Jurnal Mandiri IT
Vol. 14 No. 3, January (2026), pp. 368-380

ISSN 2301-8984 (Print), 2809-1884 (Online)
Published by Institute of Computer Science

Development of the Kamar Sandi letter agenda information system application in the Pamsisinfosan Pusdatin Kemhan RI

Findi Zhafirah[1], M Azhar Prabukusumo[2], Aulia Khamas Heikhmakhtiar[3], Nadiza Lediwara[4], Angga Ferdian Mayuni[5]

[1,2,3,4] Informatics, Republic Indonesian Defense University, Bogor, Indonesia
[5] Kementrian Pertahanan Republik Indonesia, Jakarta, Indonesia

ARTICLE INFO

Article history:

Received Dec 22, 2025
Revised Dec 30, 2025
Accepted Jan 13, 2026

Keywords:

Audit Trail;
Backup–Restore;
Correspondence Management;
RBAC;
Web Information System.

ABSTRACT

This study describes the development of a web based correspondence information application for managing incoming and outgoing letters in the Kamar Sandi unit (Pamsisinfosan Division, Pusdatin Kemhan RI), replacing a legacy Visual Basic desktop system with unreliable database access, single host limitation, no scheduled backups, and a non intuitive interface. This research employs the Rapid Application Development (RAD) method to facilitate iterative prototyping and rapid adaptation to operational requirements. Using a modular Laravel/Livewire + MySQL stack, the application centralizes letter metadata and master data (origin/destination, security degree, communication channel, cryptographic system) and provides automated agenda numbering, role-based access control (Admin, Pimpinan, Petugas), and a secure flow for classified letters via PIN validation and hashed identifiers. Supporting modules include a notification center, activity/audit logs, Excel/PDF export, and scheduled backup–restore with PIN gated downloads. Evaluation results indicate a significant increase in operational efficiency, evidenced by a ~60% reduction in mail recording time and a decrease in data retrieval duration from over 10 minutes to under 5 seconds, with a 100% success rate in eliminating agenda duplication errors. The application operationalizes these findings through granular authorization, input & CSRF validation, gated secret document access, indexed search with multi criteria filtering, and integrated backup–restore enhancing accessibility, retrieval efficiency, and auditability while lowering operational risk. Key contributions are: (1) translating migration pain points into an iterative implementation, (2) embedding security and preservation features at design time, and (3) presenting an evidence aligned functional model for government records management. Future enhancement can add retention policy automation and secure inter agency integration.

Corresponding Author:

Findi Zhafirah,
Informatics,
Republic Indonesian Defense University,
Kawasan IPSC Sentul, Jl. Anyar, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810
Email: findizhafirah2004@gmail.com

1. INTRODUCTION

The efficiency of information management within defense institutions, specifically the Data and Information Center (Pusdatin) of the Ministry of Defense of the Republic of Indonesia (Kemhan RI), relies heavily on the reliability of mail administration systems. Systematic documentation of incoming and outgoing mail activities is an absolute prerequisite for ensuring rapid and accurate information accessibility (Afifah et al., 2025). However, the current digital infrastructure in the Kamar Sandi Pamsisinfosan still relies on a legacy desktop-based application (Visual Basic) which possesses

critical limitations. Technical constraints such as locked databases (inaccessible) despite ongoing data recording, single-access restrictions tied to specific hardware, and the absence of automatic backup mechanisms have led to decreased operational efficiency and increased the risk of losing strategically valuable historical data (Chandra et al., 2024). Such weaknesses in data management often trigger information redundancy and hinder work efficiency due to the absence of centralized data validation (Nazwa Hanifah & Muhammad Irwan Padli Nasution, 2025).

Public service transformation demands a paradigm shift from isolated systems toward integrated architectures. Recent studies confirm that migration to web-based systems is a crucial step to overcome recording inconsistencies and multi-location access limitations (Hamdani et al., 2024). The application of modern frameworks like Laravel in government mail archive management systems has proven capable of improving numbering accuracy and data storage security compared to conventional methods (Lailatul Fitria & Umi Chotijah, 2024). Furthermore, effective e-government implementation requires Role-Based Access Control (RBAC) and disaster recovery mechanisms to minimize data redundancy (Supriadi & Sa'uda, 2025). The use of RBAC is crucial for limiting user access rights according to their duties, thereby maintaining data integrity from unauthorized access (Khairi, 2024). In the context of sensitive information security, system success is measured not only by functionality but also by the readiness of security infrastructure such as granular authorization, audit trails, and encryption, which must be planned from the early stages of the development cycle (Setiawan et al., 2025).

However, prior public-sector correspondence and e-archive studies generally do not integrate layered security controls, specifically Role-Based Access Control (RBAC), hashed identifiers, and PIN-gated classified access, together with centralized agenda numbering and disaster recovery into a single coherent design for sensitive units. Furthermore, existing literature rarely reports transparent, measurable efficiency and reliability outcomes before and after implementation, and provides limited guidance for multi-role, cross-location operations. SI-KASA is specifically positioned to fill this gap by combining secure-by-design architecture, centralized agenda governance, audit trails, and automated preservation (backup and restore) mechanisms with defined indicators for efficiency, reliability, and usability. This system aims to replace the problematic legacy infrastructure by managing incoming and outgoing mail centrally, ensuring the mail management process at the Kamar Sandi Pamsisinfosan Pusdatin runs efficiently, transparently, and securely.

