iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** VI **Month of publication:** June 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.83371

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

# A Web Based Privileged Access Request and Audit System for Secure Access Management

E. Krishnamoorthi[1], Dr. J. Sundaravanan[2], M. Mohammed Riyaz[3], S. Kalidasan[4]
*[1]PG Scholar, [2]Head of the Department, [3]Assistant Professor, [4]Assistant Professor, [3,4]Master of Computer Applications Department, Thanthai Periyar Government Institute of Technology, Vellore-2.*

***Abstract:*** ***In modern enterprise environments, managing privileged access to critical systems has become a significant cybersecurity challenge. Unauthorized or excessive access to sensitive resources such as production databases, cloud infrastructure, and internal tools can lead to data breaches, insider threats, and compliance violations. To address these risks, AUTHRIX is proposed as a secure and efficient Enterprise Privileged Access Management (PAM) solution.***
***The primary objective of AUTHRIX is to ensure controlled, monitored, and time-bound access to organizational resources based on the principle of least privilege. The system implements a structured multi-level approval workflow, where access requests undergo initial validation by the administrator followed by authorization from the respective manager. This ensures that only verified and approved users can gain privileged access. AUTHRIX incorporates Role-Based Access Control (RBAC), allowing employees to request access only to resources permitted for their roles. Privileged access is granted for a limited duration and is automatically revoked after the approved time, minimizing the risk of misuse. Additionally, the system maintains a comprehensive audit trail, including login activities, access requests, approvals, and session details, ensuring transparency, accountability, and regulatory compliance. Developed using modern technologies such as Java (Spring Boot), MySQL, and secure authentication mechanisms like JWT, AUTHRIX provides a scalable and robust solution. By combining strict access control, automated provisioning, and detailed auditing, the system enhances organizational security and effectively safeguards critical resources in enterprise environments.***

***Keywords: Enterprice security, Role-Based Access Control(RBAC), Employee requests/ Multi-Level approval, Time-Bound Access Control, Audit trail.***

## I. INTRODUCTION

Organizations rely on critical IT systems such as databases, cloud servers, and applications for daily operations, but uncontrolled access to these resources can lead to serious security risks and data breaches. Many companies still use manual methods like emails and spreadsheets to manage access, which causes delays, poor visibility, and lack of accountability. To solve this problem, AUTHRIX is introduced as a web-based Privileged Access Management (PAM) system that ensures only authorized employees can request access. It follows a Role-Based Access Control (RBAC) model and uses a structured multi-level approval process. The system also provides time-bound access, which is automatically revoked after the approved duration. Additionally, all activities are recorded for auditing and compliance, making the system secure, efficient, and reliable.

## II. SYSTEM ANALYSIS

### A. *Existing System*

Existing enterprise systems manage privileged access using manual methods like emails and spreadsheets, leading to delays and errors. Role-based access is not strictly enforced, increasing the risk of unauthorized usage. There is also no proper time-bound control, allowing access to remain active longer than necessary. Notifications and approval processes are slow and inefficient. Additionally, lack of audit trails makes it difficult to track activities and ensure security and compliance.

### B. *Proposed System*

The proposed system , AUTHRIX is a centralized web-based Privileged Access Management (PAM) system designed to manage secure access to enterprise resources. It automates the complete workflow, including employee verification, unique ID generation, access request submission, and manager approvals. The system enforces strict role-based access control, ensuring only authorized users can access specific resources. It provides time-bound privileged access that automatically expires to prevent misuse. Real-time notifications keep administrators and managers updated on request status. Additionally, a comprehensive audit module records all activities, ensuring security, transparency, and accountability.

©IJRASET: All Rights are Reserved 

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

## III. DEVELOPMENT ENVIRONMENT

### *A. Hardware Requirement*

Processor type : Intel i3 processor and above
RAM : 8GB
Hard disk : 250GB

### *B. Software Requirements*

Operating System : Windows 11
Front End : HTML, CSS, JS, SERVLET-
Back End : Core Java
IDE : Eclipse Oxyzen
Server : Apache Tomcat
Database : Mysql

## IV. MODULES DESCRIPTION

### *A. Admin*

The Admin Module is the core control layer of the AUTHRIX system, accessible only to the administrator. It ensures that only verified employees from the master dataset can access the system. The administrator uploads and manages employee records and approves user credentials during onboarding.
After approval, a unique Application User ID is generated for each user. The admin also performs the first-level validation of access requests before forwarding them to managers. All administrative actions are recorded in audit logs to ensure security, monitoring, and compliance.

### *B. Onboarding*

The Onboarding Module handles employee registration, credential creation, and access request initiation. It verifies employee details using the master dataset and activates accounts only after admin approval. The system generates a unique Application User ID required for submitting requests. It also enforces role-based access control and allows users to track request status securely.

### *C. Provisioning*

The Provisioning Module handles the final level of approval by authorized managers for access requests. Managers review request details and approve or reject them based on business requirements. The system ensures managers act only on resources under their control and sends email notifications to employees regarding approval or rejection status. All decisions are recorded, and approved requests are forwarded for access activation, ensuring accountability and control.

