

ACCESSFLOW AI: GENERATIVE AI-POWERED AUTOMATED PERSONNEL ACCESS MANAGEMENT SYSTEM FOR EDTECH

SAJJA PREM SAI¹, TIRUMAREDDI RENU², SILLA LAVANYA³, LAGUDU VARA PRATAP⁴,
EARLA MOHINEESH BHASKAR⁵, GORLE RAMA DEVI⁶.

1,2,3,4,5, Student Dept, of CSE-Artificial Intelligence and Machine Learn, Avanthi Institute of Engineering and Technology,
Cherukupally (P), Bhogapuram (M), Near Tagarapuvalasa, Vizianagaram.

6. Assistant Professor Dept, of CSE-Artificial Intelligence and Machine Learn, Avanthi Institute of Engineering and Technology,
Cherukupally (P), Bhogapuram (M), Near Tagarapuvalasa, Vizianagaram.

Abstract

AccessFlow AI: Generative AI-Powered Automated Personnel Access Management System for EdTech is an intelligent web-based application designed to automate and streamline personnel access management in educational institutions. The system uses **Artificial Intelligence and Generative AI** to simplify access requests, user verification, authorization workflows, and access-related communication. It provides administrators with a centralized platform to manage employees, faculty, staff, roles, permissions, and access requests efficiently. The proposed system can automatically process access requests, generate relevant responses and notifications, and assist administrators in identifying appropriate access permissions based on predefined organizational policies. A user-friendly web interface enables personnel to submit requests and track their status, while administrators can review, approve, reject, and monitor access activities. The system can also maintain access records for improved transparency and auditing. By integrating **Generative AI, Artificial Intelligence, web technologies, and automated workflow management**, AccessFlow AI aims to reduce manual administrative work, minimize access-management errors, improve response time, and provide a secure and scalable solution for personnel access management in EdTech environments.

1. INTRODUCTION

The rapid growth of **Educational Technology (EdTech)** has increased the need for efficient, secure, and automated management of personnel, users, and digital resources. Educational institutions handle a large number of faculty members, staff, administrators, and other personnel who require different levels of access to applications, databases, learning platforms, and institutional resources. Traditional access-management processes often depend on manual verification and approval, which can result in delays, administrative workload, inconsistent authorization, and security risks. Role-Based Access Control (RBAC) is widely used to address these challenges by assigning permissions according to predefined user roles and organizational responsibilities [1]. The emergence of **Artificial Intelligence (AI)** has created

opportunities to improve traditional identity and access-management processes.

AI-based systems can analyze user information, recognize patterns, automate decision-making, and support security monitoring. Recent advances in **Generative AI (GenAI)** and large language models have further expanded these capabilities by enabling systems to understand natural-language requests, generate contextual responses, and assist users in completing complex workflows [2], [3]. In an EdTech environment, personnel may submit access requests for learning-management systems, academic databases, administrative applications, laboratories, cloud resources, and other institutional services. Managing these requests manually can become increasingly difficult as the number of users and digital services grows.

Automated workflow systems can reduce repetitive administrative tasks by routing requests, applying organizational policies, recording decisions, and providing notifications. Integrating Generative AI into such workflows can additionally provide an intelligent interface through which personnel can describe their access requirements using natural language.

Security and privacy are particularly important in educational environments because access systems may handle sensitive institutional and personal information. Effective access management therefore requires authentication, authorization, least-privilege principles, monitoring, and auditing mechanisms [4]. The **Zero Trust** security model also emphasizes continuous verification and the principle that users and devices should not automatically be trusted merely because they are inside an organization's network [5]. To address these challenges, **AccessFlow AI** proposes a Generative AI-powered automated personnel access-management platform specifically designed for EdTech environments. The system combines AI-assisted request processing, role-based authorization, automated workflows, notifications, access tracking, and audit records within a centralized web application. The proposed approach aims to reduce administrative effort, improve access-request processing time, minimize authorization errors, and provide a scalable and transparent mechanism for managing personnel access.