With this research, it is expected that the contribution is not limited to the technical aspects of system development, but also provides strategic learning regarding migration from desktop to web systems (Kanugraha & Abimanyu, 2023), the importance of good system documentation (Najihah, 2023), and effective data backup-restore strategies (Sari & Nasution, 2025). Specifically, this research aims to eliminate data redundancy and ensure zero data loss through a centralized web architecture. The results are expected to serve as a reference for other work units within the Kemhan RI environment and government agencies that still use legacy desktop-based systems. To achieve these objectives, the system development employs the Rapid Application Development (RAD) method, which allows for iterative prototyping and rapid user feedback adaptation, ensuring the final logic aligns perfectly with the unique operational protocols of the Kamar Sandi.

2. RESEARCH METHOD

The method used is Rapid Application Development (RAD), which emphasizes rapid iteration with intensive user involvement. The RAD method was chosen because it prioritizes gradual development processes, which is very suitable for projects with tight deadlines. Unlike the Waterfall model which is often too rigid for evolving security requirements, or Agile Scrum which demands high product owner availability that is difficult to fulfill in this unit's operational tempo, RAD is preferred here as it allows for rapid prototyping and immediate user feedback within a fixed strict deadline. RAD focuses on short and responsive development cycles, with strategies focused on prototyping, iterative repetition, and continuous feedback acceptance (Siswaya & Setiawan, 2025). To ensure the study's replicability, the research subjects involve three specific user roles, namely Administrators, Picket Officers (*Petugas Piket*), and Leaders (*Pimpinan*). Data collection techniques utilized semi-structured interviews with Officers of Pamsisinfosan to gather core requirements and direct observation of features from the previous legacy application to identify functional gaps. The research flow is illustrated in Figure 1.

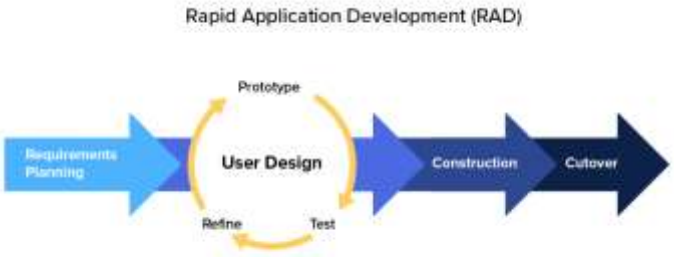

Figure 1. RAD Method

The detailed stages of the research implementation are as follows:
1. Requirements Planning: Gathering requirements through interviews and observation of the mail recording process, identifying problems (limited access, no backup, minimal audit). Success for this phase is evidenced when the agreed scope and risk controls (RBAC, audit, backups) are documented and traceable to planned features (Masaid et al., 2024).
2. User Design: Creating initial interface designs (recording forms, mail lists with filters, activity dashboards). Prototypes are evaluated by potential users (Officers, Admins, Leaders) and revised. This phase aims to achieve user consensus through iterative feedback loops before proceeding to the coding stage (Wirapraja & Kardinata, 2025).
3. Construction: Gradual implementation of core modules (incoming/outgoing mail recording, master data management, authentication & roles, notifications, backup/restore). Black-box testing is conducted per module to ensure functions meet specifications. The success criterion is a 100% "Valid" result on all functional test cases, indicating zero critical bugs (Bagus Aryandra & Cahya Wardhana, 2024).
4. Cutover: Final integration, necessary data migration, brief user training, and operational transition from the old application to SI-KASA. Evaluation is performed using User Acceptance Testing (UAT) which contains scenarios, test cases, expected results, testing results, and remarks for each role to measure the success rate of functions. Additionally, time efficiency is measured by comparing the process duration before and after implementation (Suwintana & Sudiadnyani, 2020).

3. RESULTS AND DISCUSSIONS

In this section, it is explained the results of research and at the same time is given the comprehensive This section explains the results of the system design aimed at translating requirements into clear and auditable models, minimizing ambiguity, and serving as a reference for implementation.

Use Case Diagram

The Use Case Diagram is used as a primary modeling tool due to its strong ability to describe system behavior in a way that is easily understood by all stakeholders (Setiyani, 2021). This diagram identifies external requirements and actor interactions with the designed system, as shown in Figure 2. In SI-KASA, there are three main actors: Admin (managing master data and users), Officer (recording mail and dispositions), and Leader (monitoring dashboards and reports). This diagram helps capture essential functions that the system must perform and the boundaries of actions available to each role.

