organization, modular development, and efficient handling of user roles and permissions (Kinsta, 2025).

b. The use of Laravel enables consistent enforcement of RBAC rules across system modules and supports secure

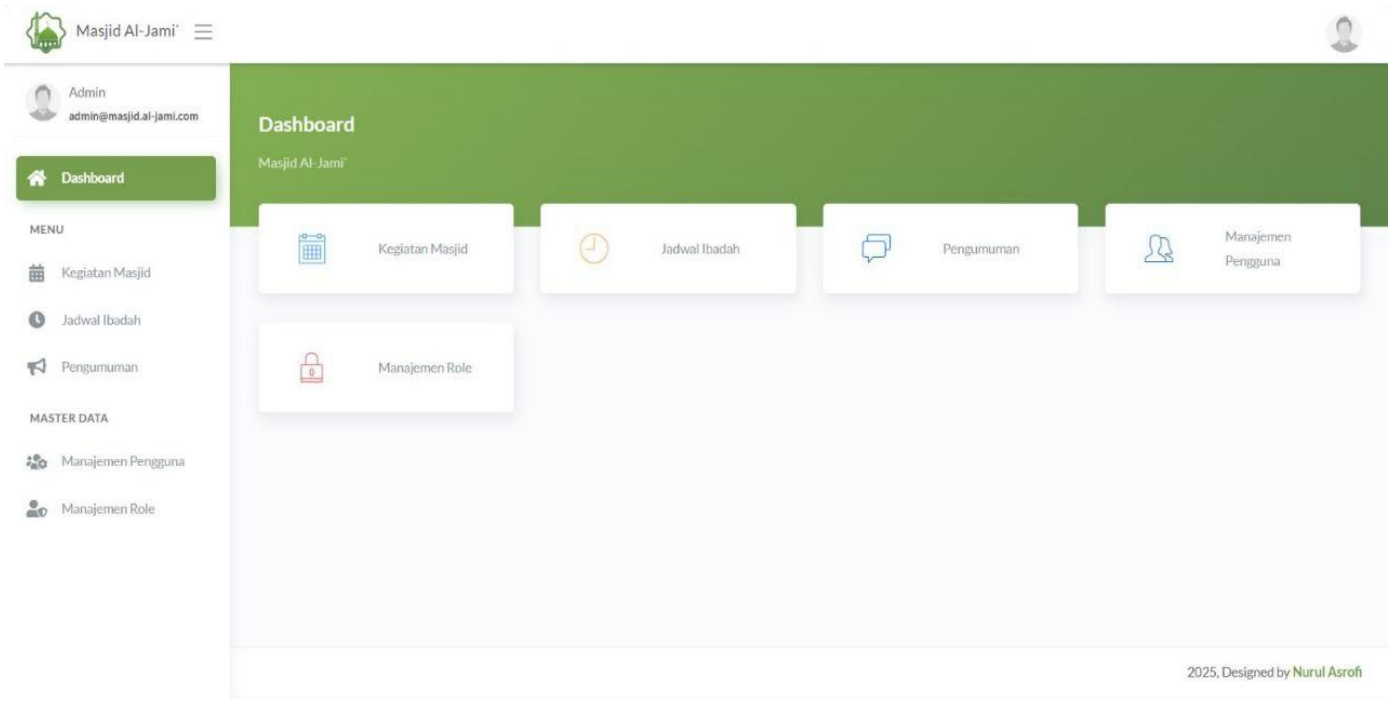

Fig. 5. Dashboard Admin

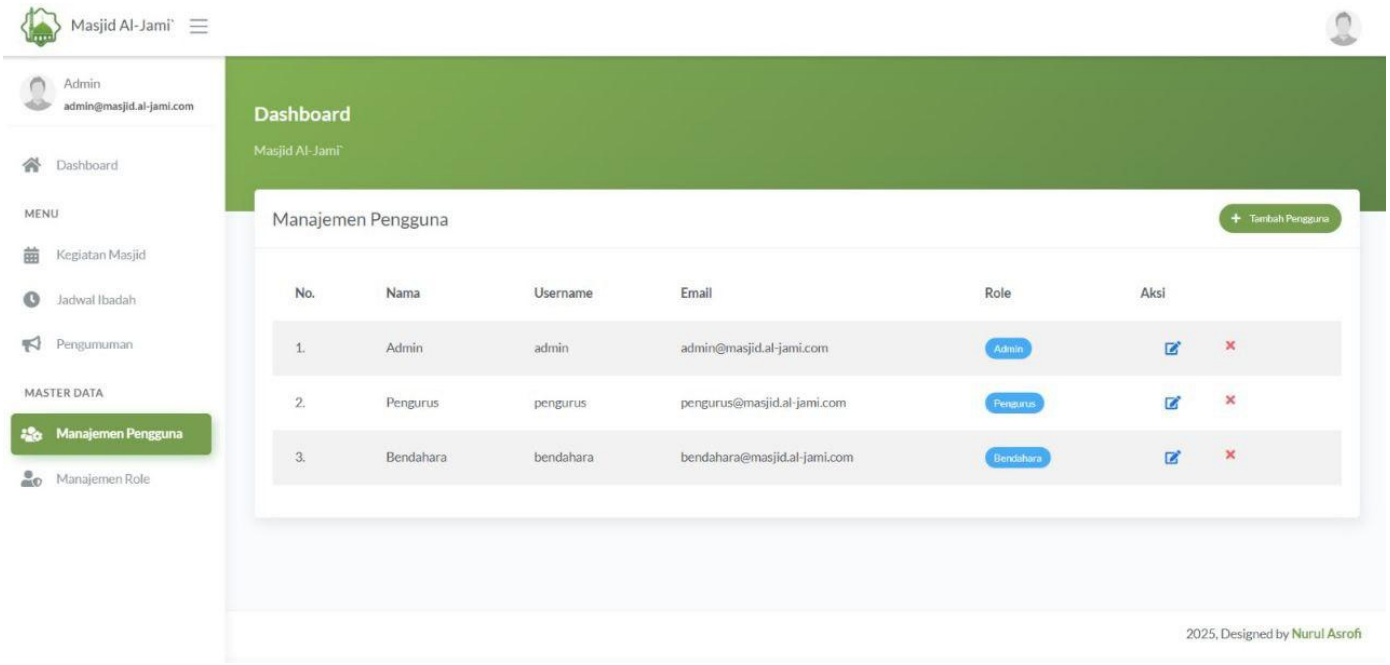

Fig. 6. Mosque Management Staff Dashboard

interaction between the application and the database. This framework-based implementation enhances system scalability, maintainability, and overall security.

2.3. *System testing*

System testing was conducted to ensure that the developed application operates in accordance with the defined requirements and that the access control mechanisms function correctly. Functional testing was performed to validate core system features, such as data input, data management, and information retrieval. In addition, role-based testing was conducted to verify that each user role could access only authorized system functionalities.

Unauthorized access attempts were also evaluated to confirm that the RBAC mechanism effectively restricted access to sensitive data and system features. The testing results

