CENTIVE
Conference on Electrical Engineering, Informatics
, Industrial Technology, and Creative Media
ISBN : 978-602-53004-0-0

Integrating Supervisor Access Using Hybrid RBAC-ABAC In A Web-Based Research Permit Information System

A Case Study At Dr. Moewardi General Hospital

Santyana Rahmawati[1*], Hanifah Permatasari[2], and Intan Okaviani[3]
[1,2,3]Faculty of Computer Science, Duta Bangsa University
[1,2,3]Jl. Bhayangkara No. 55, Tipes, Kec. Serengan, Surakarta, Jawa Tengah, 57154, Indonesia
[*]230101092@mhs.udb.ac.id

Abstract — The increasing demand for research activities in hospitas requires a secure, reliable and efficient information system to manage research permit applications. In many healthcare institutions, supervisory teams, play a crucial role in monitoring research activities to ensure compliance with institusional policies and ethical standards. This study presents the integration of supervisory team access into the existing web-based Research Permit Information System at Dr. Moewardi General Hospital. The integration is designed to enable the supervisory team to directly access and review research data through the system with access control aligned by hospital's organizational hierarchy and regulations. To enhancing security and handling some access scenarios, a hybrid access control model combining Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) is implemented. RBAC is used to define role-specific permissions for different supervisory levels, ensuring consistent enforcement of access boundaries. ABAC complements this by allowing more granular, attribute-driven policies that improve adaptibility to dynamic and context-specific access requirements. The proposed hybrid model strengthens system security and increase flexibility in access management for various supervisory role. This approach demonstrates a practical and scalable solution for integrating multiple access control mechanism in a healthcare research context.

Keywords – Access control, RBAC, ABAC, Hybrid model, Research permit system, Healthcare information system.

I. INTRODUCTION

In recent years, the increasing number of research activities conducted in hospitals has created a pressing demand for secure, efficient, and well-structured information systems to manage research permit applications [1]. Effective supervision is essential to ensure compliance with institutional regulations, maintain research quality, and safeguard patient safety, particularly in teaching hospitals where research activities form an integral part of both clinical practice and academic development [2].

Dr. Moewardi General Hospital, a Class A teaching hospital owned by the Provincial Government of Central Java, has developed a web-based Research Permit Information System to facilitate the submission, verification, and recording of research permits in an efficient and transparent manner [3]. According to the hospital's Education and Research Department performance report, research activities increased by an average of nearly 28% annually from 2021 to 2024, highlighting the need for a more structured supervision mechanism [1]. However, the current system does not provide dedicated access for supervisory teams, which consist of department heads, installation heads, and unit heads. This limitation restricts direct monitoring of research activities within their respective units, potentially delaying the detection of protocol violations, ethical deviations, or patient safety risks [2].

To address these challenges, this study proposes integrating supervisory team access into the existing system using a hybrid Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) model. RBAC provides role-specific permissions aligned with organizational hierarchy [4], while ABAC enables more granular, attribute-driven policies, such as those based on research permit status or unit location [5]. This combination enhances adaptability to dynamic cases and strengthens data security by addressing the limitations of traditional access control models [6].

Several previous studies have explored RBAC and ABAC implementations in various domains. Yuricha and Phan applied RBAC in a cloud-based supply chain system to improve security, but did not incorporate attribute-based policies [7]. Prasetia and Manongga implemented centralized RBAC authorization effectively, yet lacked contextual flexibility [8]. Jadhav and Pise as well as Ameer et al. investigated ABAC or hybrid RBAC–ABAC models in IoT and blockchain contexts [9], [10]. Aftab et al. identified hybrid models as an emerging trend, combining the strengths of both approaches, but noted limited application in hospital-based research supervision systems [11].

The novelty of this study lies in the explicit integration of supervisory roles into a web-based research permit information system through the application of a hybrid RBAC–ABAC model. Previous studies have explored access control approaches in domains such as cloud computing, IoT, and blockchain, focusing primarily on security and flexibility, but they have not specifically addressed the context of hospital research governance. In many hospital information systems, supervisory roles remain underrepresented, leading to limited oversight, delayed detection of protocol deviations, and risks to data integrity and patient safety. This study addresses that research gap by designing and implementing an information system that integrates supervisory access in a way that aligns with organizational hierarchy (RBAC) while also adapting to contextual attributes such as research location and permit status (ABAC). By doing so, the proposed model provides a practical and adaptive framework that ensures secure, regulation-compliant supervision while enhancing accountability, transparency, and effectiveness of research oversight. Ultimately, this contribution demonstrates how hybrid access control can be leveraged to improve governance in healthcare research information systems, a domain that has not been adequately explored in prior work.