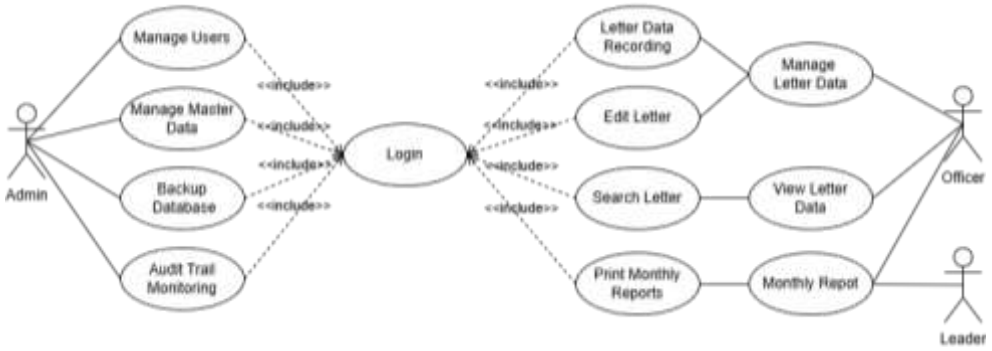

Figure 2. Use Case Diagram

Activity Diagram

The Activity Diagram is a behavioral diagram that depicts the internal processes of various operations within a program by utilizing node and edge elements (Ramdany, 2024). This diagram is highly useful for visualizing business workflows clearly, assisting in process efficiency analysis, and identifying potential issues.

a. Login Activity Diagram

Illustrates the sequence of activities when a user accesses the system, as depicted in Figure 3. The user enters credentials, the system validates the format and searches for the account in the database, then verifies the password (hash). If valid, the system directs to the dashboard according to the role (RBAC); if not, the system displays an error message. This flow asserts access control as a prerequisite for all subsequent processes.

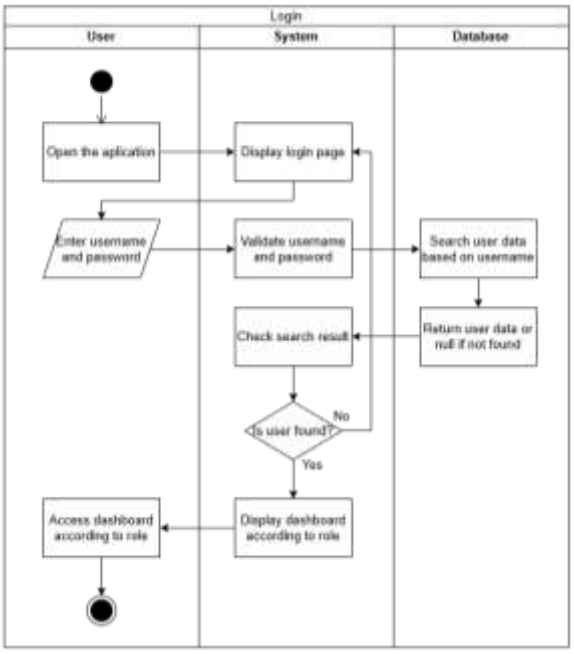

Figure 3. Login Activity Diagram

b. Mail Recording Activity Diagram

Explains the end-to-end recording flow illustrated in Figure 4. After the officer completes the form (Agenda Number, Narkom, Subject), the system validates input and checks for agenda number duplication. The system then uploads digital attachments, generates a unique number, and saves the transaction atomically to the database. Notifications are sent as feedback of success to the user.

Figure 4. Mail Recording Activity Diagram

c. Report Activity Diagram

Figure 5 illustrates how users browse data: the system loads the initial list, the user sets multi-criteria filters, the system executes indexed queries and displays results. Users can view details or export to Excel. This flow ensures rapid and consistent retrieval.

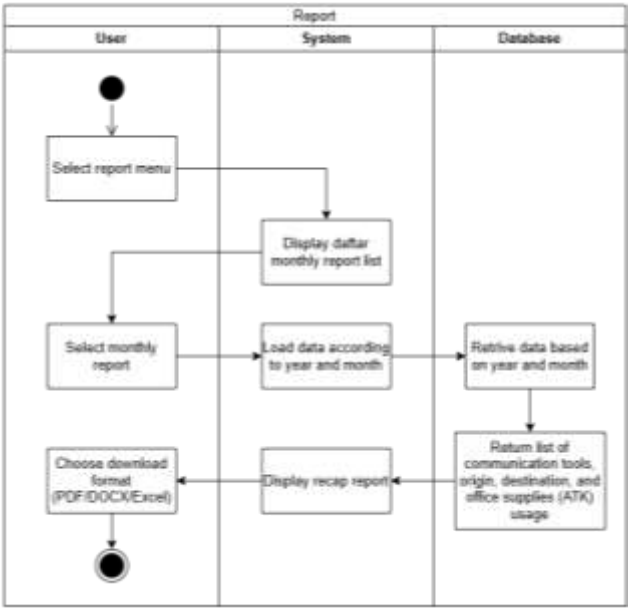

Figure 5. Report Activity Diagram

d. View Letter Data Activity Diagram

Depicts the data retrieval and filtering workflow as shown in Figure 6. The user selects the letter data menu, triggering the system to load and display all available letter records from the database. When the user applies search filters (date range, category, type, sender, recipient), the

system queries the database with the specified criteria and presents the filtered results. The user can then view detailed information for specific letters or export the data to Excel format for external analysis. This flow ensures efficient data browsing with flexible filtering capabilities and multiple output options.