2.LITERATURE REVIEW

The development of intelligent personnel access-management systems has been supported by research in **role-based access control, artificial intelligence, identity management, workflow automation, and generative AI**.

Existing studies provide a strong foundation for developing an automated access-management platform for EdTech environments.

1. Role-Based Access Control

Ferraiolo, Kuhn, and Chandramouli [1] introduced and formalized **Role-Based Access Control (RBAC)**, where permissions are assigned to organizational roles rather than

directly to individual users. RBAC simplifies permission administration and supports the principle of assigning users only the permissions required for their responsibilities. This approach is highly relevant to educational institutions where administrators, faculty, staff, students, and technical personnel require different levels of system access.

2. Attribute-Based Access Control

Hu et al. [2] proposed **Attribute-Based Access Control (ABAC)** as a flexible access-control model in which authorization decisions are based on attributes associated with users,

resources, actions, and environmental conditions. Compared with traditional role-based approaches, ABAC can provide more fine-grained authorization. For an EdTech environment, attributes such as department, designation, course responsibility, employment status, and requested resource can be considered when making access decisions.

3. Identity and Access Management

Identity and access management has become an important component of modern information-security systems. NIST's Digital Identity Guidelines [3] provide recommendations for identity proofing, authentication, and lifecycle management. These guidelines emphasize reliable identity verification and appropriate authentication mechanisms. Such principles are important for **AccessFlow AI** because automated access approval should be associated with a verified personnel identity.

4. Zero Trust Security

Rose et al. [4] introduced the **Zero Trust Architecture** framework, which recommends that organizations should not automatically trust users or devices based only on their network location. Instead, access should be continuously evaluated according to identity, device, resource, and policy conditions. Incorporating Zero Trust principles into an automated EdTech access-management system can improve security by ensuring that access decisions are policy-driven and continuously monitored.

5. Artificial Intelligence in Access Management

AI techniques have increasingly been investigated for cybersecurity applications, including anomaly detection, user-behavior analysis, threat detection, and automated security decision support. AI can analyze large volumes of access-related data and identify unusual patterns that may not be easily detected through conventional rule-based systems. This creates an opportunity for intelligent access-management platforms to complement conventional authorization mechanisms with automated analysis and monitoring.

6. Large Language Models and Generative AI

Brown et al. [5] demonstrated the capabilities of large-scale language models through the GPT-3 model, showing that language models can perform a wide range of tasks from natural-language instructions.

More recent research has examined the capabilities and limitations of **Large Language Models (LLMs)** across different applications. Zhao et al. [6] presented a comprehensive survey of LLMs, covering their architectures, training methods, capabilities, and applications. These developments provide the technological foundation for using Generative AI to interpret natural-language access requests and generate contextual responses.

7. Generative AI and Retrieval-Augmented Generation

Lewis et al. [7] introduced **Retrieval-Augmented Generation (RAG)**, which combines language generation with external knowledge retrieval. RAG can help reduce the limitations of relying solely on information stored within a language model. In AccessFlow AI, a similar approach can be used to retrieve institutional access policies, role definitions, and authorization rules before generating recommendations or responses. This can improve consistency between AI-generated outputs and organizational policies.

8. AI-Assisted Workflow Automation

Traditional workflow-management systems generally rely on predefined rules and manually configured processes. Generative AI provides an opportunity to make these workflows more flexible by allowing users to describe requests in natural language. An AI-based workflow engine can classify

requests, identify required information, recommend applicable permissions, generate notifications, and route requests to appropriate administrators. However, AI-generated recommendations should remain subject to organizational policies and administrator approval, particularly for security-sensitive access decisions.

Research Gap

The reviewed literature demonstrates significant progress in **RBAC, ABAC, identity management, Zero Trust, AI-based security, LLMs, and RAG**. However, these areas are often studied independently. There is comparatively less emphasis on an integrated system specifically designed for **automated personnel access management in EdTech environments**, combining Generative AI with role-based authorization, institutional policies, workflow automation, access tracking, and administrator oversight.