II. RESEARCH METHOD

This study followed a structured methodology consisting of four main stages:

a) Problem Identification. It began with identifying the limitedness of supervisory access in the existing data research on Research Permit Information System at Dr Moewardi General Hospital, which hindered the process of research monitoring.
b) Data Collection and Requirement Analysis. Data were collected throug interviews and by reviewing existing regulations. The analysis highlighted the need for two additional access role: Supervisor: their access to data is read-only, related to their unit and hierarchy. And Superadmin: full access to manage user (specifically the supervisory teams) and research datas.
c) System Design. In this stage of study, it includes the UML Use Case Diagrams, UML Class Diagram, and Database Relationship Schemas that used as references in system development. RBAC and ABAC policies are established, with RBAC controlling role permissions and ABAC adding contextual constraints based on attributes such as research status and the unit that is used as a location of the research.
d) Implementation. The features were implemented into the existing web-based system using the CodeIgniter framework and for the relational database management system, it is using MySQL.

The scope of this study focuses solely on access control feature development and does not include performance benchmarking or comprehensive user evaluation.

III. RESULT

System Requirement Analysis

The requirements analysis was conducted through interviews with the Education and Research Department of Dr. Moewardi General Hospital, a review of Ministry of Health regulations on hospital research governance, and direct observation of the existing web-based Research Permit Information System. The findings indicated that the system did not provide a dedicated access control mechanism for the supervisory team, limiting their ability to monitor research activities in real time. All administrative functions were handled by the same level of system administrators, without hierarchical separation for supervisory roles.

Further analysis revealed that the current system lacked several essential capabilities. There was no restriction of research data visibility based on the supervisor's unit, meaning supervisors could not directly view activities relevant only to their area of responsibility. These limitations contributed to delayed detection of protocol deviations, ethical non-compliance, or potential risks to patient safety.

Based on these findings, two new roles were defined to enhance the system's access management:

a) **Supervisor**, with read-only access to research data within their assigned unit; and
b) **Superadmin**, with full privileges to manage users, research data, and surveillance area for the supervisory team.

The implementation of these roles was supported by a hybrid RBAC–ABAC model, in which RBAC assigned permissions according to organizational hierarchy, and ABAC applied additional attributebased filters such as research permit status and unit affiliation.

System Implementation

Clear documentation of system design is necessary to ensure effective development. Therefore, Use Case Diagrams, Class Diagram, and Database documentation, including Table Design Scheme and Relational Table Structure were created as references for the system development process. These documents serve as working guidelines for developers and system analyst to ensure that the system operates according to the defined requirements and can be further enhanced as needed.

a) Flow Chart System
The flowchart as figured in Fig. 1 illustrated login process in the Research Permit Information System at Dr. Moewardi General Hospital. The process begins with the user entering a username and password on the login page. The system validates the form input, if any required field is empty or invalid, an error message will be displayed. If the input passes validation, the system verifies the credentials against the AUTH table. Upon successful authentication, the user is redirected to page based on their assigned role. In this study, the development focused on adding two new role i.e: **Supervisor** and **Superadmin**.

b) Usecase Diagram
The use case diagram in Fig. 2 illustrates the new role. The Supervisor actor, upon successful login, is directed to the Supervisor Dashboard, which provides read-only access to the Research Dashboard. From this interface, supervisors can view research data filtered according to their assigned monitoring area. This restriction ensures that supervisors can perform monitoring tasks effectively without altering existing records and within the scope defined by the organizational hierarchy.
The Superadmin actor, after login, can access the Supervisor Management Dashboard to perform Create, Read, Update and Delete (CRUD) operations on supervisor accounts and define specific monitoring areas. In addition, the superadmin has full access to the Research Dashboard, enabling the ability to read, update, and delete research data across all units.

c) UML Class Diagram
The UML Class Diagram in Fig. 3 illustrate the existing entity and class structure on the development system. Each Research may involve several Unit and is supervised by one or more Supervisors, who associated with their respective posisition according to organizational hierarchy on RSUD Dr Moewardi. User authentication is managed through the Auth entity, which store login credential and role information.

d) Relational Table Structure
In this Fig. 4 bellow, the relational table schema is the result of the representation of the previously designed Class Diagram. It is translating conceptual entitites into database table.

