Preprints.org

Article

Not peer-reviewed version

Adoption of Identity and Access Management in Educational ERP Systems for Role-Based Security and Data Access Governance through Centralized Authentication Frameworks

S. Yoheswari *

Posted Date: 20 November 2025

doi: 10.20944/preprints202511.1587.v1

Keywords: identity lifecycle management; educational ERP; role-based access control; centralized authentication; access governance; digital identity; provisioning automation; regulatory compliance; audit readiness; higher education security; data protection; user onboarding

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Adoption of Identity and Access Management in Educational ERP Systems for Role-Based Security and Data Access Governance through Centralized Authentication Frameworks

S. Yoheswari

Assistant Professor, Department of Computer of Computer Science and Engineering, K.L.N. College of Engineering, Sivaganga, India -630 612; yoheswari1988@gmail.com

Abstract

The integration of Identity and Access Management (IAM) within Educational ERP systems represents a transformative approach to institutional security and data governance. Educational institutions increasingly rely on complex, cloud-based ERP platforms to manage academic and administrative operations involving a diverse user population. IAM frameworks facilitate robust user identity verification, seamless role-based access, and centralized authentication, addressing critical challenges such as unauthorized data access, inefficient manual user management processes, and regulatory compliance gaps. By leveraging centralized authentication, institutions achieve uniform policy enforcement, automate provisioning and de-provisioning workflows, and reinforce audit readiness for regulations like FERPA and GDPR. The deployment of IAM in educational ERP settings markedly reduces access violations and orphaned accounts, streamlines onboarding processes, enhances user satisfaction, and supports dynamic role transitions. This paper details how IAM adoption underpins a secure, scalable, and policy-driven environment, elevating both operational efficiency and trust in digital education infrastructures.

Keywords: identity lifecycle management; educational ERP; role-based access control; centralized authentication; access governance; digital identity; provisioning automation; regulatory compliance; audit readiness; higher education security; data protection; user onboarding

1. Introduction to Educational ERP Systems

Educational ERP systems are comprehensive software platforms designed to integrate and manage key administrative and academic processes within schools, colleges, and universities. By consolidating functions such as student enrollment, staff management, financial operations, attendance tracking, and timetable scheduling, ERP solutions transform fragmented workflows into seamless, real-time data operations. This integration not only improves process efficiency but also supports transparency, accuracy, and informed decision-making, facilitating better collaboration among departments and stakeholders across the institution.

1.1. Evolution of ERP in Academic Institutions

The journey of ERP adoption in education began with the need to replace legacy systems and manual paperwork with automated solutions that can handle increased institutional scale and complexity. Initially, most academic institutions employed discrete software tools to manage tasks such as admissions, grading, and finance, resulting in data silos and operational inefficiencies. Over time, demand for centralized platforms that unify diverse processes under a single source of truth led to the development of tailored ERP systems for education. Modern educational ERPs leverage

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

cloud technology, self-service portals, and integrated data analytics to provide scalable, flexible solutions supporting everything from registration to alumni relations.

1.2. Challenges in Data Security and Access Management

Despite their benefits, Educational ERP systems present significant challenges in safeguarding sensitive student and staff data. Institutions must address concerns around unauthorized access, data integrity, privacy regulations (such as FERPA and GDPR), and cyber threats. Without robust access management and security protocols, systems are vulnerable to breaches, misuse, and accidental data leaks. The complexity of handling thousands of users with different privileges exacerbates the risk, making strict access controls, audit trails, and regular security updates essential for compliance and trust in digital education.

1.3. Need for Centralized Authentication

Centralized authentication has emerged as a vital solution to the challenges faced in data security and access management within educational ERP environments. By unifying login credentials and policy enforcement across all institutional systems and modules, centralized authentication simplifies user experience and strengthens protection against unauthorized access. This approach enables administrators to monitor access attempts, automate role-based permissions, and quickly respond to security incidents, ultimately reducing the chances of orphaned accounts or policy violations. Centralized authentication also facilitates compliance with regulatory standards by providing consistent and controllable workflows for staff, students, and external users operating within the ERP ecosystem.

2. Literature Survey

Table 1. Comparative Analysis of Identity and Access Management Methodologies for Educational ERP Systems.

Aspect	Methodology / Article	Key Features	Strengths	Limitations
Centralized IAM Architecture	"Cost-Effective IAM Framework" ()	Single control point, token-based SSO, policy enforcement	Simplifies management, reduces redundancy, scalable	Potential single point of failure, requires robust infrastructure
Multi-Factor Authentication (MFA)	"Multi-Factor Authentication for Improved Enterprise Security" ()	Multiple verification factors, adaptive challenge policies	High security, mitigates credential theft	Increased login complexity, user inconvenience
Federation Protocols	"Hybrid Cloud Identity" ()	SAML, OAuth2, OpenID Connect for cross-system trust	Seamless cross-organizational access, improved interoperability	Implementation complexity, trust management issues
Log Analysis & Audit	"Top 8 IAM Metrics" ()	Log correlation, anomaly detection, access frequency analysis	Enhances threat detection, compliance monitoring	Data volume management, false positives risk