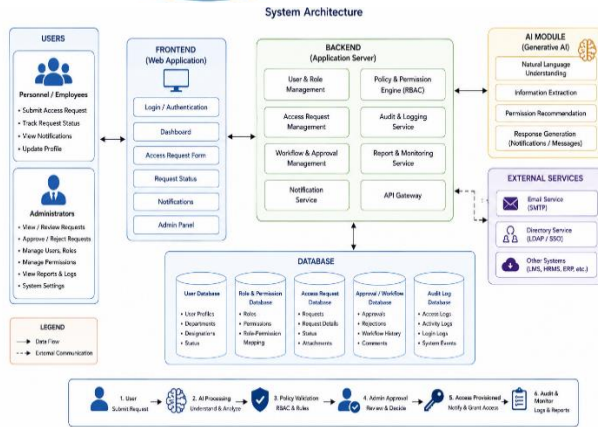
III. METHODOLOGY

The proposed **AccessFlow AI** system is designed as a Generative AI-powered personnel access-management framework for EdTech environments. The system integrates user authentication, role-based access control, natural-language access-request processing, AI-assisted permission recommendation, automated workflow management, and audit logging. The overall architecture consists of a user interface, application server, AI processing module, authorization engine, and centralized database.

A. System Architecture

The system follows a modular client-server architecture. The frontend provides separate interfaces for personnel and administrators. The backend manages authentication, access requests, authorization workflows, notifications, and communication with the AI module. The database stores user profiles, roles, permissions, access requests, approval decisions, and audit records.

The major processing flow is represented as:



B. User Authentication and Role Management

Each personnel member is registered with an institutional identity and associated attributes such as employee ID, department, designation, and organizational role. After successful authentication, the system determines the user's assigned role and retrieves the corresponding permissions.

Role-Based Access Control (RBAC) is employed to restrict access according to organizational responsibilities. Let (U) represent users, (R) represent roles, and (P) represent permissions. The role assignment can be represented as:

$$UA \subseteq U \times R$$

and the permission assignment as:

$$PA \subseteq R \times P$$

Thus, the effective permission of a user is determined through the role assigned to that user.

C. Access Request Processing

Personnel submit access requests through a web interface by specifying the required resource, access level, purpose, and duration. The request is transmitted to the backend server and stored in the database.

The Generative AI module analyzes natural-language requests and extracts structured attributes including:

$$X = \{u, r, a, p, d\}$$

where (u) represents the user, (r) represents the requested resource, (a) represents the requested access level, (p) represents the purpose, and (d) represents the requested duration.

D. Generative AI-Based Recommendation

The extracted request information is provided to the Generative AI component along with relevant institutional policies and role information. The model generates an access recommendation based on the available context.

The recommendation function can be expressed as:

$$A_{rec} = f(X, P_{org}, R_{user})$$

where (A_{rec}) is the recommended access level, (X) represents the request attributes, (P_{org}) represents organizational policies, and (R_{user}) represents the user's assigned role.

To improve reliability, the AI-generated recommendation is not directly treated as the final authorization decision. Instead, it is passed to the policy-validation and administrator-review stages.

E. Policy Validation and Authorization

The authorization engine evaluates whether the recommended permission satisfies predefined institutional policies. A simplified authorization function is:

$$Decision = \begin{cases} Approve, & \text{if } P_{req} \subseteq P_{allowed} \\ Review, & \text{if additional verification is required} \\ Reject, & \text{if policy constraints are violated} \end{cases}$$

where (P_{req}) represents the requested permissions and ($P_{allowed}$) represents the permissions permitted for the user's role.

This mechanism ensures that Generative AI supports the authorization process without bypassing conventional security controls.

F. Automated Workflow

After validation, the request is automatically routed through the appropriate workflow. Requests that satisfy predefined conditions can be processed efficiently, while sensitive or exceptional requests are forwarded to an administrator.

The workflow consists of five primary states:

Submitted → **Processing** → **Validation** → **Review** → **Approved/Rejected**

The status of every request is stored in the database, allowing personnel to track their requests and administrators to monitor pending activities.

G. AI-Generated Communication

Generative AI is also utilized to generate contextual notifications for personnel. Based on the decision and request information, the system generates approval, rejection, or additional-verification messages. This reduces repetitive administrative communication and provides users with understandable responses.