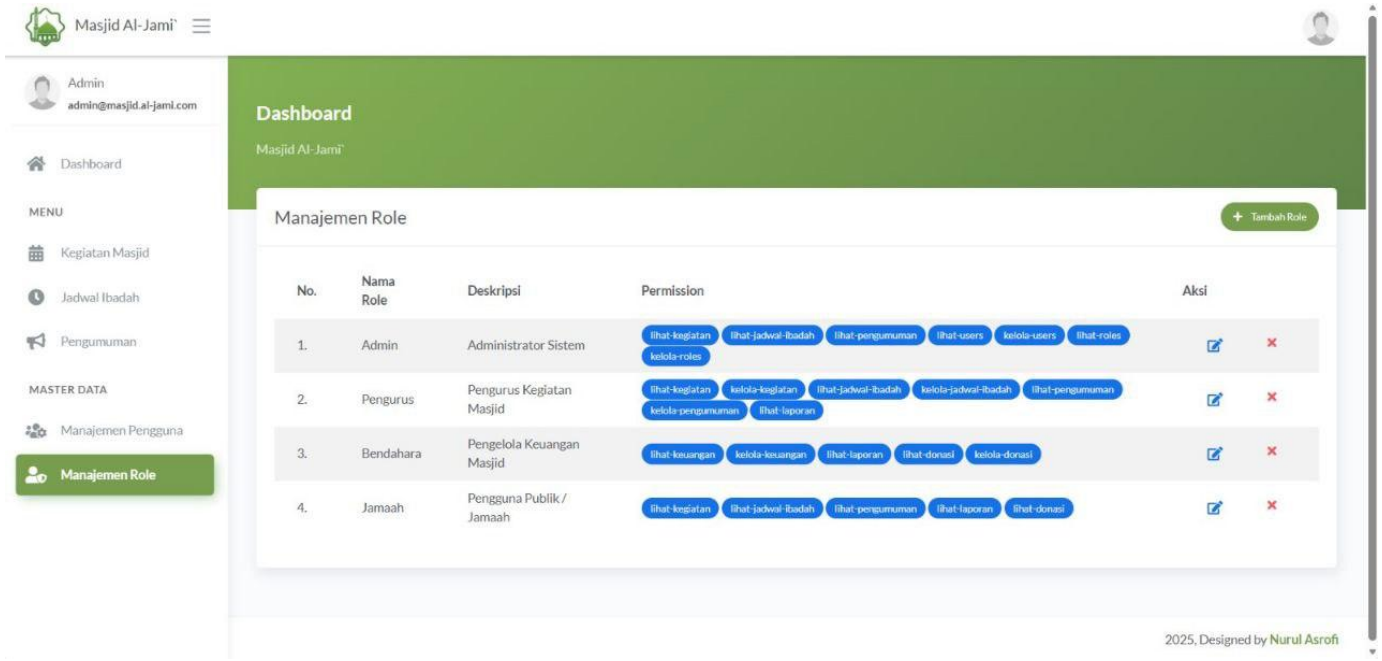

Fig. 7. Dashboard Treasurer

demonstrate that the system enforces access rules consistently and operates reliably within the defined scope.

In addition to functional and role-based access testing, basic penetration testing was conducted to evaluate common web application vulnerabilities. The testing was performed using OWASP ZAP to identify potential risks, including SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). The results showed no high-risk vulnerabilities under the tested scenarios, indicating that the access control mechanisms effectively restrict unauthorized interactions at the application level.

3. Results

3.1. System architecture

To provide a clearer understanding of the system structure beyond the user interface, this study presents the overall architecture of the web-based mosque information system. The architecture illustrates how users interact with the application and how access control mechanisms are enforced before any system functionality is executed. This architectural view emphasizes centralized data management, layered application design, and the integration of role-based access control within the application workflow.

As shown in Figure 2, all users—including administrators, mosque management staff, treasurers, and public users—access the system through a web browser. User requests are processed by the application layer, where authentication and RBAC middleware validate user identity and access permissions before forwarding requests to the business logic layer. This mechanism ensures that only authorized users can execute specific system functions, while all data interactions are handled centrally through the database server. Such architecture supports controlled access, data consistency, and maintainable system development.

3.2. RBAC implementation or system testing (access control)

To explain how access control decisions are enforced at runtime, a diagram of the authorization flow is presented. This diagram illustrates the step-by-step process of user authentication and role-based authorization applied in the system. The flow highlights the decision points where access is granted or denied based on user roles and permissions stored in the system database.

Figure 3 demonstrates that access control is enforced before any controller logic is executed. After successful authentication, each access request is evaluated by the RBAC middleware, which checks the user's assigned role and associated permissions against the authorization rules stored in the database. If the required permission is available, the requested feature is granted access; otherwise, the system denies access. This authorization flow ensures consistent enforcement of access policies and reduces the risk of unauthorized operations within the system.