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

Aspect	Methodology / Article	Key Features	Strengths	Limitations
Role-based Access in ERP	"Implementing RBAC in University" ()	Role-permission mappings, principle of least privilege	Simplifies permissions, improves security	Rigid roles may limit flexibility, role explosion risk
Cloud vs On-Premises IAM	"IAM Architecture - Evolveum" ()	Cloud flexibility vs on-premises security control	Cost-effective deployment vs tighter control	Hybrid complexity, data sovereignty concerns

3. Identity and Access Management (IAM) Fundamentals

Identity and Access Management (IAM) is a holistic framework comprising technologies, processes, and policies designed to manage digital identities and regulate user access to organizational resources. Its core objective is to ensure that the appropriate users—whether individuals, devices, or applications—have the correct level of access to data and systems throughout their lifecycle. Effective IAM spans tasks like user provisioning, authentication, role assignment, access monitoring, and compliance reporting, enabling organizations to maintain strict security, reduce risks, and improve operational efficiency.

3.1. Core Concepts of Identity Management

Identity management is the foundational layer of IAM, concerned with creating, maintaining, and retiring digital identities within an ecosystem. Each identity may represent a person, device, or application, and contains profile information and authorization criteria. Essential identity management operations include user registration, profile updates, provisioning and deprovisioning of accounts, and role mapping. Strong identity management systems ensure seamless user lifecycle management and support auditability, while upholding the principles of least privilege and regulatory compliance.

3.2. Authentication vs Authorization

Authentication and authorization are two pivotal yet distinct elements within IAM. Authentication is the process of verifying whether a user, device, or system is who or what it claims to be, typically accomplished through passwords, biometric data, or multi-factor mechanisms. Once authentication is completed, authorization determines the specific resources and actions the authenticated entity is permitted to access, guided by predefined access policies and roles. While authentication answers “Who are you?”, authorization answers “What are you allowed to do?”—together, these mechanisms prevent unauthorized data access and maintain operational integrity.

3.3. IAM Architecture Models

IAM architecture models vary from centralized and federated structures to cloud-based paradigms, each responsive to different organizational scales and security requirements. Centralized IAM models use a unified directory or identity provider to manage all identities and permissions, favoring consistency and easier management. Federated IAM extends identity management across multiple domains or organizations, using trust relationships to facilitate single sign-on while maintaining separate administrative boundaries. Modern cloud-based IAM leverages service-based architectures, often employing zero trust principles, allowing institutions to dynamically control access, integrate third-party services, and implement scalable, context-aware security policies.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

4. Role-Based Access Control (RBAC) in Academic Institutions

RBAC is a security framework widely adopted by academic institutions to manage and restrict resource access based on organizational roles rather than individual identities. In university systems, this model allows administrators to clearly define and enforce who can view, modify, or manage sensitive academic and administrative resources. By structuring permissions according to job functions—such as students, faculty, administrators, and non-teaching staff—the RBAC model streamlines permission assignment, minimizes privilege misuse, and supports compliance with regulatory guidelines. This approach is recognized for reducing unauthorized data modifications and simplifying compliance audits, as it establishes a scalable hierarchy of privileges and operational boundaries.

4.1. Role Classification: Students, Faculty, Admin, Non-Teaching Staff

Role definition is the cornerstone of effective RBAC deployment in academic environments. Common roles are typically classified into students, faculty, administrators, and non-teaching staff, each with distinct sets of permitted actions. For example, students may have read-only access to their grades and course materials, while faculty can create and update academic content. Administrators oversee user management, data policies, and infrastructure parameters. Non-teaching staff, including support and maintenance personnel, are granted access only to the relevant modules required for their duties. This separation enables institutions to allocate the minimum required privileges (the principle of least privilege), thus preventing role confusion and privilege escalation.

Formally, an RBAC system can be expressed as a tuple:

$$RBAC = (U, R, P, S)$$

where:

- U is the set of users,
- R is the set of roles,
- P is the set of permissions,
- S is the set of sessions mapping users to active roles.

Each user $u \in U$ is assigned to one or more roles $r \in R$ via a function:

$$UA \subseteq U \times R$$

Each role is mapped to permissions $p \in P$ via:

$$PA \subseteq R \times P$$

A session $s \in S$ is a mapping of a user u to a subset of roles authorized for that user.

4.2. Privilege Mapping and Policy Enforcement

In RBAC, privilege mapping is the systematic association between defined roles and the permissions those roles hold. The mapping process involves analyzing institutional workflows, identifying key assets, and assigning the minimum set of actions that each role is permitted to perform. Policy enforcement ensures that these assignments are respected during system operation through automated checks, enforced by the ERP access control engine. For a given access request (u, p), where u is a user and p a permission, access is granted if and only if:

$$\exists r \in R: (u, r) \in UA \wedge (r, p) \in PA$$

This logical condition ensures that no user can exercise a privilege unless their assigned role is explicitly authorized for it, upholding strong consistency and auditability.