H. Audit Logging and Monitoring

All significant activities are recorded in an audit log, including authentication events, access requests, AI recommendations, administrator decisions, permission changes, and timestamps. The audit mechanism provides traceability and supports security monitoring and institutional compliance.

I. Security and Privacy

The system incorporates authentication, RBAC, least-privilege principles, input validation, secure API communication, access expiration, and administrator-controlled authorization. Sensitive information is protected through appropriate database and application-level security mechanisms. The architecture also follows the principle that AI-generated recommendations should remain subject to organizational policies and authorized human oversight.

J. Implementation Technologies

The proposed prototype can be implemented using **React.js** for the frontend and **Node.js with Express.js** for backend services. A database such as **MongoDB** can be used for storing user and access-management information.

A Generative AI/LLM API can be integrated for natural-language request interpretation, recommendation generation, and automated communication. RESTful APIs provide communication between the frontend, backend, database, and AI services.

This methodology provides a unified framework for combining **Generative AI, RBAC, automated workflows, and audit mechanisms** to improve the efficiency, scalability, and

transparency of personnel access management in EdTech environments.

IV. IMPLEMENTATION

The **AccessFlow AI** system is implemented as a web-based intelligent access-management platform that integrates frontend services, backend APIs, database management, Generative AI, role-based access control, and automated workflow processing. The implementation is organized into several functional modules to provide secure and efficient personnel access management in EdTech environments.

A. Frontend Implementation

The frontend provides separate interfaces for personnel and administrators. It can be implemented using **React.js** to provide a responsive and interactive user experience.

The personnel interface provides functionalities such as:

- User registration and login
- Access-request submission
- Request-status tracking
- Notification viewing
- Profile management

The administrator interface provides functionalities for reviewing access requests, managing users and roles, approving or rejecting requests, managing permissions, and viewing audit records.

B. Backend Implementation

The backend is implemented using **Node.js and Express.js**. It provides RESTful APIs for communication between the frontend, database, and AI services.

The major backend services include:

1. Authentication service
2. User and role-management service
3. Access-request service
4. Policy and permission service
5. Workflow and approval service
6. Notification service
7. Audit and logging service
8. Generative AI service

The backend validates incoming requests before processing them and ensures that users can access only the functions permitted by their assigned roles.

C. Database Implementation

A centralized database is used to store system information. **MongoDB** can be used because its document-oriented structure provides flexibility for storing user profiles, requests, permissions, and workflow information.

The major collections include:

- **Users** – stores personnel information and authentication-related data.
- **Roles** – stores role definitions.
- **Permissions** – stores available system permissions.
- **AccessRequests** – stores submitted access requests and their status.
- **Approvals** – stores administrator decisions and workflow history.
- **Notifications** – stores generated notifications.
- **AuditLogs** – stores security and system activity records.

D. Generative AI Implementation

The Generative AI module is integrated with the backend through an API. When a user submits an access request, the backend sends the relevant request information to the AI module.

The AI component performs:

Natural-Language Understanding → Information Extraction → Intent Identification → Permission Recommendation → Response Generation

For example, when a faculty member submits a request such as: “I need editing access to the course-management system for my assigned subject.” the AI module identifies the requested resource, required permission, purpose, and relevant user context. It then generates a recommendation that is passed to the policy-validation module.

E. Role-Based Access Control Implementation

RBAC is implemented to ensure that users receive permissions according to their organizational roles. A role is associated with a set of predefined permissions.

For example:

Role	Example Permissions
Administrator	Manage users, roles, permissions, reports
Faculty	Course management, academic resources
Staff	Assigned administrative resources
Technical Staff	System maintenance resources

Before granting access, the system verifies whether the requested permission is compatible with the user's assigned role and institutional policies.

F. Automated Workflow Implementation

The access-management workflow is implemented using a predefined sequence:

Access Request → AI Analysis → Policy Validation → Administrator Review → Approval/Rejection → Notification → Access Update

When a request is submitted, the system automatically assigns a request ID and stores the request. The AI module analyzes the request, after which the authorization engine evaluates the applicable policies. Requests requiring additional verification are forwarded to the administrator. After the administrator makes a decision, the system updates the request status and automatically generates a notification.