e) User Interface
Figure 5 shows the login page of the Research Permit Information System at Dr. Moewardi General Hospital. This page is accessible to all registered users and required username and password to login in to system. The system will validating input form to ensure all fields are filled correctly. If validation fails, an error will be displayed. Once validated, the credentials are checked against the database. Upon successful authentication, the system will redirecting the user to the appropriate page based on their assigned role, ensuring that each role, such as researcher, supervisor, research admin or superadmin, has access privileges consistent with its responsibilities.
After user successfully logs in, if the role is supervisor, the system redirects the user to the supervisor dashboard page, as shown in Fig. 6. In this page, the top section summarizes key indicators, including the total number of research titles under the supervisor's surveillance unit, the number of active research, and the number of surveillance areas assigned to the supervisor. Below this summary, research data are displayed in a data tables, filtered according to the supervisor's organizational position and assigned surveillance area as defined in the database. This mechanism ensures that supervisors can only view research records within their scope of authority, consistent with their role in the organizational hierarchy.
When a supervisor accesses the detail of a research title, the system redirects the user to the Research Detail Page, as shown in Fig. 7. At this stage, the system reads the role_id of the logged-in user. If the user is identified as a supervisor, the page automatically applies access restrictions, allowing the user to view the research information in a read-only mode. This ensures that supervisors can perform monitoring functions effectively without the ability to alter or modify the research data, thereby maintaining data integrity and compliance with the organizational access control policies.
Figure 8 illustrates the Supervisor Management Dashboard, which is accessible only to the Superadmin role. On this page, the superadmin can view a list of supervisors along with their details, such as name, position, organizational unit, and associated username. The dashboard provides full CRUD (Create, Read, Update, Delete) functionality, including options to add new supervisors, update existing records, reset user credentials, and delete supervisor accounts if necessary. This capability ensures that supervisory accounts are

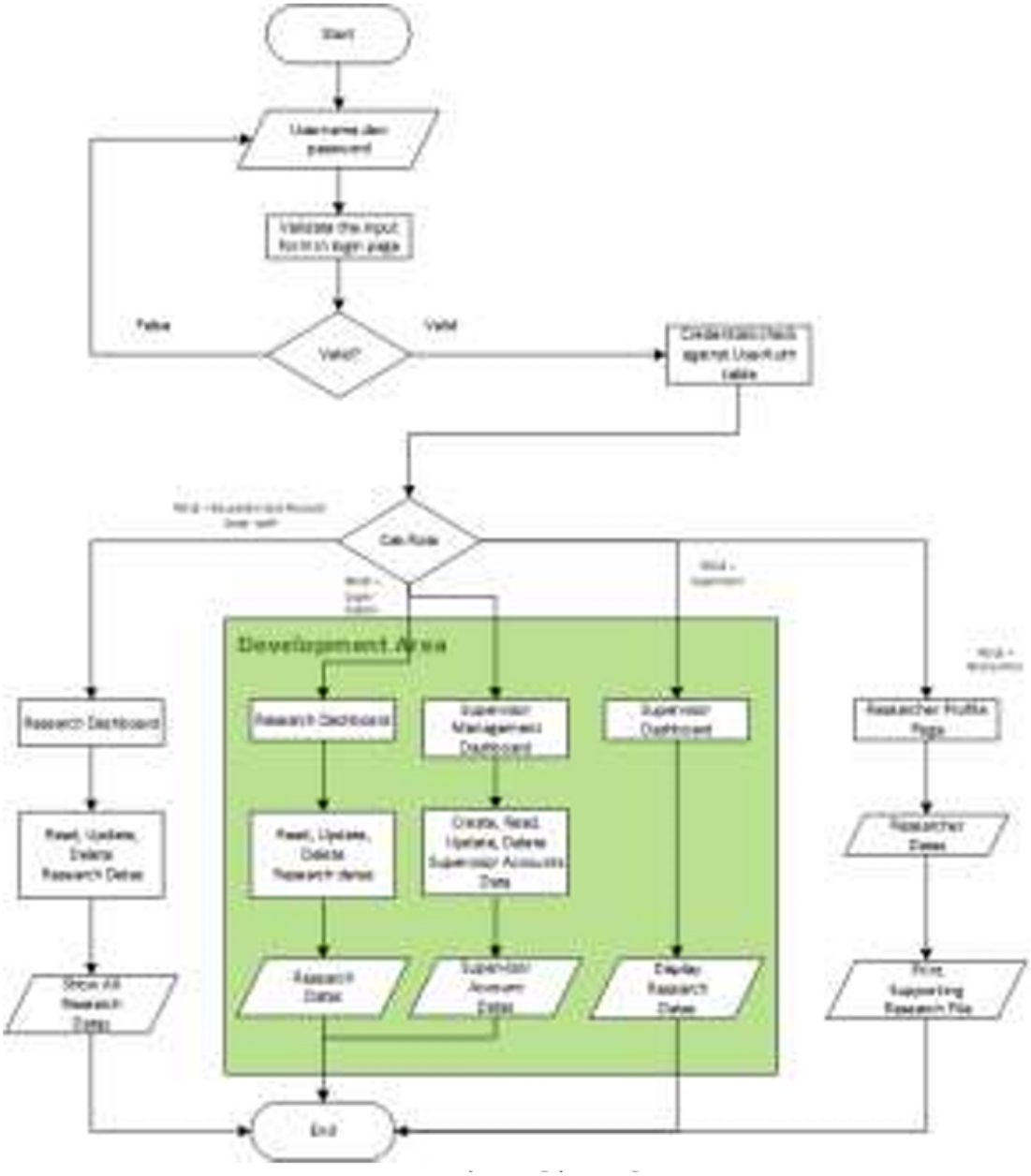

Fig. 1. Flow Chart System.

centrally managed and aligned with the organizational hierarchy, thereby maintaining proper authorization flow within the Research Permit Information System.