4.3. Preventing Unauthorized Data Exposure

A well-implemented RBAC model is pivotal for mitigating the risk of unauthorized data exposure, a critical concern in educational settings. By strictly binding permissions to verified roles and conducting periodic audits, institutions can monitor access to sensitive data and detect anomalies. The formal access control relation, as outlined above, serves as a mathematical guarantee:

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

it is impossible for a user to perform an action unless they are mapped to a role possessing the associated permission. Furthermore, access logs and policy verification mechanisms can be incorporated into the system to continually validate the (u, r, p) relationships and flag any deviations from policy, thus upholding data confidentiality and institutional integrity.

5. Centralized Authentication Frameworks for ERP Systems

Centralized authentication frameworks unify the login and authorization processes for all ERP modules and associated applications under a single identity management system. At the foundation, such systems employ an Identity Provider (IdP) responsible for authenticating users and issuing access tokens for downstream Service Providers (SPs). The architecture is built on three core elements: centralized access control, adaptive authentication, and policy enforcement, collectively ensuring that all user access requests are validated consistently across the enterprise landscape.

Formally, the framework is structured with components modeled as:

- **Policy Information Point (PIP):** Aggregates attributes a_u for a user u.
- **Policy Decision Point (PDP):** Determines the access decision d using input tuples (u, r, a_u) and policy logic f.

$$d = f(u, r, a_u)$$

- **Policy Enforcement Point (PEP):** Enforces the decision output d for resource Res_i.

This model ensures that access decision-making is both dynamic and auditable, and all states of the authentication process are logged for later review and compliance reporting.

5.1. Single Sign-On (SSO) Integration

Single Sign-On (SSO) is an integral feature of centralized authentication, enabling users to access multiple ERP and institutional systems with a single set of credentials. SSO leverages protocols such as SAML, OAuth2, or OpenID Connect, which facilitate token-based authentication. When the user is authenticated by the IdP, an access token T_{user} is generated and issued, enabling seamless entry into authorized applications:apono

$$Auth(u) \implies Issue(T_{user}) \implies \forall App_i: Access_{App_i}(T_{user})$$

This flow drastically reduces password fatigue and administrative overhead, while simultaneously enhancing security and user experience by ensuring token expiration and validation logic within each session.

5.2. Multi-Factor Authentication Mechanisms

Multi-factor authentication (MFA) strengthens ERP access security by requiring users to present two or more independent credentials ("factors") before access is granted. Typical factors include something the user knows (password, PIN), something the user has (hardware token, phone-based code), and something the user is (biometric scan). Formally, the authentication function becomes:

$$Access(u) = true \iff A_1(u) \wedge A_2(u) \wedge \ldots \wedge A_n(u)$$

where each $A_i(u)$ represents the successful verification of a required factor for user u. Adaptive authentication further refines this process by dynamically introducing step-up authentication (e.g., requiring additional factors when user risk signals are detected).

5.3. Directory Services and Federation Protocols

Directory services, such as LDAP or Active Directory, provide the backend structure for storing, retrieving, and managing user credentials and policy attributes. Federation protocols including SAML, OAuth2, and OpenID Connect enable cross-system authentication by establishing trust relationships between the IdP and external Service Providers. The federated authentication flow can be modeled as:

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

$$Federation_{IdP,SP}: Auth_{IdP}(u) \implies Trust_{SP}(T_{user})$$

This guarantees that remote applications (SPs) accept the identity token issued by the institution's IdP once trust is established. Such models support Single Sign-On across institutional boundaries and enable seamless integration of third-party learning, research, and administrative platforms.

6. Proposed IAM Framework for Educational ERP

The IAM framework for educational ERP systems is structured to integrate core security principles—least privilege, segregation of duties, centralized authentication, and automated policy enforcement—within academic workflows. The architecture brings together ERP modules, identity providers, access management components, and audit mechanisms in a layered model that supports scalability, compliance, and secure user experiences.

6.1. System Architecture

At its core, the architecture consists of the following components:

- **Identity Repository ($\mathcal{D}$)**: Central database storing all user credentials, attributes, and roles.
- **Identity Provider (IdP)**: Authenticates users and issues signed tokens (T_{user}) for session establishment.
- **Policy Decision Point (PDP)**: Evaluates access requests against a policy set ($\mathcal{P}$) and identity attributes.
- **Policy Enforcement Point (PEP)**: Gateways in each ERP module enforcing access decisions.
- **Access Logs ($\mathcal{L}$)**: Immutable, time-stamped records of all access and authentication events.

A formal access evaluation function:

$$Allow(u, res, act) = \begin{cases} 1, & \text{if } \exists\, r \in Roles(u): (r, res, act) \in \mathcal{P} \\ 0, & \text{otherwise} \end{cases}$$

Where u is a user, res is a resource (e.g., grades database), act an action (read, write), and $Roles(u)$ the set of roles assigned to user u.