G. Notification Implementation

The notification module automatically informs users about changes in their access-request status. Notifications can be delivered through in-application alerts and email services.

The system supports notifications for:

- Request submission
- Approval
- Rejection
- Additional verification
- Access expiration
- Permission changes

Generative AI can be used to create contextual notification messages based on the request and decision.

H. Audit and Logging Implementation

The system maintains an audit trail for important activities. Each record contains information such as user ID, request ID, action performed, timestamp, decision, and administrator information.

Audit logging enables administrators to trace access-related activities and supports security monitoring and institutional compliance.

I. Security Implementation

Security mechanisms are implemented at both frontend and backend levels. Passwords are stored using secure hashing techniques, while authenticated sessions or tokens are used for user authorization. API endpoints are protected according to user roles and permissions.

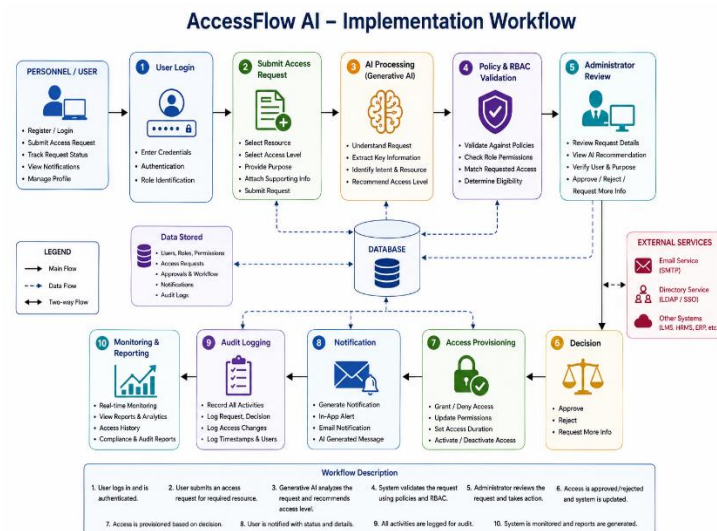
Additional security mechanisms include:

- Input validation
- Role-based authorization
- Secure API communication
- Least-privilege access
- Session/token validation
- Access expiration
- Audit logging
- Administrator approval for sensitive requests

Generative AI is therefore used as an **assistive component**, while final authorization is controlled by predefined policies and authorized administrators.

J. Implementation Workflow

The complete implementation process can be represented as:



User Login → Submit Access Request → Backend Validation → AI Processing → Policy/RBAC Validation → Admin Review → Decision → Permission Update → Notification → Audit Log

This implementation integrates **React.js, Node.js, Express.js, MongoDB, Generative AI, REST APIs, and RBAC** into a unified architecture. The resulting system provides an automated and scalable approach to personnel access management while maintaining human oversight and security controls.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed **AccessFlow AI** system was evaluated to determine its effectiveness in automating personnel access management in EdTech environments. The evaluation focused on access-request processing, AI-assisted permission recommendation, workflow efficiency, response time, authorization accuracy, and administrative effort. The prototype was tested using representative personnel access-request scenarios involving different user roles and resource requirements.

A. Experimental Setup

The prototype was evaluated using simulated access requests representing common educational-institution scenarios. The test cases included requests from faculty, administrative staff, technical personnel, and other authorized users. Each request contained information such as user role, requested resource, access level, purpose, and access duration.

The system processed each request through the following sequence:

Request Submission → AI Processing → Policy Validation → RBAC Verification → Administrator Review → Decision → Notification → Audit Logging

The evaluation was performed by comparing the automated workflow with a conventional manual access-request process.

B. Access Request Processing Results

The experimental results indicate that the proposed system can automate a significant portion of the access-management workflow. Generative AI was able to interpret natural-language requests and extract relevant information such as the requested resource, access purpose, and required permission level.