Figure 4 shows the landing page of the web-based mosque information system. This page serves as the main entry point for users and provides general information about mosque activities, announcements, and public services. The landing page can be accessed without authentication, allowing public users to obtain essential information while maintaining restricted access to administrative features. This design supports transparency and public information dissemination without compromising system security.

Figure 5 illustrates the administrator dashboard interface of the mosque information system. This dashboard provides full access to system management functionalities, including user management, role configuration, activity management, and financial data oversight. The administrator role has the highest

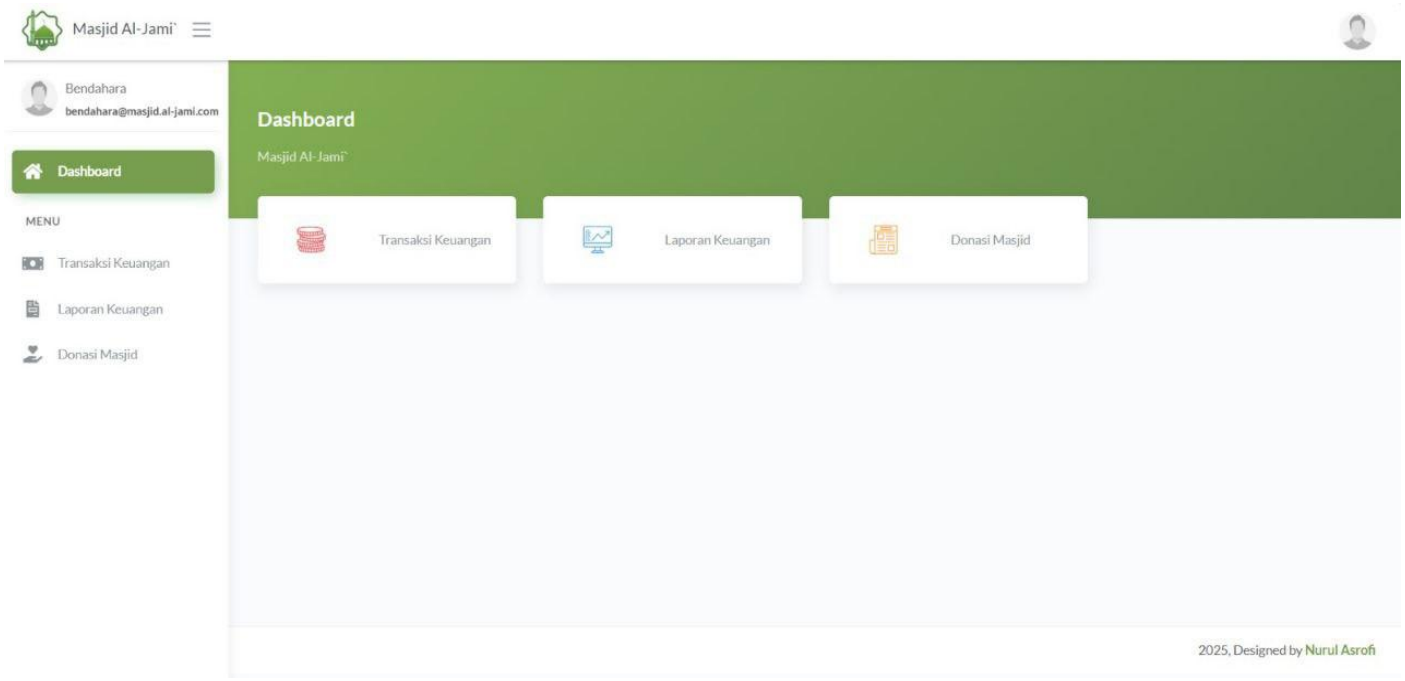

Fig. 8. Financial Report Display

level of access within the RBAC model, enabling centralized control and monitoring of system operations.