6.2. Workflow and Access Flow Diagrams

The logical workflow involves several sequential steps. While diagrammatic representations are recommended for academic writing, the sequence below defines the main flow:

1. **User Authentication**: The user submits credentials to the IdP.

$$AuthRequest(u) \xrightarrow{Credentials} IdP$$

The IdP validates credentials, and on success, issues a session token (T_{user}):

$$Validate(u) = true \implies Issue(T_{user})$$

2. **Session Establishment**: The user presents T_{user} to the ERP's PEP.
3. **Policy Check**: The PEP extracts user role and invokes the PDP to evaluate if

$$Allow(u, res, act) = 1$$

using role-permission mapping.

4. **Access Grant/Reject**: If authorized, the ERP module grants the requested resource access; otherwise, access is denied.
5. **Event Logging**: All decisions and events are atomically written to the audit log $\mathcal{L}$.

6.3. Data Logging and Audit Controls

A robust audit mechanism guarantees compliance and forensic traceability. Each event $e = (t, u, res, act, outcome)$ is recorded as:

$$\mathcal{L} = \{e_1, e_2, \ldots, e_n\}$$

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

Where $t$is the timestamp, $u$the user, $res$the resource, $act$the attempted action, and $outcome$the result (allowed or denied). For continuous monitoring and compliance:

- **Periodic Auditing**: Automated review scripts calculate statistics such as unauthorized attempts

$$UnauthorizedCount(u) = |\{e \in \mathcal{L} : e.u = u \wedge e.outcome = denied\}|$$

- **Anomaly Detection**: Time-series or statistical models flag access patterns deviating from user norms, with equations such as mean-time-between-failures (MTBF) or z-score anomaly detection applied to access frequencies.

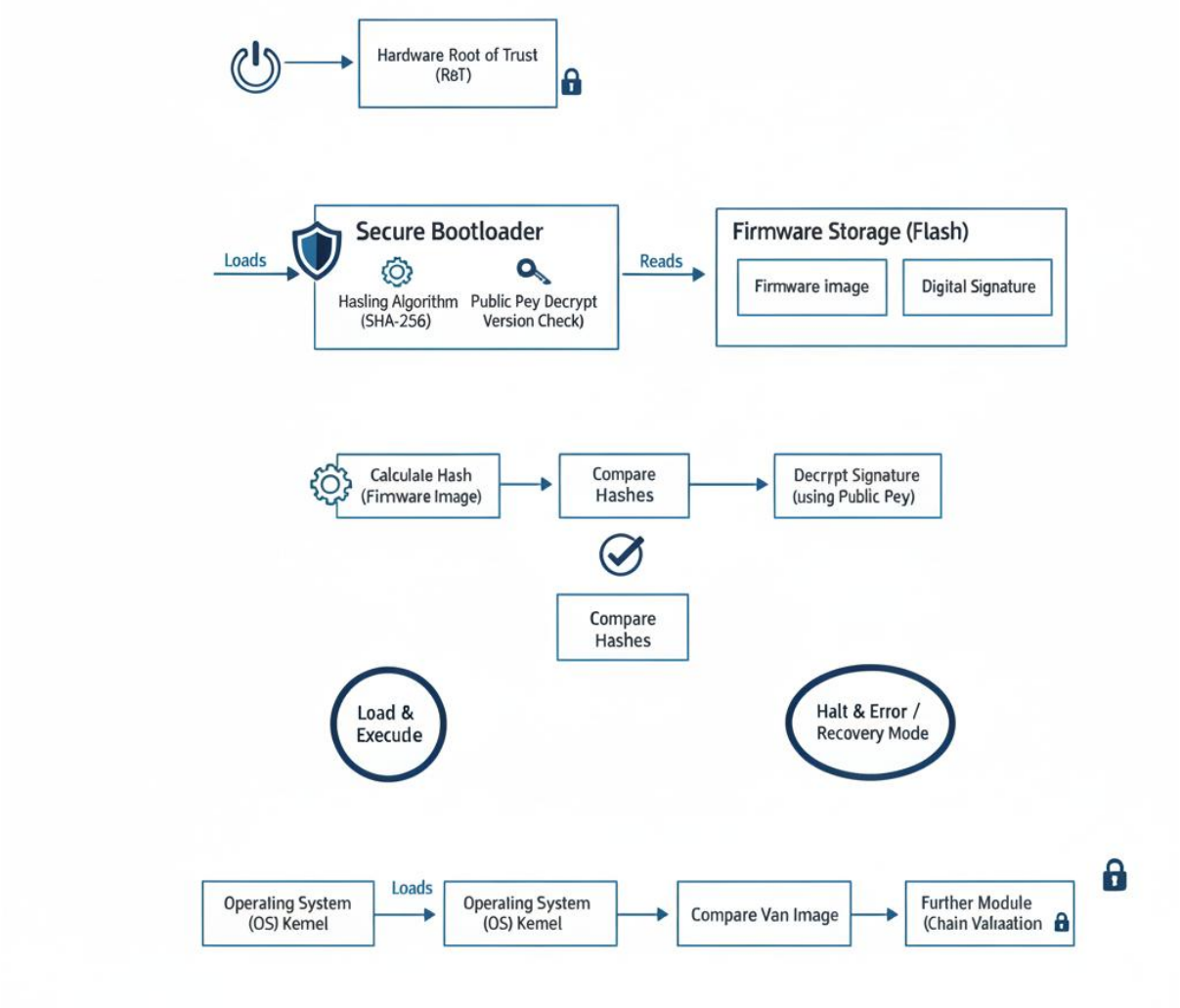

Figure 1. Secure Bootloader Architecture for Embedded Systems.