Figure 9 shows the page for adding a new supervisor, which is accessible to the superadmin role. This interface allows the superadmin to register a new supervisor by defining attributes such as position, organizational unit, username, and password. The form ensures that all required information is entered correctly before submission. By enabling centralized creation of supervisory accounts, this feature enhances access governance and also supports the implementation of hybrid RBAC–ABAC policies in the system.

As shown in Fig. 10, this page is the research dashboard that accessible to the superadmin role. This page presents a summary of research data through visualizations and data table displays. It has internal research data using pie chart, and external research data that was presented using trend chart monthly in a year. In addition, a main data table is provided to list all research titles, equipped with a search feature to facilitate quick data retrieval. From this page, the superadmin can also navigate directly to the Research Dashboard and Supervisor Management modules using the available navigation buttons, ensuring efficient oversight and comprehensive data management.

As shown in Fig. 11, research detail page for superadmin role has difference to supervisor role. Unlike the supervisor role, which is restricted to

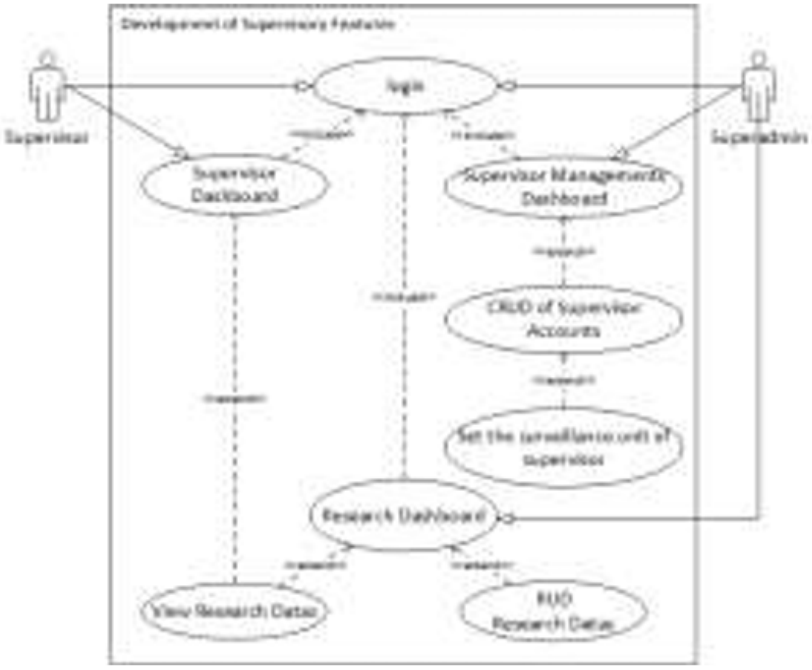

Fig. 2. Use Case Diagrams.