Figure 6 presents the dashboard interface for mosque management staff. This dashboard allows authorized users to manage mosque activities, schedules, and announcements. Access to financial and user management modules is restricted, demonstrating the enforcement of role-based access control by limiting system functionality based on the mosque management role's responsibilities.

Figure 7 shows the treasurer dashboard, specifically designed for financial management tasks. This dashboard enables the treasurer to record income and expenditure data, manage financial transactions, and generate financial reports. Access to non-financial modules is restricted, ensuring that financial data is handled only by authorized users and reinforcing secure access management.

Figure 8 illustrates the financial report display interface that presents summarized mosque financial information. This page is designed for public users with read-only access, allowing congregants to view financial reports transparently without the ability to modify data. The implementation supports accountability and transparency while preserving data integrity through controlled access mechanisms.

3.3. Performance evaluation

To provide an initial quantitative indication of system performance, a page load time evaluation was conducted on the most resource-intensive module of the application, namely the Financial Report page. This page was selected because it retrieves and processes aggregated financial data from the database, representing the highest computational load within the system.

The evaluation was performed in a local server environment using the browser's built-in Network monitoring tool. The total page load time was measured from the moment the request was initiated until the page was fully rendered in the browser.

The results show that the Financial Report page achieved an average load time of approximately 2.3 seconds. This performance is considered acceptable for a small-scale web-based information system intended for community-based organizational use. The findings suggest that implementing the RBAC middleware does not introduce noticeable performance overhead during request authorization.

4. Discussion

The implementation of a web-based mosque information system with Role-Based Access Control (RBAC) reflects broader efforts to transform mosque governance through digital technology. Previous studies have shown that digitalization in mosque management can significantly improve operational efficiency, transparency, and accountability by replacing manual administrative processes with centralized digital systems (Amin & Muhammadah, 2024; Chaniago et al., 2024; Sa'ari et al., 2025). In line with these findings, the system developed in this study supports digital transformation by structuring administrative workflows, clarifying responsibilities among mosque administrators, and enabling more transparent access to information for both internal stakeholders and the public.

From an access management perspective, the RBAC model applied in this system provides a structured authorization mechanism that aligns with role-oriented organizational structures commonly found in mosque management. Identity and Access Management (IAM) literature emphasizes that effective authorization mechanisms are essential for preventing unauthorized access while maintaining operational efficiency

(Premsai, 2024b; Vitla, 2023). The results of role-based access testing presented in Table 1 confirm that system functionality can be accessed only according to predefined permissions. Authorized actions were consistently permitted, while unauthorized access attempts were consistently denied, indicating that the RBAC mechanism effectively enforces application-level access boundaries.

Despite these advantages, the current RBAC implementation relies on predefined and static role definitions. In practice, mosque organizations often exhibit role fluidity, in which individuals may temporarily hold multiple responsibilities, such as serving as treasurer while also being part of the general management team. This organizational flexibility is not fully accommodated in the present system design. Similar challenges have been reported in the digital transformation of community-based organizations, where rigid role structures may limit adaptability to real-world operational dynamics (Kaur et al., 2025; Nurrahman et al., 2025). To address this limitation, the RBAC model can be extended to support temporary role assignments or multi-role activation for a single user account, preserving RBAC's administrative simplicity while enhancing organizational flexibility.

The system also addresses the balance between transparency and privacy, which is a critical concern in digital governance. While public access to financial reports supports transparency and strengthens community trust, as highlighted by (Haryono & Sujarwo, 2023), unrestricted access to detailed financial or personal data may raise ethical and security concerns (Goroz et al., 2017; Pina et al., 2024; Renuka et al., 2024). In this study, public users can view aggregated financial information, while detailed transaction records and donor identities remain restricted to authorized roles. This design aligns with best practices in access management that emphasize controlled openness to mitigate privacy risks while maintaining accountability (Alsamaualy et al., 2024).