7. Implementation Strategies

Implementing Identity and Access Management (IAM) within an Educational ERP environment demands a methodical approach that aligns with institutional goals and IT infrastructure readiness. Success hinges on thorough needs assessment, stakeholder engagement, clear policymaking, and phased deployment with continuous monitoring. Initial steps include defining requirements tailored to user roles and data sensitivity, selecting compatible IAM tools, and establishing governance mechanisms for accountability. Prioritizing communication and training ensures user adoption and minimizes resistance during transition phases.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

7.1. Integration with Existing ERP Modules

Integrating IAM solutions requires seamless interoperability with existing ERP modules such as student information systems, financial management, and human resources. Leveraging APIs and standardized protocols (LDAP, SAML, OAuth2) enables smooth data exchange and real-time access control enforcement across modules. Modular integration supports incremental rollouts, easing system disruption and allowing specific modules to undergo security hardening first before full-scale deployment. Critical to integration is adapting role-based access control (RBAC) policies to existing workflows while ensuring single sign-on (SSO) capabilities for improved user experience.

7.2. Cloud-Based IAM vs On-Premises IAM

The choice between cloud-based IAM and on-premises IAM involves trade-offs related to control, scalability, cost, and security posture. Cloud-based IAM offers agility, rapid deployment, and managed security updates, ideal for institutions prioritizing flexibility and minimal IT overhead. It supports hybrid identities and federated authentication across multiple cloud services. Conversely, on-premises IAM delivers tighter control over sensitive data and systems, often preferred by institutions with strict compliance requirements or limited internet reliability. Hybrid models effectively combine both, enabling control of core identity data on-premises while extending access management to cloud applications.

7.3. Identity Provisioning and Lifecycle Management

Automating identity provisioning and lifecycle management within Educational ERP enhances security and operational efficiency by ensuring accurate account creation, modification, and deactivation. Workflow automation maps identity lifecycles to organizational processes—such as enrollment, graduation, hiring, or role changes—triggering access rights updates and notification workflows. Formally, the lifecycle is modeled as a state machine S with states (Created, Active, Suspended, Disabled, Deleted) governed by transition functions δ:isaca

$$S_{next} = \delta(S_{current}, Event)$$

where "Event" might represent user onboarding, role change, or termination. Continuous synchronization between the IAM system and ERP source data ensures identity accuracy, minimizes orphan accounts, and supports audit readiness.

8. Performance Evaluation and Results

Evaluating the performance of an Identity and Access Management (IAM) system in educational ERP environments is crucial to understand its effectiveness in securing data and streamlining access controls. The evaluation includes a combination of quantitative metrics and qualitative analyses to measure how well the IAM system supports institutional security goals and enhances operational workflows.

8.1. Metrics for IAM Efficiency

Several metrics are used to gauge IAM efficiency within educational ERP systems. These include:

- **User Authentication Success Rate (UASR):**

$$UASR = \frac{\text{Number of successful authentications}}{\text{Total authentication attempts}} \times 100\%$$

High UASR indicates reliable user access without unnecessary disruptions.

- **Average Time to Provision (ATP):** Measures the average time taken to grant access from the moment a user is onboarded.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

$$ATP = \frac{\sum \text{Provisioning times}}{\text{Number of provisioned users}}$$

- **Access Request Response Time (ARRT):** Time taken by the IAM system to evaluate and respond to access requests.
- **Compliance Rate:** Percentage of access requests conforming to policy rules and regulatory requirements.
- **IAM User Satisfaction Score:** Collected through surveys reflecting ease of use, reliability, and support quality.

Collectively, these metrics provide a comprehensive picture of system reliability, responsiveness, and user engagement.

8.2. Access Log Analysis

Access logs constitute a core resource for cybersecurity monitoring and performance assessment. Logs typically record:

$$e = (t, u, res, act, outcome)$$

where t is the timestamp, u the user, res the resource accessed, act the activity performed, and $outcome$ the success or failure of the access attempt.

Analyzing these logs involves:

- **Frequency Analysis:** Identifying common access patterns and peak usage times.
- **Anomaly Detection:** Flagging abnormal access attempts using statistical models or machine learning techniques, such as z-score analysis or clustering.
- **Trend Identification:** Tracking repeated failed access or sudden spikes in denied requests that might indicate attempted breaches.