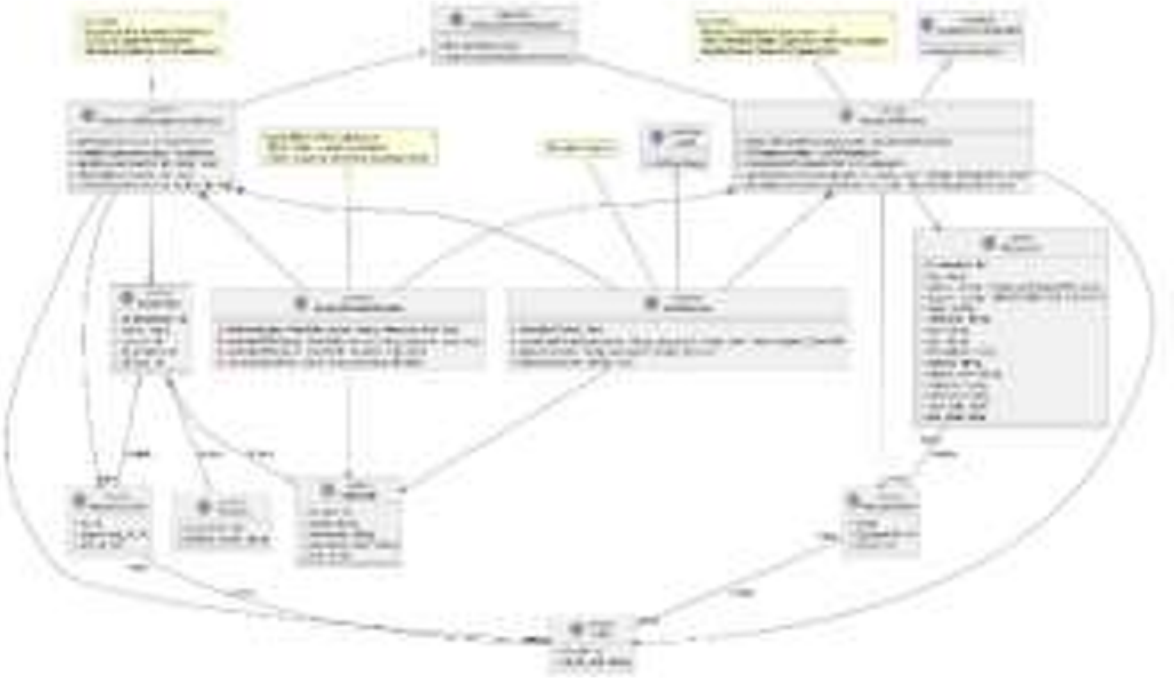

Fig. 3. UML Class Diagram.

readonly access, the superadmin is granted full privileges to manage research records. On this page, the superadmin can view complete details of a research, including researcher identity, institutional affiliation, proposal documents, research objectives, and ethical approval information. In addition to viewing, the superadmin can perform CRUD (Create, Read, Update, Delete) operations, ensuring centralized control over research data. This capability allows for data correction, validation, or removal when necessary, thereby maintaining the accuracy, integrity, and compliance of the research information stored in the system.

System Testing

To ensure that the implemented system functions according to the specified requirements, a series of functional tests were conducted using the Blackbox Testing approach. This method focuses on evaluating the system's behavior by providing input and observing the corresponding output, without considering the internal program logic. Blackbox testing is particularly

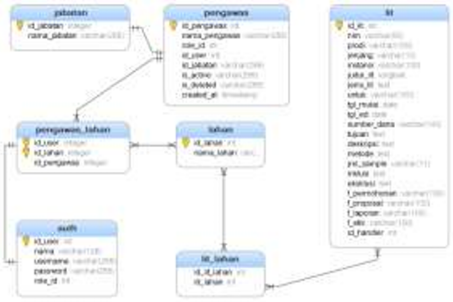

Fig. 4. Relational Table Structure.

Fig. 5. Login Page.

Fig. 6. Supervisor Dashboard Page.

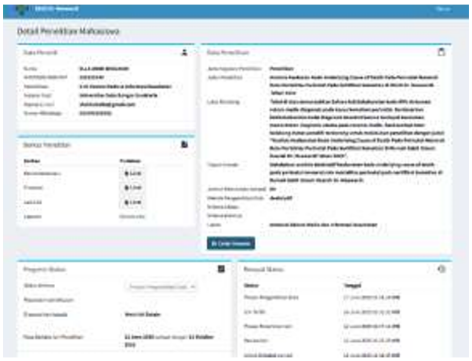

Fig. 7. Research Detail Page for Supervisor Role.

suitable for validating whether the features of the Research Permit Information System, such as login, user management, and access restrictions, operate correctly and meet user expectations.

The test cases were designed based on the main modules of the system. The results of testing demonstrate whether the implemented hybrid RBACABAC access control mechanism successfully enforces role-based and attribute-based restrictions in practice. Thefollowing table presents several test cases and their outcomes as part of the Blackbox Testing evaluation.

All functional tests were conducted using the Black-box Testing approach to verify that the Superadmin Dashboard and Supervisor Management features perform correctly according to system requirements. The results confirm that the Superadmin can fully manage supervisor data creating, editing, and deleting records consistent with the role privileges defined in the hybrid RBAC–ABAC access control model.

IV. DISCUSSION

Interpretation of Results

The integration of the Supervisor and Super Administrator roles into the Research Permit Information System is a practical step to strengthen governance and ensure compliance in hospital-based research management. Previously, oversight of research activities relied heavily on manual reports prepared by administrative staff, a process prone to delays, incomplete information, and weak monitoring mechanisms. This reliance often led to ineffective oversight and non-compliance with applicable regulations. With the introduction of two additional user roles, supported by attribute-based restrictions and unit-based authority assignments, the system now provides a structured framework that significantly improves data security and oversight reliability.

The Supervisor role is designed as a read-only role with limited access to menus and research data within designated monitoring areas, as defined in the hospital's organizational hierarchy. This ensures that supervisors can monitor research activities relevant to their responsibilities without the ability to alter or manipulate existing data. By limiting supervisors to non-editable scopes, the system maintains the integrity of research data and empowers supervisors to carry out their duties more effectively and in accordance with the institution's governance structure. This separation of responsibilities also reduces the potential for conflicts of interest by ensuring that monitoring activities are conducted independently of administrative functions.