In terms of security evaluation, basic penetration testing using OWASP ZAP supports the effectiveness of the RBAC implementation in controlling unauthorized access to system features. No high-risk vulnerabilities were identified across the tested scenarios, suggesting that application-level access control enforcement functions as intended. However, consistent with IAM research, access control alone does not guarantee comprehensive system security (Kaleru, 2025a). The security evaluation in this study is therefore limited to authorization enforcement and does not include advanced attack simulations, formal verification, or adaptive security mechanisms such as behavior-based authentication. Future research may explore integrating more advanced IAM approaches, including dynamic trust models or attribute-based access control, to further enhance system resilience in evolving threat environments.

5. Conclusion

This study demonstrates that implementing a web-based mosque information system integrated with Role-Based Access Control (RBAC) can support digital transformation in mosque administration by organizing access management and structuring administrative workflows based on defined roles. The RBAC mechanism effectively enforces authorization rules, ensuring that administrative, financial, and public information services are accessed only by authorized users.

System evaluation results indicate that the application operates reliably within its intended scope. Functional and role-based access testing confirm that access restrictions are consistently enforced, while a basic security evaluation reveals no high-risk vulnerabilities across the tested scenarios. In addition, an initial performance evaluation based on page-load time measurements indicates that the most resource-intensive module has an average load time of approximately 2.3 seconds, which is considered acceptable for small-scale community-based web applications.

Despite these positive results, this study has several limitations. The performance evaluation is limited to single-user page-load time measurements and does not include concurrent user stress testing or large-scale performance benchmarking. Furthermore, the assessment of administrative efficiency is based on system functionality and workflow organization rather than controlled usability testing or quantitative time-on-task measurement. Future research may incorporate comprehensive performance testing, user-based usability studies, and more flexible role management models to further enhance system scalability, efficiency assessment, and security resilience.

Data availability

All data generated or analyzed during this study are included in this published article. The system design, implementation results, and testing data are presented within the paper to support the research findings.

Declaration of competing interest

The authors declare that they have no known financial or personal competing interests that could have influenced the work reported in this paper.

Authors' contributions

Nurul Asrofi contributed to the system design, implementation, data collection, and drafting of the manuscript. Kasmawi supervised the research process, provided methodological guidance, and critically reviewed the manuscript. Pretti Ristra contributed to the literature review, data analysis, and manuscript revision. All authors discussed the results, reviewed, and approved the final version of the manuscript.

Acknowledgements

The authors would like to express their sincere gratitude to the academic supervisors and reviewers for their valuable guidance and constructive feedback, which significantly contributed to the improvement of this research.

References

Alsamaualy, I. A. C., Raisi, L., Al-Azzawi, M. I. Q., & Ashrafi, M. (2024). The Boundaries of Freedom in the Use of the Internet in Cyberspace. *Isslp*, *3*(2), 180–190. https://doi.org/10.61838/kman.isslp.3.2.18

Amin, M., & Muhammadah, S. (2024). Improving Mosque Management: Strategies Towards A Center For Islamic Activities.