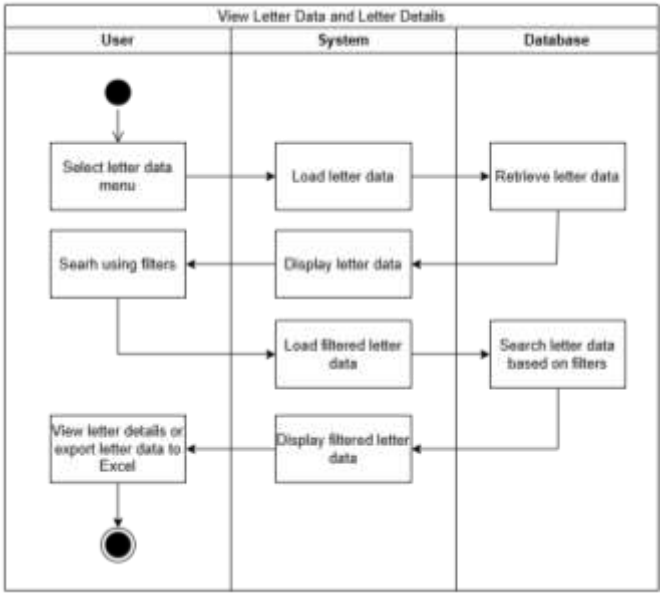

Figure 6. View Letter Data Activity Diagram

Class Diagram

The Class Diagram allows for the declarative modeling of the static structure of an application domain by representing concepts and the relationships between them (Paradis et al., 2022). This diagram plays a crucial role in depicting the static structure of the SI-KASA system as shown in Figure 7, displaying main classes such as User, SuratMasuk, SuratKeluar, Disposisi, and LogAktivitas along with their attributes and methods. This visualization helps developers understand the system architecture in an organized manner, facilitating the code implementation process and the maintenance of data entity relationships in the future.

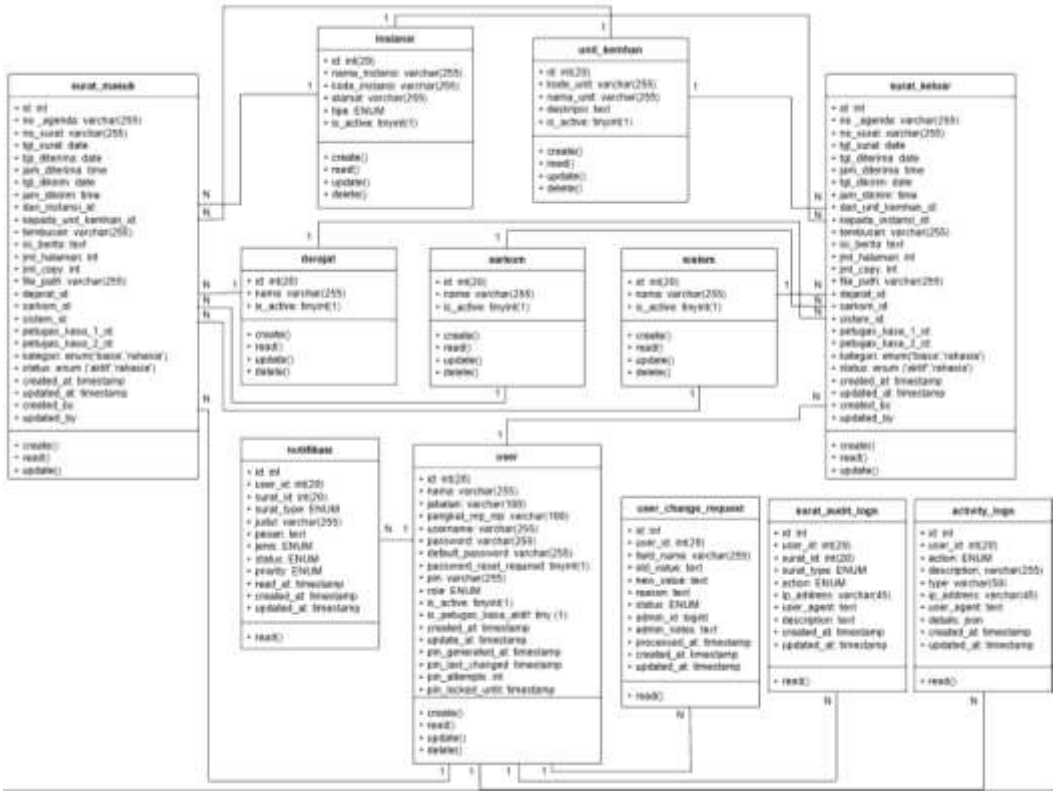

Figure 7. Class Diagram

System Results

The next development step is implementation. This stage demonstrates the tangible interface design of SI-KASA and how each page supports the mail agenda management business process in a structured, secure, and easily traceable manner.

a. Login Page

Figure 8 displays the login page which serves as the initial gateway to the system. Users enter their username and password, then the system validates the format and credentials. A minimalist layout focusing on authentication elements helps reduce input errors and speeds up access. The agency logo at the top reinforces the system identity and official usage context.