In contrast, the superadmin role serves as a centralized authority with full access to all user accounts and research data. This role is responsible for managing supervisor accounts, configuring monitoring areas, and performing CRUD (Create, Read, Update, Delete) operations on research data. By granting comprehensive privileges to superadmins, the system ensures a clear locus of responsibility for maintaining overall data

Fig. 8. Superadmin, Supervisor Management Dashboard.

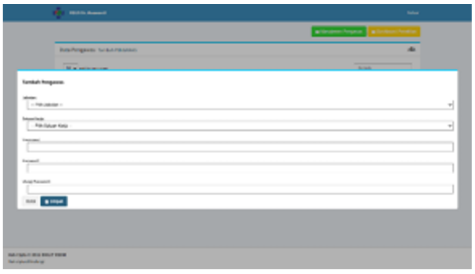

Fig. 9. Adding New Supervisor Page for Superadmin role.

integrity and enforcing access policies. The integration of these two roles creates a layered governance model in which authority and accountability are clearly distributed: supervisors oversee research activities within their scope, while superadmins maintain control across the system. This balance strengthens organizational accountability, reduces the risks associated with unfettered access, and improves compliance with healthcare research regulations.

More broadly, the integration of these roles reflects a shift from reactive oversight to proactive monitoring in research governance. Instead of waiting for administrative summaries or periodic reports, supervisors can now directly access real-time data filtered through RBAC and ABAC policies, enabling faster detection of potential issues such as protocol deviations or risks to patient safety. At the same time, superadmins can intervene when necessary to correct or validate data, ensuring responsiveness and accuracy in decision-making. Overall, these results demonstrate how role differentiation and hybrid access controls can transform research governance into a system that is not only more secure, but also more transparent, efficient, and aligned with hospital regulatory obligations.

To validate the functionality of the implemented system, a series of Blackbox Testing scenarios were conducted on four main modules: Login, Supervisor Dashboard, Research Detail, and Superadmin Dashboard. The tests aimed to ensure that each feature operates according to the defined functionalspecifications and access control policies. Table bellow summarizes the test results across all modules.

The results show that all test cases passed successfully, confirming that the system's functional and access control requirements were fully met. These outcomes demonstrate that the hybrid RBAC–ABAC model was correctly implemented and effectively enforced in the Research Permit Information System.

Fig. 10. Research Dashboard Page for Superadmin Role.

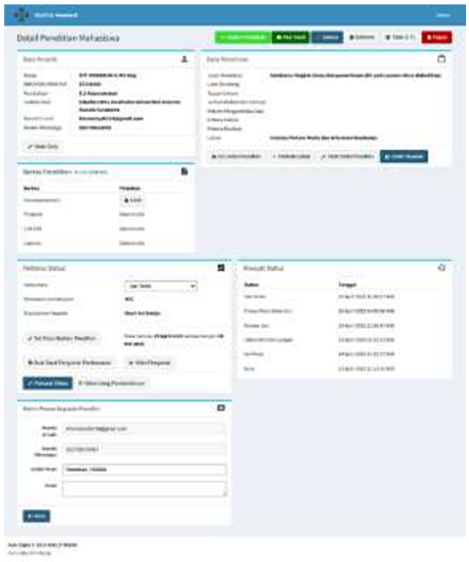

Fig. 11. Research Detail Full Access for Superadmin Role.

Advantages of the Hybrid Model

The implementation of the hybrid RBAC–ABAC model produced several key advantages:

a) Enhanced Security Unauthorized access is prevented by combining static roles with dynamic attribu te checks, ensuring that even authorized users cannot bypass restrictions outside their scope.
b) Operational Efficiency Supervisors no longer rely on secondar y reports; instead, they can directly access filtered data in real time, which shortens the monitoring cycle.
c) Flexibility of Policies RBAC roles, making it easier to adapt policies when hospital regulations change.
d) Transparency and Accountability Supervisors' read-only access provides transparency while preserving data integrity, and all Superadmin activities can be logged for audit purposes.