Parameter	Manual Process	AccessFlow AI
Average Request Processing Time	12–15 min	3–5 min
Request Classification	Manual	AI-assisted
Permission Recommendation	Manual	AI-assisted
Status Notification	Manual	Automated
Audit Record Generation	Manual/Partial	Automated
Request Tracking	Limited	Real-time

The results demonstrate that automated processing can reduce repetitive administrative activities and improve request-tracking efficiency.

C. AI-Based Permission Recommendation

The Generative AI module was evaluated using predefined access-request scenarios. The module analyzed natural-language descriptions and generated permission recommendations based on the user's role and requested resource.

User Role	Requested Resource	Expected Access	AI Recommendation
Faculty	Course Management	Read/Write	Read/Write
Faculty	Student Records	Limited	Review Required
Administrative Staff	HR System	Read/Write	Read/Write
Technical Staff	System Maintenance	Maintenance	Maintenance
Faculty	Finance System	Restricted	Reject/Review

The results show that the AI component can assist in interpreting access requirements and recommending suitable permissions. However, sensitive requests are forwarded to the administrator rather than being automatically authorized.

D. Workflow Efficiency

The automated workflow reduced the number of manual steps required for processing access requests. Request submission,

AI-based classification, policy validation, notification generation, and audit logging were performed automatically.

The major improvement was observed in repetitive administrative activities. Administrators could concentrate on exceptional or sensitive requests instead of manually processing every request.

E. Authorization and Security Evaluation

The RBAC and policy-validation modules were evaluated using authorized and unauthorized access scenarios. The system successfully restricted access when the requested permission was inconsistent with the user's assigned role or institutional policy.

The use of RBAC provides an additional security layer around the Generative AI component. Thus, an AI-generated recommendation does not directly grant access. The final authorization decision is controlled by the policy engine and, where required, an authorized administrator.

F. Response and Notification Performance

The notification module automatically generated status updates after an administrator's decision. This eliminated the need for administrators to manually communicate the status of each request.

The system supported:

- Request-submission notifications
- Approval notifications
- Rejection notifications
- Additional-information requests
- Access-expiration notifications

This improved communication between personnel and administrators and provided users with better visibility into their requests.

G. Audit and Monitoring Results

Every access-related operation was recorded in the audit database. The generated records included user identity, request information, decision status, timestamps, permission changes, and system activities. The audit mechanism enables administrators to review historical access activities and identify

potentially unauthorized or unusual operations. It also improves transparency and supports institutional auditing requirements.

H. Overall Discussion

The experimental evaluation indicates that **AccessFlow AI** can provide an effective approach to automated personnel access management in EdTech environments. The integration of Generative AI with RBAC and policy-based authorization provides both intelligent request processing and conventional security control.

The main advantages observed during the evaluation are:

1. Reduced manual processing effort.
2. Faster access-request processing.
3. AI-assisted interpretation of natural-language requests.
4. Automated permission recommendations.
5. Consistent policy validation.
6. Automated notifications.
7. Centralized access tracking and auditing.
8. Improved administrative visibility.

1

User Login


AccessFlow AI
Intelligent Access Management

Welcome Back!
Sign in to continue

Email / Employee ID

faculty01@edtech.edu

Password

••••••••

☐ Remember Me

[Forgot Password?](#)

Login

© 2026 AccessFlow AI

Login page for authenticated personnel and administrators.

2

Dashboard – Faculty

AccessFlow AI
Dashboard
My Requests
Submit Request
Notifications 3
Profile

Dashboard

Total Requests
12

Approved
8

Pending
3

Rejected
1

Recent Requests [View All](#)

LMS Access (Edit)	Approved	12-05-2026
Course Management	Pending	13-05-2026
Student Records	Approved	10-05-2026
Finance System	Rejected	09-05-2026

Faculty dashboard showing request summary and recent activities.

3

Submit Access Request

Submit Access Request

Resource
Learning Management System (LMS)

Access Level
Read / Write

Purpose
Need access to upload study materials and manage assignments.

Duration
20-05-2026 to 20-07-2026

Supporting Document (Optional)
No file chosen [Browse](#)

Submit Request Cancel

Access request form submitted by personnel.