Figure 8. Login Page

Figure 9 shows the security code verification mechanism (captcha) after credentials are entered. Users are required to retype the displayed random numbers. This layer adds protection

against automated attacks (bots) while enhancing the integrity of the login process before access rights are granted. A code refresh button allows regeneration if the code is difficult to read.

Figure 9. Login Page (2)

b. Officer Dashboard

Figure 10 represents the initial view after successful authentication for the Officer role. The dashboard presents function cards (recording, reports, mail data) and metric summaries (total mail, incoming/outgoing classification, ordinary/secret category). This aggregate presentation helps prioritize daily work and provides data health indicators (e.g., distribution of secret vs. ordinary mail). Side navigation maintains consistent access to modules.

Figure 10. Officer Dashboard

c. Data Recording

Figure 11 shows the top section of the recording page with two selection blocks: mail type (incoming or outgoing) and category (ordinary or secret). This visual separation forces users to classify from the start, preventing miscategorization that could affect disposition flows and access control. Active status is marked with contrasting colors to reduce selection ambiguity.

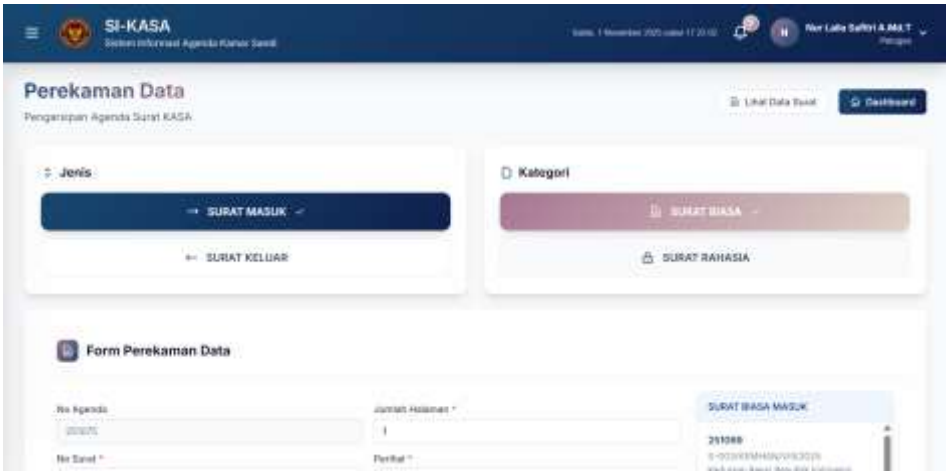

Figure 11. Data Recording

Figure 12 displays the complete recording form. Fields provided include agenda number (automatic or controlled), mail number, date and time, origin/destination, carbon copy (CC), degree, sarkom/cryptographic system, number of pages/copies, document upload, and assignment of related officers. The side panel displays a list of recent mail as a quick reference to avoid duplication. Validation is applied to ensure data completeness before atomic transaction storage.

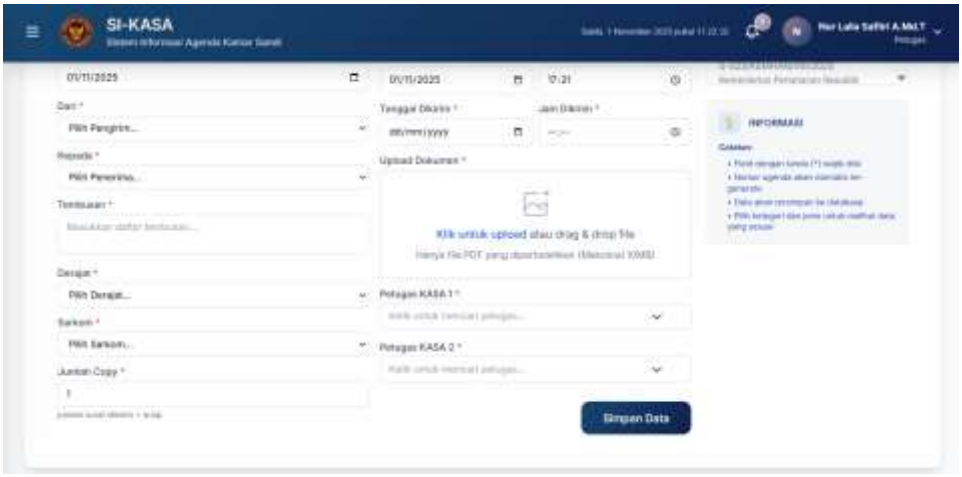

Figure 12. Data Recording

d. Report Page

Figure 13 shows the report module presenting a recap per period. Users can select a year, then view a summary per month: total mail, incoming/outgoing classification, and separation of secret and ordinary categories. The table structure allows for quick auditing of volume trends and anomaly identification (e.g., spikes in secret mail). Formatted data is ready to be exported for leadership reporting needs.