Dedica, *1*(1).
Ardian, Z., Abdullah, D., Bintoro, A., Yusra, M., Akbar, A. H., & Lubis, F. A. (2024). A Smart Accounting System for Real-Time Mosque Financial Fund Management Based On Android and Web Mobile through The Implementation of The Agile Development Scrum Method. *JINAV: Journal of Information and Visualization*, *5*(2), 220–228. https://doi.org/10.35877/454ri.jinav3044
Aspizain, C. (2025). Improving Transparency and Efficiency of Administrative and Organizational Governance Through Smart Digital Technology and Cloning Systems. *Journal of Educational Technology and Learning Creativity*, *3*(2), 554–570. https://doi.org/10.37251/jetlc.v3i2.2481
Budhy, E., Dewi, R., & Negara, H. F. (2021). Sistem Informasi Manajemen Masjid Berbasis Website (Studi Kasus: Masjid Baitul Ikhwan). *Jurnal Sistem Informasi*, *22*(2).
Chaniago, S., Nurlaila, N., & Rokan, M. K. (2024). Transparency and Accountability in the Management of Independent Mosque Funds: A Case Study of Medan City Mosque. *Society*, *12*(2). https://doi.org/10.33019/society.v12i2.730
Goroz, D., Polonetsk, J., & Tene, O. (2017). Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data. *AAPSS*, *675*(1). https://doi.org/10.1177/0002716217742605
Grandhi, V. S. K. (2025). The Role of Identity and Access Management (IAM) in Modern Cybersecurity: Implementing Zero Trust Principles for Enhanced Enterprise Security. *World Journal of Advanced Engineering Technology and Sciences*, *15*(3), 179–186. https://doi.org/10.30574/wjaets.2025.15.3.0907
Haryono, K., & Sujarwo, A. (2023). Peningkatan Layanan Jemaah Melalui Implementasi Sistem Pengelolaan Keuangan Dan Aset Masjid Berbasis Web. *Transformasi Jurnal Pengabdian Masyarakat*, *19*(1), 22–34. https://doi.org/10.20414/transformasi.v19i1.5992
Kaleru, A. K. (2025a). Converged IAM: Transforming Enterprise Identity Management in the Cloud Era. *Journal of Computer Science and Technology Studies*, *7*(2), 598–603. https://doi.org/10.32996/jcsts.2025.7.2.64
Kaleru, A. K. (2025b). Identity and Access Management: Foundations, Principles, and Best Practices. *World Journal of Advanced Engineering Technology and Sciences*, *15*(1), 1894–1904. https://doi.org/10.30574/wjaets.2025.15.1.0393
Kaur, H., Reddy, K. K., Reddy, M. K., & Hanafiah, M. M. (2025). Collaborative Approaches to Navigating Complex Challenges and Adapting to a Dynamically Changing World. *Integration of AI, Quantum Computing, and Semiconductor Technology*. https://doi.org/10.4018/979-8-3693-7076-6.ch010
Kinsta. (2025). *The Laravel PHP Framework: Web App Construction for Everyone*.
Kirom, C., Cahyadi, I. F., Afandi, J., Adni, R., Cahya, B. T., & Muflih, B. K. (2024). Assistance in Management and Technology-Based Mosque Digitalization to Improve the Quality of Community Services. *Jurnal Pengabdian Undikma*, *5*(2), 205. https://doi.org/10.33394/jpu.v5i2.10920
Marquis, Y. A. (2024). From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts. *Journal of Engineering Research and Reports*, *26*(5), 138–154. https://doi.org/10.9734/jerr/2024/v26i51141
Mutambik, I., Lee, J., Almuqrin, A., Alkhanifer, A., & Baihan, M. S. (2023). Gulf Cooperation Council Countries and Urbanisation: Are Open Government Data Portals Helping? *Sustainability*, *15*(17), 12823. https://doi.org/10.3390/su151712823
Nurrahman, S., Saefullah, A., Abas, F., Tohiroh, T., Saksana, J. C., Azzahra, S. A., Hajar, E. S., Farsiah, L., Zainudidin, Z., & Nurdin, N. (2025). Pemberdayaan Pengurus Dan Jamaah Masjid Melalui Implementasi Sistem Informasi Manajemen Terpadu Berbasis Digital. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan*, *4*(1), 2373–2382. https://doi.org/10.31004/jerkin.v4i1.1974
Piasecki, J., Walkiewicz-Żarek, E., Figas-Skrzypulec, J., Kordecka, A., & Dranseika, V. (2021). Ethical Issues in Biomedical Research Using Electronic Health Records: A Systematic Review. *Medicine Health Care and Philosophy*, *24*(4), 633–658. https://doi.org/10.1007/s11019-021-10031-6
Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzelle, C., Abbasi, M., & Martins, P. (2024). Data Privacy and Ethical Considerations in Database Management. *Journal of Cybersecurity and Privacy*, *4*(3). https://doi.org/10.3390/jcp4030024
Premsai, R. (2024a). Cybersecurity Risks in Identity and Access Management Using an Adaptive Trust Authenticate Protocol. *Interantional Journal of Scientific Research in Engineering and Management*, *08*(12), 1–5. https://doi.org/10.55041/ijsrem25645
Premsai, R. (2024b). Mitigating Cyber Threats With Robust Identity and Access Management Techniques. *Interantional Journal of Scientific Research in Engineering and Management*, *08*(12), 1–7. https://doi.org/10.55041/ijsrem17705
Rahmawati. (2024). *Improving Mosque Information Media Based on Web Applications Using the System Development Life Cycle Method*.
Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection: Legal and Ethical Challenges. *Emerging Threats and Countermeasures in Cybersecurity*. https://doi.org/10.1002/9781394230600.ch19
Rizki, A., & Ekawati, N. (2023). Sistem Informasi Manajemen dan Keuangan Masjid Berbasis Web. *Jurnal Sistem Informasi*.
Rosidin, M., H., M. H. Z., & Sulistyo, W. Y. (2025). Perancangan Sistem Informasi Manajemen Asosiasi dengan Metode Waterfall dan RBAC di Majelis Diktilitbang Muhammadiyah. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *7*(3), 401–409. https://doi.org/10.47233/jteksis.v7i3.2012
Ross-Hellauer, T., Reichmann, S., Cole, N. L., Fessl, A., Klebel, T., & Pontika, N. (2022). Dynamics of Cumulative Advantage and Threats to Equity in Open Science: A Scoping Review. *Royal Society Open Science*, *9*(1). https://doi.org/10.1098/rsos.211032
Sa'ari, H., Mohammad, A., & Othman, R. (2025). Smart Mosque Information System (SMIS): A Framework for Digital Da'wa and Religious Tourism in Malaysia. *International Journal Of Academic Research In Business And Social Sciences*, *15*(9). http://dx.doi.org/10.6007/IJARBSS/v15-i9/26428
Siregar, N. H., Oktavia, A., & Nusantara, A. P. (2023). Sistem Informasi Manajemen Masjid Al-Ikhlas Berbasis Web. *Jurnal Bisantara Informatika*, *7*(2).
Sutrisno, N. A., Kamarulzaman, M. H., & Ibrahim, S. S. (2022). Digitalisation Empowerment in Mosque Tourism Management; A Potential and Current Practice. *International Journal of Academic Research in Business and Social Sciences*, *12*(7). https://doi.org/10.6007/ijarbss/v12-i7/14324
Vitla, S. (2023). Pioneering IAM Innovations: Securing Data, Mitigating Cyber Threats, and Driving Compliance in the Cybersecurity Landscape. *International Journal of Science and Research Archive*, *10*(1), 1130–1150. https://doi.org/10.30574/ijsra.2023.10.1.0714

Nurul Asrofi is currently pursuing a Bachelor's degree in Informatics Engineering from Bengkalis State Polytechnic, Indonesia. Her research interests focus on the development of web-based information systems, role-based access control mechanisms, and the implementation of information security in organizational and community-based systems, particularly to improve data protection, access management, and system transparency.

Kasmawi is a lecturer and Head of the Informatics Engineering Department at Bengkalis State Polytechnic. He specializes in information systems development, data security, and the implementation of digital solutions for education and public services. He is active in community service, collaboration with schools (vocational high schools), research, and supervision of application development and student. training. He is involved in research and scientific publications, including mobile/web applications and information systems for MSMEs and digital services

Pretti Ristra is a lecturer at Politeknik Negeri Bengkalis, specializing in English for Specific Purposes. She holds a Master's degree in Education (TESL) from the University of Malaya, Kuala Lumpur, Malaysia. Pretti has contributed to various research publications and has extensive experience in language education, particularly in enhancing students' community-based systems by improving data protection, access management, and system transparency.