Limitations of the Study

Despite the benefits, several limitations remain. First, no performance benchmarking was conducted to measure how hybrid policy enforcement affects system speed and scalability under heavy loads. Second, user acceptance testing (UAT) was not performed with ac-

Table 1. Test Case Login

No	Test Case: Login		
	Test Case Title	*Expected Result*	*Pass/Fail*
1	**Successful Login (Superadmin)** **Precondition:** Superadmin account is active **Steps:** 1. Open /login 2. Enter valid credentials 3. Click Submit	Redirects to Superadmin Dashboard	Passed
2	**Successful Login (Supervisor)** **Precondition:** Supervisor account for Area A is active **Steps:** 1. Open /login 2. Enter valid supervisor credentials 3. Click Submit	Redirects to Supervisor Dashboard	Passed
3	**Form Validation (Empty Field)** **Precondition:** Login page is available **Steps:** Submit form with empty username or password field	Displays validation message for the corresponding field	Passed
4	**Incorrect Password - Login Failed** **Precondition:** Registered user account exists **Steps:** 1. Enter valid username and incorrect password 2. Click Submit	Displays generic error message: "Invalid username or password"	Passed
5	**Logout** **Precondition:** User is logged in **Steps:** Click Logout	Session is cleared and redirected to login page	Passed

Table 2. Test Case Supervisor Dashboard

No	Test Case: Supervisor Dashboard		
	Test Case Title	*Expected Result*	*Pass/Fail*
1	**Redirect and Dashboard Access** **Precondition:** Logged in as Supervisor **Steps:** 1. Log in using Supervisor account 2. Access Supervisor Dashboard page	Supervisor Dashboard page is displayed successfully	Passed
2	**Summary of Active and Total Research** **Precondition:** Research data exists in the database **Steps:** 1. Open Supervisor Dashboard 2. Observe the summary section	Summary values are displayed correctly according to database query results	Passed
3	**Research Table Display** **Precondition:** Research data is stored in the database **Steps:** 1. Open Supervisor Dashboard 2. Verify that the research table is visible on the dashboard home page	Columns (title, researcher, status, and period) are displayed correctly	Passed
4	**Open Research Details** **Precondition:** A research record with ID X exists in the supervisor's area **Steps:** 1. Click on the research title in the table 2. System redirects to the research detail page	Redirects to the detail page of research ID X and displays the correct data	
5	**RBAC Area Filtering** Precondition: Supervisor's monitoring area has been configured **Steps:** 1. Open Supervisor Dashboard 2. Observe the research list displayed	Only research within the supervisor's authorized area is shown	Passed
6	**Search Function** **Precondition:** Search feature is available **Steps:** 1. Enter a keyword into the search box 2. Observe the filtered table results	The research table is filtered according to the search keyword	Passed

tual supervisors and administrators, meaning usability and satisfaction levels are not yet validated. Third, the ABAC attributes currently implemented are limited to research location and permit status, leaving out more advanced attributes such as sensitivity levels, login time, and geolocation. Addressing these limitations will be essential to ensure broader adoption and long-term sustainability.

Future Work

Future research should focus on expanding the attribute set in ABAC policies. For example, integrating time-based constraints would allow supervisors to access data only during working hours, while sensitivity-based filtering could restrict certain types of high-risk research data. In addition, performance evaluations should be carried out using stress testing to determine how the hybrid model performs in large-scale deployments. Usability studies involving supervisors and administrators are also recommended to ensure that the system is not only secure but also user-friendly.

Furthermore, this approach can be extended to other hospital information systems beyond research permits, such as electronic medical records (EMR) or clinical trial management systems. By integrating access control across multiple systems, hospitals can establish a comprehensive and unified governance framework, enhancing both operational efficiency and compliance with healthcare regulations.

V. CONCLUSSION

This study successfully integrating supervisor access into a web-based research permit information system at RSUD Dr Moewardi General Hospital using a hybrid RBAC-ABAC Model. In this development, it is adding new roles: Supervisor and Superadmin,

Table 3. Test Case: Research Detail for Supervisor and Superadmin Roles

No	Test Case: Research Detail for Supervisor and Superadmin Roles		
	Test Case Title	*Expected Result*	*Pass/Fail*
1	**Complete Detail Display (Supervisor)** **Precondition:** Logged in as Supervisor for Area A; research with ID Y belongs to Area A **Steps:** 1. Access research detail page with ID Y 2. Observe the displayed data	All main research fields are displayed completely and correctly	Passed
2	**Navigation and Related Links (Supervisor)** **Precondition:** Research detail page is open **Steps:** 1. Click "Back" button or related navigation links 2. Observe navigation behavior	Navigation and links function correctly without errors	Passed
3	**Full Access to Research Detail (Superadmin)** **Precondition:** Logged in as Superadmin **Steps:** 1. Access any research detail page via /research/detail/id 2. Observe the displayed data	All research details are fully visible for any record	Passed