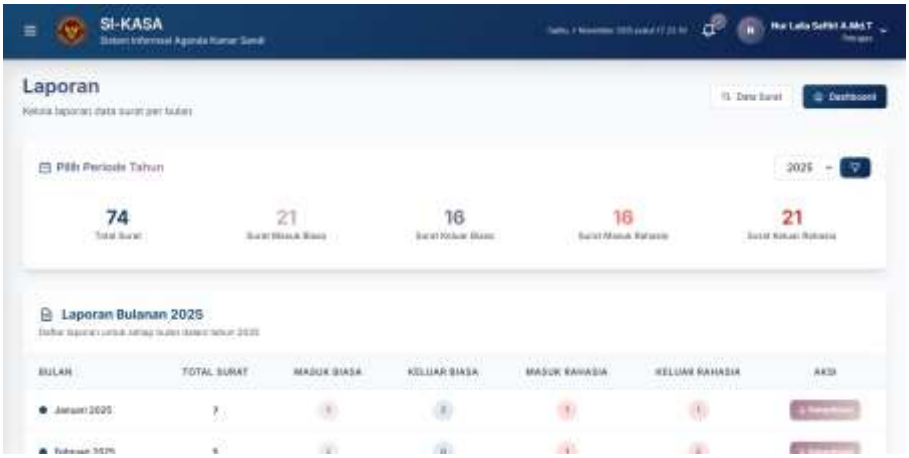

Figure 13. Report Page

e. Mail Data Page

Figure 14 displays the retrieval feature with multi-criteria filters: date range, category, type, agenda number, mail number, sender, recipient. This targeted search mechanism speeds up the investigation process or specific document retrieval. The bottom section displays dynamic metric summaries (total mail, incoming mail, outgoing mail, active period) as feedback on the data context being filtered.

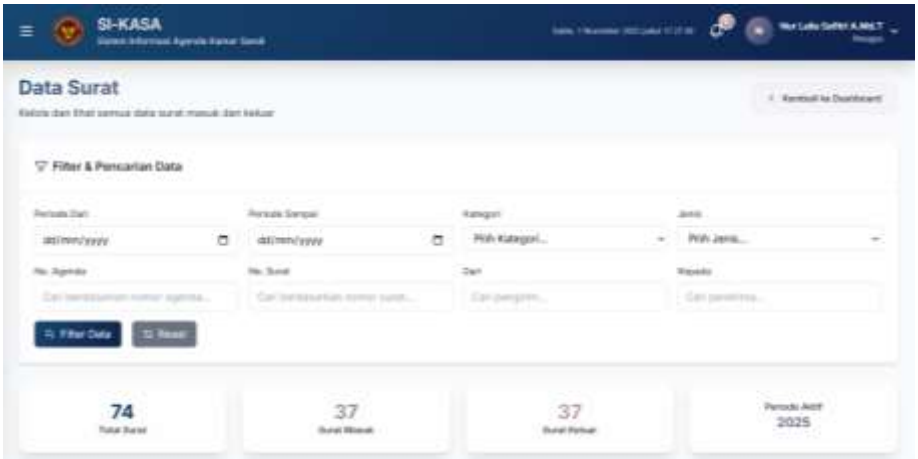

Figure 14. Mail Data Page

Testing and Comparative Evaluation

Testing was conducted to verify functional compliance and measure operational efficiency improvements.

a. Black-Box testing

Black-Box testing is a specification-based testing method that assesses software from the outside without knowing the internal structure/code; testers design test cases from requirements or contracts, provide input through available interfaces, then evaluate whether the observed output and behavior meet expectations. Its utility includes verification of functional requirement fulfillment, input-output and business rule validation, and interface compatibility and regression checks at the real usage level (Romdhana et al., 2022). The goal is to ensure features visible to users or other systems run according to contract, finding functional/integration defects as early as possible, and enhancing reliability from the user's perspective without relying on implementation details (Dharmaadi et al., 2025). The results of the system functionality testing can be seen in Table 1.

Table 1. Blackbox Testing

Page / Module	Test Scenario	Expected Result	Test Result	Remark
Login	User (Admin/Officer/Leader) logs in with valid credentials	System validates and redirects to role-specific dashboard	Successfully entered appropriate dashboard	Pass
Login	User logs in with invalid credentials	System rejects and displays error message	Input error message appeared	Pass
Dashboard	Admin/Officer/Leader views statistical summary	Dashboard displays mail metrics, charts, and notifications	Statistics and charts displayed accurately	Pass
User Management	Admin adds or updates user data	User data saved/updated in database	New user successfully created/updated	Pass
Mail Recording	Officer records new incoming/outgoing mail	Mail saved with auto-generated agenda number	Mail successfully saved and notified	Pass
Mail Recording	Officer uploads PDF attachment	File uploaded and saved on server	File successfully uploaded and previewable	Pass
Mail Data	Officer searches mail by agenda number or date filter	System displays relevant search results	Searched mail data successfully displayed	Pass
Report	User views and downloads monthly recapitulation	Report preview appears and file downloads (PDF/DOCX)	Report successfully previewed and downloaded	Pass
Document Access	User downloads secret mail document	System requests security PIN before download	Correct PIN input grants download	
Notification	System receives new or urgent mail	Real-time notification appears for related users	Notification received with badge counter	Pass

b. User Acceptance Testing (UAT)