### *D. Enforcement*

The Enforcement Module activates and controls privileged access based on approved requests. It ensures access is strictly time-bound by validating session start and expiry times before granting access. All user activities during the session are monitored and logged for security. Once the approved duration ends, access is automatically revoked, preventing misuse of privileged permissions.

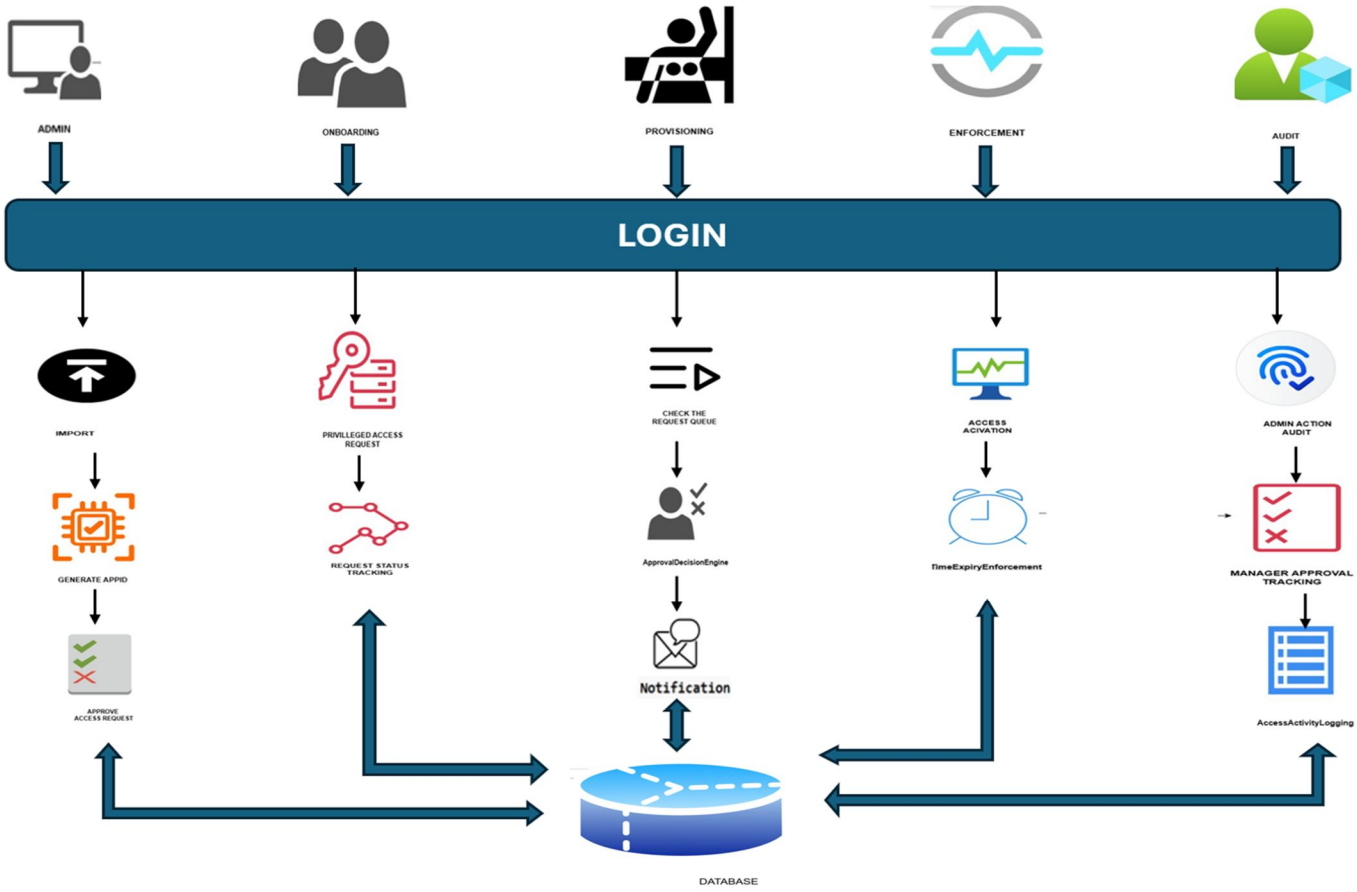
### *E. Audit*

The Audit Module records all critical system activities, including logins, access requests, approvals, and session usage. It securely stores audit logs and allows only authorized personnel to access them. The system generates detailed reports for monitoring, tracking, and compliance purposes. This module ensures transparency, accountability, and strengthens overall security within the organization.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue VI June 2026- Available at www.ijraset.com*

## V. SYSTEM ARCHITECTURE




## VI. CONCLUSION

The Privileged Access Management System provides a secure and structured approach for managing user access by ensuring only verified and authorized employees can access resources. It implements controlled registration and administrative approval to prevent unauthorized access and reduce security risks. By integrating role-based control and secure technologies, the system enhances organizational security and efficiency.