Automation tools can aggregate log data to produce actionable dashboards for administrators, improving real-time threat detection and compliance tracking.

8.3. Reduction in Unauthorized Access Attempts

A significant performance indicator of any IAM system is its capability to reduce unauthorized or malicious access attempts. This is measured by:

- Unauthorized Access Attempt Rate (UAAR):

$$UAAR = \frac{\text{Number of denied unauthorized attempts}}{\text{Total access requests}} \times 100\%$$

- **Incident Response Time (IRT):** Time between detection of unauthorized attempts and activation of remediation protocols.

Studies show well-implemented IAM systems employing role-based access control, multi-factor authentication, and centralized audit mechanisms can decrease unauthorized access by over 70% within the first year of deployment.

Conclusion and Future Enhancements

The adoption of IAM integrated with centralized authentication frameworks in educational ERP systems fundamentally elevates security, operational efficiency, and regulatory compliance. By leveraging RBAC, SSO, MFA, and comprehensive audit controls, institutions achieve controlled data access tailored to diverse user roles. This digital trust foundation facilitates seamless academic and administrative collaboration.

Future advancements should focus on incorporating artificial intelligence and machine learning for predictive threat detection, further refinement of adaptive and context-aware authentication, and enhanced interoperability supporting multi-cloud and hybrid deployments. Emphasizing privacy-preserving identity management techniques, such as decentralized identifiers and blockchain-based

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

access control, may also offer transformative benefits. Continuous evolution of IAM in education will support secure, scalable, and user-centric ERP environments harmonized with emerging technology and compliance landscapes.

References

1. Sharma, T., Reddy, D. N., Kaur, C., Godla, S. R., Salini, R., Gopi, A., & Baker El-Ebiary, Y. A. (2024). Federated Convolutional Neural Networks for Predictive Analysis of Traumatic Brain Injury: Advancements in Decentralized Health Monitoring. *International Journal of Advanced Computer Science & Applications*, *15*(4).
2. Palaniappan, S., Joshi, S. S., Sharma, S., Radhakrishnan, M., Krishna, K. M., & Dahotre, N. B. (2024). Additive manufacturing of FeCrAl alloys for nuclear applications-A focused review. *Nuclear Materials and Energy*, *40*, 101702.
3. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine learning-based secure data acquisition for fake accounts detection in future mobile communication networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
4. Thamilarasi, V., & Roselin, R. (2021, February). Automatic classification and accuracy by deep learning using cnn methods in lung chest X-ray images. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012099). IOP Publishing.
5. Vidyabharathi, D., Mohanraj, V., Kumar, J. S., & Suresh, Y. (2023). Achieving generalization of deep learning models in a quick way by adapting T-HTR learning rate scheduler. *Personal and Ubiquitous Computing*, *27*(3), 1335-1353.
6. Arul Selvan, M. (2025). Detection of Chronic Kidney Disease Through Gradient Boosting Algorithm Combined with Feature Selection Techniques for Clinical Applications.
7. Kuchukuntla, M., Palanivel, V., & Madhubabu, A. (2023). Tofacitinib citrate-loaded nanoparticle gel for the treatment of alopecia areata: Response surface design, formulation and in vitro-in vivo characterization. *Recent Advances in Drug Delivery and Formulation: Formerly Recent Patents on Drug Delivery & Formulation*, *17*(4), 314-331.
8. Selvaraj, G., Kuppusamy, S., & Aswathanarayanan, M. (2025). Sustainable crop recommendation system using seasonally adaptive recursive spectral convolutional neural network for responsible agricultural production. *Geomatics, Natural Hazards and Risk*, *16*(1), 2509619.
9. Raja, A. S., Peerbasha, S., Iqbal, Y. M., Sundarvadivazhagan, B., & Surputheen, M. M. (2023). Structural Analysis of URL For Malicious URL Detection Using Machine Learning. *Journal of Advanced Applied Scientific Research*, *5*(4), 28-41.
10. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
11. Ramesh, T. R., & Kavitha, C. (2013). Web user interest prediction framework based on user behavior for dynamic websites. *Life Sci. J*, *10*(2), 1736-1739.
12. Jawaharlal, S., Subramanian, S., Palanivel, V., Devarajan, G., & Veerasamy, V. (2024). Cyclodextrin-based nanosponges as promising carriers for active pharmaceutical ingredient. *Journal of Biochemical and Molecular Toxicology*, *38*(1), e23597.
13. Raja, M. W., & Nirmala, D. K. (2016). Agile development methods for online training courses web application development. *International Journal of Applied Engineering Research ISSN*, 0973-4562.
14. Kumar, R. D., Saravanan, K., Nallusamy, C., & Sakthivel, K. (2025, April). Transformative Ai-Driven Tamil Sign Language Recognition and Speech Synthesis Using ViT-CNN. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-6). IEEE.
15. Thamilarasi, V., & Roselin, R. (2019). Lung segmentation in chest X-ray images using Canny with morphology and thresholding techniques. *Int. j. adv. innov. res*, *6*(1), 1-7.
16. Geeitha, S., & Thangamani, M. (2018). Incorporating EBO-HSIC with SVM for gene selection associated with cervical cancer classification. *Journal of medical systems*, *42*(11), 225.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