UAT validated specific security workflows involving actual users. The results demonstrate that the "Document Access" feature successfully demands a PIN before downloading secret files, and the "Notification" module delivers real-time alerts. This confirms that SI-KASA's security infrastructure—specifically granular authorization—is operationally ready, addressing the gaps found in generic e-office systems.

c. Quantitative Comparative Analysis

To measure success, a comparative analysis between the legacy desktop system and SI-KASA was conducted (Table 2).

Table 2. Efficiency comparison

Metric	Legacy System	SI-KASA	Improvement Impact
Avg. Recording Time	4 - 5 minutes	1 - 2 minutes	~60% Faster
Retrieval Speed	> 10 mins (manual scroll)	< 5 secs (indexed search)	~99% Faster
Error Rate	High (Duplicate Agendas)	Zero (System Validation)	Eliminated
Availability	Single Access (Queueing)	Multi-User Concurrent	High Availability

4. CONCLUSION

The development of SI-KASA using the RAD method successfully modernizes mail management in sensitive environments by replacing legacy systems through centralized recording, cross-location accessibility, and automatic backup mechanisms that reduce data redundancy. Empirically, this research confirms a significant increase in operational efficiency, evidenced by the reduction of data retrieval time from minutes to under five seconds and the complete elimination of agenda number duplication errors compared to the legacy infrastructure.The system strengthens information security architecture through the implementation of Role-Based Access Control (RBAC), CSRF validation, hashed IDs to prevent IDOR, as well as PIN gating and audit trails aligned with global standards (Marín-López et al., 2020; Taresh Mehra, 2024; Чечет et al., 2024). In line with literature, the adoption of web-based mail systems accelerates data recording and retrieval, while demanding

mature digital archive governance (Santosa, 2024). However, this study is currently limited to the internal operational scope of the Kamar Sandi and has not yet addressed integration with external inter-agency systems or mobile platform accessibility. For sustainability, the integration of end-to-end encryption, two-factor authentication (2FA), and smart notifications is recommended to enhance operational effectiveness and compliance with high-level security protocols.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the Head of the Cryptographic System Development Subdivision (Subbid Bangsissan) and the staff of the Data and Information Center, Ministry of Defense of the Republic of Indonesia, for their support, cooperation, and valuable input throughout this research. Appreciation is also extended to colleagues and academic supervisors for their constructive feedback and encouragement during the study and manuscript preparation.

REFERENCES

Afifah, Y., Hazairin, I. N., & Agustino, A. (2025). Pembekalan Penataan Administrasi Persuratan dan Kearsipan: Manajemen Kinerja Tenaga Kependidikan di Lingkungan Madrasah. *Jurnal Pengabdian Kepada Masyarakat Nusantara*, *6*(3), 3825–3832. https://doi.org/https://doi.org/10.55338/jpkmn.v6i3.5601

Bagus Aryandra, B., & Cahya Wardhana, A. (2024). PERANCANGAN SISTEM INFORMASI DESA WISATA BERBASIS WEBSITE DENGAN METODE RAPID APPLICATION DEVELOPMENT (RAD). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5936–5944. https://doi.org/10.36040/jati.v8i4.9768

Chandra, A. Y., Widhiantoro, D., & Utami, B. (2024). Perancangan Sistem Automasi Backup Konfigurasi Perangkat Pada Internet Service Provider. *Seminar Nasional Teknik Elektro*, *10*(1), 155–161.

Dharmaadi, I. P. A., Athanasopoulos, E., & Turkmen, F. (2025). Fuzzing frameworks for server-side web applications: a survey. *International Journal of Information Security*, *24*(2), 73. https://doi.org/10.1007/s10207-024-00979-w

Hamdani, A., Saleh, T., Samad, A., & Adiman, M. F. (2024). Sistem Informasi E-Arsip Berbasis WEB di Kantor Desa Bulusari. *Justify: Jurnal Sistem Informasi Ibrahimy*, *2*(2), 124–134.

Kanugraha, N. Y., & Abimanyu, F. A. (2023). *OPTIMISASI MIGRASI SISTEM DESKTOP KE PLATFORM WEBSITE QIS (Quick Information System)*.

Khairi, A. S. (2024). Implementasi Role Based Access Control dalam Pengelolaan Hak Akses Koperasi Berbasis Mobile. *Jurnal Teknik Informatika Unika ST. Thomas (JTIUST)*, *9*(1).