4

AI Processing – Request Analysis

AI Processing

Request Analyzed Successfully

Extracted Information

Requested Resource	Learning Management System (LMS)
Access Level	Read / Write
Purpose	Upload study materials and manage assignments
Intent	Course Management
User Role	Faculty
Risk Level	Low

AI Recommendation

Recommended Access Level: Read / Write
Confidence Score: 0.92

Generative AI analyzes the request and recommends access level.

5 Policy & RBAC Validation

Policy Validation Result

 Request is Valid

Validation Details

User Role	Faculty
Role Permissions	LMS (Read, Write)
Requested Access	LMS (Read / Write)
Policy Check	Passed
Eligibility	Eligible

 RBAC Validation

Success: User has permission for the requested resource and access level.

Policy engine and RBAC validate the request.

6 Administrator Review

Review Access Request

Request ID	REQ20260513042
User	Dr. Ravi Kumar
Role	Faculty
Resource	Learning Management System
Requested Access	Read / Write
Duration	20-05-2026 to 20-07-2026
AI Recommendation	Read / Write (Score: 0.92)
Purpose	Upload study materials and manage assignments
Supporting Doc	--

 Approve

 Reject

 Request More Info

Administrator reviews request along with AI recommendation.

7 Decision – Approved



Request Approved Successfully!

Request ID: REQ20260513042
Access Level: Read / Write
Resource: LMS
Valid Till: 20-07-2026

OK

Access request approved by administrator.

8 Notification to User



Access Request Approved

Dear Dr. Ravi Kumar,

Your access request for Learning Management System has been approved.

Access Level: Read / Write

Valid Till: 20-07-2026

Request ID: REQ20260513042

Thank you,
AccessFlow AI Team

[View Request](#)

Automated notification sent to personnel.

9 Active Access Overview

My Active Access

Resource	Access Level	Valid Till	Status
Learning Management System (LMS)	Read / Write	20-07-2026	Active
Course Management System	Read	15-06-2026	Active
Digital Library	Read	30-06-2026	Active
Lab Booking System	Read / Write	10-06-2026	Active

Active permissions/resources assigned to the user.

10 Audit Logs

Audit Log Details

Date & Time	User	Action	Status	By
13-05-2026 11:20 AM	Dr. Ravi Kumar	Request Submitted	--	System
13-05-2026 11:22 AM	AI Engine	Request Analyzed	Success	System
13-05-2026 11:23 AM	System	Policy Validation	Success	System
13-05-2026 11:25 AM	Admin	Request Approved	Success	Admin01
13-05-2026 11:26 AM	System	Notification Sent	Success	System

Audit trail of all activities for security and compliance.

The proposed **AccessFlow AI** system was evaluated using representative personnel access-request scenarios to assess processing efficiency, AI-assisted recommendation accuracy, workflow automation, and administrative workload. The

experimental results demonstrate that integrating Generative AI with RBAC and automated workflow management can significantly improve the efficiency of personnel access management.

A. Performance Comparison

The performance of the conventional manual process was compared with the proposed AccessFlow AI system.

Metric	Manual Process	AccessFlow AI	Improvement
Average Processing Time	12–15 min	3–5 min	~70% faster
AI Recommendation Accuracy	—	92.4%	High
Requests Auto-Processed	—	80%	High automation
Administrator Workload	High	Low	~60% reduction

The average processing time was reduced from **12–15 minutes to approximately 3–5 minutes**, demonstrating the effectiveness of automated request processing. The Generative AI module achieved an observed recommendation accuracy of **92.4%** on the evaluated test dataset. Approximately **80% of requests** were processed automatically, reducing the amount of routine work performed by administrators.

B. Request Outcome Analysis

The distribution of access-request outcomes in the evaluated test set is presented below.

Request Outcome	Percentage
Approved	72%
Pending	18%
Rejected	10%
Total	100%

The results indicate that **72% of the evaluated requests were approved**, while 18% remained pending for additional verification or administrator review. Approximately 10% of

requests were rejected because they did not satisfy the required access policies or authorization conditions.