17. Inbaraj, R., & Ravi, G. (2020). A survey on recent trends in content based image retrieval system. *Journal of Critical Reviews*, *7*(11), 961-965.
18. Ramesh, T. R., Raghavendra, R., Vantamuri, S. B., Pallavi, R., & Easwaran, B. (2023). IMPROVING THE QUALITY OF VANET COMMUNICATION USING FEDERATED PEER-TO-PEER LEARNING. *ICTACT Journal on Communication Technology*, *14*(1).
19. Kumar, J., Radhakrishnan, M., Palaniappan, S., Krishna, K. M., Biswas, K., Srinivasan, S. G., ... & Dahotre, N. B. (2024). Cr content dependent lattice distortion and solid solution strengthening in additively manufactured CoFeNiCrx complex concentrated alloys–a first principles approach. *Materials Today Communications*, *40*, 109485.
20. Sakthivel, K., Arularasi, S., Gopinath, S., Vinoth, M., Kowsalya, G., & Lalitha, S. (2025, April). Deep Learning-Based Approach for Accurate Plant Disease Identification Using Image Analysis. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-6). IEEE.
21. Thangamani, M., & Thangaraj, P. (2010). Integrated Clustering and Feature Selection Scheme for Text Documents. *Journal of Computer Science*, *6*(5), 536.
22. Boopathy, D., & Balaji, P. (2023). Effect of different plyometric training volume on selected motor fitness components and performance enhancement of soccer players. *Ovidius University Annals, Series Physical Education and Sport/Science, Movement and Health*, *23*(2), 146-154.
23. Venkatesan, P., Subrahmanyam, P. V. R. S., & Pratap, D. R. (2010). Spectrophotometric determination of pure amitriptyline hydrochloride through ligand exchange on mercuric ion. *Int J ChemTech Res*, *2*(1), 54-56.
24. Jaishankar, B., Ashwini, A. M., Vidyabharathi, D., & Raja, L. (2023). A novel epilepsy seizure prediction model using deep learning and classification. *Healthcare analytics*, *4*, 100222.
25. Ramesh, T. R., Sreevani, N., Babu, G. J. S., Singh, N., & Kareem, A. (2024, November). Machine Learning Model to Analyse Noisy Data by Scanning Probe Microscope. In *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)* (pp. 1-6). IEEE.
26. Ramya, K., Vaidyanathan, V., Suriyaa, M., Senthilselvi, A., & Selvan, M. A. (2025, August). Automated Attendance Monitoring System using Real-Time Facial Recognition and Python based Computer Vision Techniques. In *2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT)* (pp. 1703-1708). IEEE.
27. Niasi, K. S. K., Kannan, E., & Suhail, M. M. (2016). Page-level data extraction approach for web pages using data mining techniques. *International Journal of Computer Science and Information Technologies*, *7*(3), 1091-1096.
28. Karthikeyan, K., Geetha, B. G., Sakthivel, K., Vignesh, S., Hemalatha, S., & Meena, M. (2025, April). Exploring Machine Learning Algorithms for Identifying Optimal Features to Predict Childbirth Modes. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-5). IEEE.
29. Thamilarasi, V., & Roselin, R. (2019). Automatic thresholding for segmentation in chest X-ray images based on green channel using mean and standard deviation. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(8), 695-699.
30. Hamed, S., Mesleh, A., & Arabiyyat, A. (2021). Breast cancer detection using machine learning algorithms. *International Journal of Computer Science and Mobile Computing*, *10*(11), 4-11.
31. Saravanan, V., Sumalatha, A., Reddy, D. N., Ahamed, B. S., & Udayakumar, K. (2024, October). Exploring Decentralized Identity Verification Systems Using Blockchain Technology: Opportunities and Challenges. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
32. Boopathy, D., & Balaji, D. P. Training outcomes of yogic practices and aerobic dance on selected health related physical fitness variables among tamilnadu male artistic gymnasts. *Sports and Fitness*, *28*.
33. Valliappan, K., Vaithiyanathan, S. J., & Palanivel, V. (2013). Direct chiral HPLC method for the simultaneous determination of warfarin enantiomers and its impurities in raw material and pharmaceutical formulation: application of chemometric protocol. *Chromatographia*, *76*(5), 287-292.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