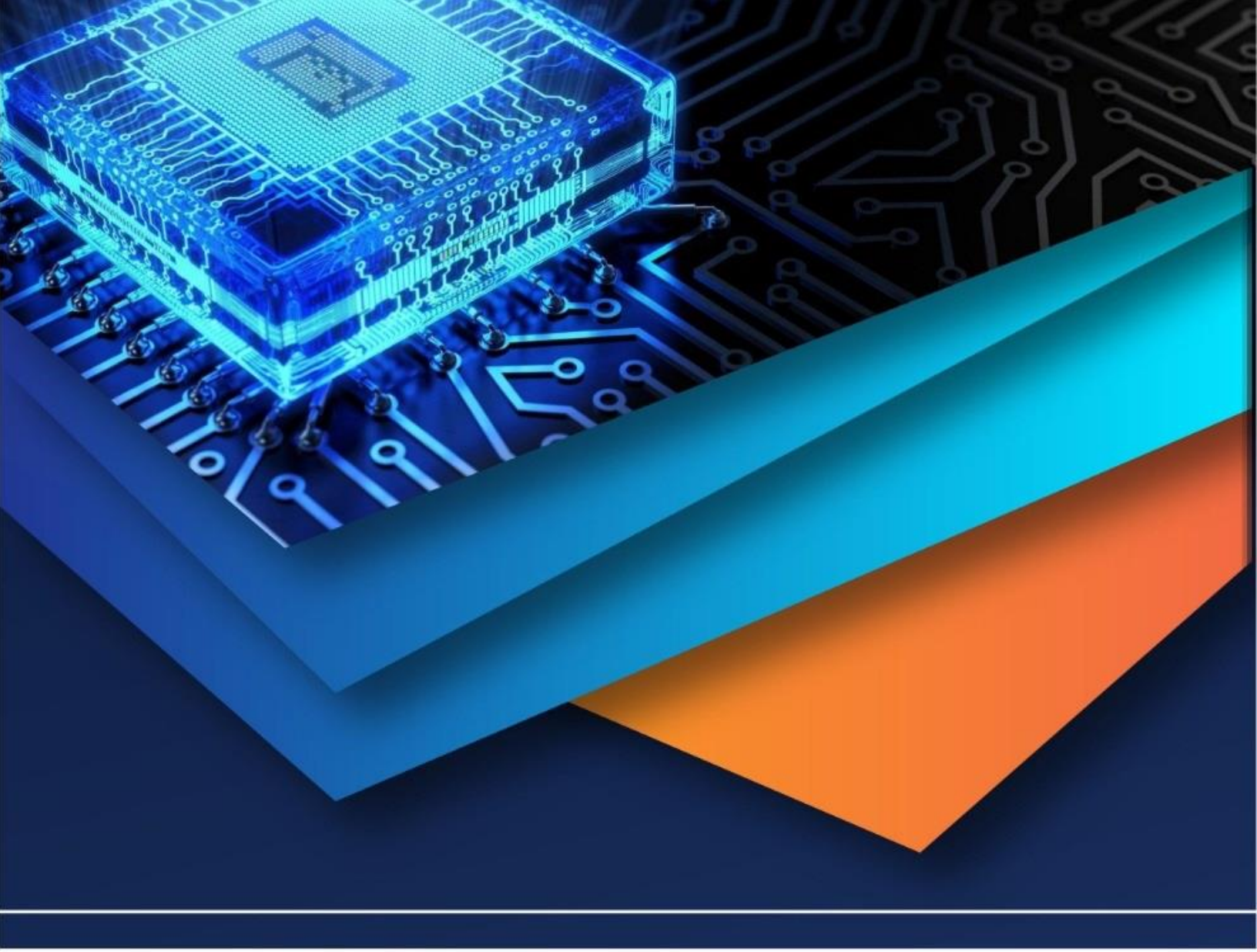
## VII. FUTURE ENHANCEMENT

The system can be enhanced by integrating multi-factor authentication (MFA) to strengthen security and ensure additional user verification. Future improvements may include real-time monitoring, encryption of sensitive data, and automated alerts for better threat detection and compliance. Additionally, adopting a cloud-based architecture can improve scalability, accessibility, and overall system performance.

## REFERENCES

[1] Rout Shiksha., et al. (2023). "Privileged User Access Audits: Techniques for Identifying and Mitigating Insider Threats." International Journal of Future Management Research (IJFMR) 5(3): 1-6.
[2] Sandhu, R., et al. (1996). "Role-Based Access Control Models for Secure Systems." International Journal of Computer Security Applications (IJCSA) 5(2): 12-20.
[3] Ferraiolo, D., Kuhn, D. (1992). "Role-Based Access Control for Efficient Security Management." International Journal of Information Security Research (IJISR) 3(1): 15-23.
[4] Sharma, N., et al. (2022). "Audit Logging System for Secure Access Management in Web Applications." International Journal of Advanced Academic Research (IJAAR) 8(4): 45-52.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)