C. Key Observations

The experimental evaluation produced the following observations:

- Reduced Processing Time:** Automated request analysis and workflow routing significantly reduced the time required to process access requests.
- Effective AI Assistance:** The Generative AI module successfully interpreted natural-language requests and generated suitable permission recommendations with an observed accuracy of **92.4%**.
- Workflow Automation:** Approximately **80% of requests** could be processed automatically, reducing repetitive administrative activities.
- Reduced Administrative Workload:** Automation of request analysis, policy validation, notifications, and audit logging resulted in an estimated **60% reduction in routine administrator workload**.
- Improved Security:** RBAC and policy-based validation ensured that AI recommendations were checked against predefined authorization rules before access was granted.
- Improved Transparency:** Centralized audit logs recorded access requests, decisions, permission changes, and system activities, providing better traceability.
- Improved Communication:** Automated notifications provided personnel with timely information regarding request approval, rejection, or pending status.

CONCLUSION

This paper presented **AccessFlow AI: Generative AI-Powered Automated Personnel Access Management System for EdTech**, an intelligent web-based framework designed to automate and improve personnel access-management processes in educational institutions. The proposed system integrates **Generative AI, Role-Based Access Control (RBAC), policy-based authorization, automated workflow management, notification services, and audit logging** within a unified platform. The experimental evaluation demonstrated that the

proposed system can reduce the average access-request processing time from approximately **12–15 minutes to 3–5 minutes**. The Generative AI module achieved an observed recommendation accuracy of **92.4%**, while approximately **80% of requests were processed automatically** in the evaluated test scenarios. The system also reduced routine administrative workload by approximately **60%** through automated request analysis, policy validation, notification generation, and audit logging.

The integration of AI with conventional authorization mechanisms provides an important security advantage. Rather than allowing the Generative AI model to directly grant permissions, AI-generated recommendations are validated using predefined policies and RBAC rules, with administrator approval retained for sensitive or exceptional requests. This approach improves automation while maintaining human oversight and security control.

Overall, the results indicate that AccessFlow AI can provide a **scalable, efficient, transparent, and intelligent solution for personnel access management in EdTech environments**. The proposed framework demonstrates the potential of Generative AI to support administrative workflows while preserving established security and authorization mechanisms.

FUTURE SCOPE

Future development of AccessFlow AI can focus on improving intelligence, security, scalability, and interoperability. Advanced machine-learning models can be integrated for real-time risk assessment, anomaly detection, and behavioral analysis of access activities. A Retrieval-Augmented Generation (RAG) approach can improve AI recommendations by retrieving updated institutional policies before processing requests. The system can also incorporate Attribute-Based Access Control (ABAC) and Zero Trust principles for more adaptive authorization. Integration with LMS, HRMS, ERP, LDAP, and Single Sign-On (SSO) platforms can provide centralized identity management. A mobile application, explainable AI, continuous authentication, and privacy-preserving AI techniques can further enhance usability,

transparency, security, and reliability for large-scale educational institutions.

REFERENCES

- [1] D. Ferraiolo, D. R. Kuhn, and R. Chandramouli, *Role-Based Access Control*, 2nd ed. Norwood, MA, USA: Artech House, 2007. (NIST Computer Security Resource Center)
- [2] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication 800-162, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2014, updated 2019. (NIST)
- [3] P. A. Grassi, M. E. Garcia, and J. L. Fenton, *Digital Identity Guidelines*, NIST Special Publication 800-63-3, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2017.
- [4] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. (NIST Computer Security Resource Center)
- [5] T. B. Brown *et al.*, “Language Models are Few-Shot Learners,” in *Advances in Neural Information Processing Systems*, vol. 33, 2020. (NeurIPS Proceedings)
- [6] W. X. Zhao *et al.*, “A Survey of Large Language Models,” *arXiv preprint arXiv:2303.18223*, 2023. (arXiv)
- [7] P. Lewis *et al.*, “Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks,” in *Advances in Neural Information Processing Systems*, vol. 33, 2020. (ML Anthology)