Lailatul Fitria, & Umi Chotijah. (2024). Implementasi Framework Laravel pada Sistem Manajemen Penomoran dan Arsip Surat Bawaslu Kota Surabaya. *SABER : Jurnal Teknik Informatika, Sains Dan Ilmu Komunikasi*, *2*(4), 58–72. https://doi.org/10.59841/saber.v2i4.1676

Marín-López, A., Chica-Manjarrez, S., Arroyo, D., Almenares-Mendoza, F., & Díaz-Sánchez, D. (2020). Security Information Sharing in Smart Grids: Persisting Security Audits to the Blockchain. *Electronics*, *9*(11), 1865. https://doi.org/10.3390/electronics9111865

Masaid, A. J., Suseno, P., Al Raidhan, M. A., & Setiawan, I. (2024). RANCANG BANGUN SISTEM INFORMASI LAYANAN MASYARAKAT MENGGUNAKAN MODEL RAPID APPLICATION DEVELOPMENT (RAD) STUDI KASUS DESA HARJATANI. *Jurnal Digit*, *14*(2), 179. https://doi.org/10.51920/jd.v14i2.411

Najihah, W. 'Ainun. (2023). Pentingnya Manajemen Perkantoran dan Informasi dalam Sebuah Organisasi. *Opportunity Jurnal Penelitian Dan Pengabdian Masyarakat*, *1*(1), 40–46. https://doi.org/10.55352/oppotunity.v1i1.492

Nazwa Hanifah, & Muhammad Irwan Padli Nasution. (2025). Manajemen Data Yang Efektif: Solusi Untuk Mencegah dan Mengatasi Duplikasi Data Dalam Perusahaan. *Epsilon Journal of Management*, *3*(1), 27–38. https://doi.org/10.62951/epsilon.v3i1.124

Paradis, C. N., Robert Yusuf, M., Farhanudin, M., & Ainul Yaqin, M. (2022). Analisis dan Perancangan Software Pengukuran Metrik Skala dan Kompleksitas Diagram Class. *Journal Automation Computer Information System*, *2*(1), 58–65. https://doi.org/10.47134/jacis.v2i1.40

Ramdany, S. (2024). Penerapan UML Class Diagram dalam Perancangan Sistem Informasi Perpustakaan Berbasis Web. *Journal of Industrial and Engineering System*, *5*(1), 30–41. https://doi.org/10.31599/2e9afp31

Romdhana, A., Merlo, A., Ceccato, M., & Tonella, P. (2022). Deep Reinforcement Learning for Black-box Testing of Android Apps. *ACM Transactions on Software Engineering and Methodology*, *31*(4), 1–29. https://doi.org/10.1145/3502868

Santosa, F. (2024). Transformation of Record Keeping: Development of E-Archive Applications Towards Modern Information Governance. *JOURNAL OF ICT APLICATIONS AND SYSTEM*, *3*(1), 1–8. https://doi.org/10.56313/jictas.v3i1.337

Sari, M. I., & Nasution, M. I. P. (2025). Optimalisasi Kinerja Sistem Informasi Manajemen Melalui Penerapan Database yang Efektif. *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, *2*(11).

Setiawan, U. S. M. A., Putra, P., & Syarif, V. D. P. (2025). Implementasi Aplikasi E-Arsip di Lingkungan SMAN 2 Mesuji Raya. *Journal of GLAM Terekam Jejak*, *1*(1), 105–113.

Setiyani, L. (2021). Desain sistem: use case diagram. *Prosiding Seminar Nasional Inovasi Dan Adopsi Teknologi (INOTEK)*, *1*(1), 246–260.

Siswaya, S., & Setiawan, A. (2025). Perancangan Sistem Pengarsipan Surat Berbasis Web dengan Menggunakan Metode RAD dan Disposisi Surat. *Insect (Informatics and Security): Jurnal Teknik Informatika*, *11*(1), 127–137.

Supriadi, M., & Sa'uda, S. (2025). Pengembangan Dan Implementasi Sistem Informasi Pengarsipan Surat Berbasis Web Pada Bagian Kesra Kantor Walikota Palembang. *Jurnal Pengabdian Masyarakat Bangsa*, *3*(5), 2205–2217.

Suwintana, I. K., & Sudiadnyani, I. O. (2020). The development of information system for garments industry using the android platform. *Journal of Physics: Conference Series*, *1569*(2), 022007. https://doi.org/10.1088/1742-6596/1569/2/022007

Taresh Mehra. (2024). The Critical Role of Role-Based Access Control (RBAC) in securing backup, recovery, and storage systems. *International Journal of Science and Research Archive*, *13*(1), 1192–1194. https://doi.org/10.30574/ijsra.2024.13.1.1733

Wirapraja, A., & Kardinata, E. A. (2025). Design of Web-Based Motor Vehicle Spare Parts Sales Application Using the Rapid Application Development (RAD) Method. *Indonesian Journal of Information Systems*, *8*(1), 103–116. https://doi.org/10.24002/ijis.v8i1.11206

Чечет, А. С., Черних, М. В., Панасюк, Я. С., & Абдуллін, І. І. (2024). FRONT-END SECURITY ARCHITECTURE: PROTECTION OF USER DATA AND PRIVACY. *Systems and Technologies*, *68*(2), 102–111. https://doi.org/10.32782/2521-6643-2024-2-68.12