Table 4. Superadmin Dashboard & Supervisor Management

No	Test Case: Superadmin Dashboard & Supervisor Management		
	Test Case Title	*Expected Result*	*Pass/Fail*
1	**Redirect and Dashboard Access (Superadmin)** **Precondition:** Logged in as Superadmin **Steps:** 1. Log in using Superadmin account 2. Access Superadmin Dashboard page 3. Observe displayed content	Upon successful login, user is redirected to the Supervisor Management Dashboard page. Buttons to access the Research Dashboard and Supervisor Management are visible and functional.	Passed
2	**Create New Supervisor** **Precondition:** Logged in as Superadmin **Steps:** 1. Open Create Supervisor form 2. Fill in all fields with valid data 3. Click Submit	New supervisor record is successfully saved and redirected to the Supervisor Management Dashboard.	Passed
3	**Edit Supervisor Data** **Precondition:** Supervisor record exists in the database **Steps:** 1. Open Edit page for existing supervisor 2. Modify one or more valid fields 3. Click Save	Data changes are saved successfully and updated in the database.	Passed
4	**Delete Supervisor** **Precondition:** Supervisor record exists in the database **Steps:** 1. Click Delete button for the selected supervisor 2. Confirm the deletion 3. Observe the result	Selected supervisor record is successfully deleted from the database.	Passes

that provide role-specific permissions combined with attribute-based restrictions. The results demonstrated that this approach enhances security, align authority according to organizational hierarchy, and increasing flexibility in managing research surveillance.

This study provides a practical reference, particularly in health research governance systems at hospitals through an adaptive and secure access management framework. Future research is needed to further improve system performance and adaptability. Further research is needed regarding the addition of other broader attributes in the implementation of ABAC policies. In addition, it is important to conduct User Acceptance Testing (UAT) to assess the level of system usability and ensure the system is in accordance with the needs of stakeholders. These steps will support the broader goal of comprehensive hospital information systems integration and strengthening research oversight mechanisms that are more sustainable, secure, and accountable in the healthcare environment.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Education and Research Department of Dr. Moewardi General Hospital for granting permission to conduct this study. The authors also extend their appreciation to the Faculty of Computer Science, Duta Bangsa Univcersity Surakarta, for its continuous support and for providing the academix environment that enabled the successful completion of this paper.

REFERENCES

[1] Kepala Bagian Pendidikan dan Penelitian, "Laporan kinerja bagian pendidikan dan penelitian," n.d.

[2] Kementerian Kesehatan Republik Indonesia, "Keputusan menteri kesehatan republik indonesia tentang penyelenggaraan penelitian klinik di rumah sakit." https://ina-crr.id/, 2023.

[3] "Inovasi sistem informasi perizinan penelitian melalui web moewardi (sirian lemoe) di rumah sakit umum daerah dr. moewardi," 2020.

[4] C. A. Gemawaty and Y. Yuliani, "Manajemen identitas dan akses dalam keamanan sistem informasi (pendekatan literature review)," *Jurnal Manajemen Informatika Jayakarta*, vol. 4, pp. 396–403, Sept. 2024.

[5] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," in *Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS)*, pp. 83–89, Jan. 2016.

[6] H. F. Atlam and Y. Yang, "Enhancing healthcare security: A unified rbac and abac risk-aware access control approach," *Future Internet*, vol. 17, p. 262, June 2025.

[7] Yuricha and I. K. Phan, "Penerapan role based access control dalam sistem supply chain management berbasis cloud," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, pp. 339–348, Nov. 2023.

[8] Y. A. Prasetia and D. Manongga, "Role based access control (rbac) untuk sistem otorisasi terpusat berbasis flask studi kasus pt. xyz," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, pp. 1768–1778, Nov. 2024.

[9] S. Ameer, J. Benson, and R. Sandhu, "Hybrid approaches (abac and rbac) toward secure access control in smart home iot," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, pp. 4032–4051, Sept. 2023.

[10] S. Jadhav and N. Pise, "Secure and transparent blockchain donations: An attribute-based access control (abac) framework for enhanced donor control," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, (Pune, India), IEEE, Oct. 2024.

[11] M. U. Aftab, Z. Qin, Zakria, S. Ali, P. Pirah, and J. Khan, "The evaluation and comparative analysis of role based access control and attribute based access control model," in *15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 35–39, July 2018.

VI. Appendix

Table 5. Summary of blackbox testing results for all modules

No	Module Test Case	Number Of Test Case	Test Focus	Expected Outcome	Result
1	Login Module	5	Validation of authentication process, session control, and error handling	All login, validation, and logout functions operate correctly according to specifications.	All Passed
2	Supervisor Dashboard Module	6	Access validation, data filtering by role and area (RBACABAC), and search functionality	Supervisor Dashboard correctly displays research data limited to assigned monitoring areas.	All Passed
3	Research Detail Module	3	Validation of detailed data display for Supervisor (read-only) and Superadmin (full access)	Research detail pages show accurate data according to user role permissions.	All Passed
4	Superadmin Dashboard & Supervisor Management Module	4	CRUD operations for Supervisor accounts and navigation between dashboards	Superadmin can create, edit, and delete supervisor records successfully.	All Passed