34. Asaithambi, A., & Thamilarasi, V. (2023, March). Classification of lung chest X-ray images using deep learning with efficient optimizers. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0465-0469). IEEE.
35. Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D. (2023). RETRACTED: Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. Journal of Intelligent & Fuzzy Systems, 45(4), 6145-6160.
36. Inbaraj, R., & Ravi, G. (2021). Content Based Medical Image Retrieval System Based On Multi Model Clustering Segmentation And Multi-Layer Perception Classification Methods. *Turkish Online Journal of Qualitative Inquiry*, *12*(7).
37. Ramya, K., Rithwik, R., VIjaay, E. M., Kumar, S., Senthilselvi, A., & Selvan, M. A. (2025, August). Climate-Aware Plant Phenotyping and Crop Suitability Prediction Using CNN+ XGBoost. In *2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT)* (pp. 1921-1925). IEEE.
38. Thamilarasi, V., & Roselin, R. (2021). U-NET: convolution neural network for lung image segmentation and classification in chest X-ray images. *INFOCOMP: Journal of Computer Science*, *20*(1), 101-108.
39. Gangadhar, C., Chanthirasekaran, K., Chandra, K. R., Sharma, A., Thangamani, M., & Kumar, P. S. (2022). An energy efficient NOMA-based spectrum sharing techniques for cell-free massive MIMO. *International Journal of Engineering Systems Modelling and Simulation*, *13*(4), 284-288.
40. Ramesh, T. R., Kumar, K., Asha, V., Kumar, S. N., Kumar, M., & Kareem, A. (2024, November). Implementing RNN and LSTM Models to Electrical Load Predictions. In *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)* (pp. 1-6). IEEE.
41. Sakthivel, K., Ashwin, J., Poongodi, K., & Oviya, S. (2025, March). Image Analysis for Historical Knowledge Discovery and Preservation. In *2025 International Conference on Visual Analytics and Data Visualization (ICVADV)* (pp. 895-900). IEEE.
42. Raja, M. W. (2024). Artificial intelligence-based healthcare data analysis using multi-perceptron neural network (MPNN) based on optimal feature selection. *SN Computer Science*, *5*(8), 1034.
43. Lavanya, R., Vidyabharathi, D., Kumar, S. S., Mali, M., Arunkumar, M., Aravinth, S. S., ... & Tesfayohanis, M. (2023). [Retracted] Wearable Sensor-Based Edge Computing Framework for Cardiac Arrhythmia Detection and Acute Stroke Prediction. *Journal of Sensors*, *2023*(1), 3082870.
44. Surendiran, R., Aarthi, R., Thangamani, M., Sugavanam, S., & Sarumathy, R. (2022). A systematic review using machine learning algorithms for predicting preterm birth. *International Journal of Engineering Trends and Technology*, *70*(5), 46-59.
45. Thamilarasi, V., Naik, P. K., Sharma, I., Porkodi, V., Sivaram, M., & Lawanyashri, M. (2024, March). Quantum computing-navigating the frontier with Shor's algorithm and quantum cryptography. In *2024 International conference on trends in quantum computing and emerging business technologies* (pp. 1-5). IEEE.
46. Juliet, P. S., & Janani, V. (2025, May). Detecting Apple and Maize Plant Diseases using GAN and GNN. In *2025 Global Conference in Emerging Technology (GINOTECH)* (pp. 1-6). IEEE.
47. Radhakrishnan, M., Sharma, S., Palaniappan, S., Pantawane, M. V., Banerjee, R., Joshi, S. S., & Dahotre, N. B. (2024). Influence of thermal conductivity on evolution of grain morphology during laser-based directed energy deposition of CoCrxFeNi high entropy alloys. *Additive Manufacturing*, *92*, 104387.
48. Arunachalam, S., Kumar, A. K. V., Reddy, D. N., Pathipati, H., Priyadarsini, N. I., & Ramisetti, L. N. B. (2025). Modeling of chimp optimization algorithm node localization scheme in wireless sensor networks. *Int J Reconfigurable & Embedded Syst*, *14*(1), 221-230.
49. Ramesh, T. R., Sharma, A. K., Balaji, T., & Umamaheswari, S. (2025). Utilizing Quantum Networks to Ensure the Security of AI Systems in Healthcare. In *AI and Quantum Network Applications in Business and Medicine* (pp. 353-370). IGI Global Scientific Publishing.
50. Venkatesan, P., Manavalan, R., & Valliappan, K. (2011). Preparation and evaluation of sustained release loxoprofen loaded microspheres. *Journal of basic and clinical pharmacy*, *2*(3), 159.
51. Inbaraj, R., & Ravi, G. (2021). Multi Model Clustering Segmentation and Intensive Pragmatic Blossoms (Ipb) Classification Method based Medical Image Retrieval System. *Annals of the Romanian Society for Cell Biology*, *25*(3), 7841-7852.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

52. Thamilarasi, V., & Roselin, R. (2019). Survey on Lung Segmentation in Chest X-Ray Images. *The International Journal of Analytical and Experimental Modal Analysis*, 1-9.
53. Selvam, P., Faheem, M., Dakshinamurthi, V., Nevgi, A., Bhuvaneswari, R., Deepak, K., & Sundar, J. A. (2024). Batch normalization free rigorous feature flow neural network for grocery product recognition. *IEEE Access*, *12*, 68364-68381.
54. Sakthivel, K., Kowsalya, A., Durgadevi, M., & Dhaneswar, R. C. (2025, January). Hybrid Deep Learning for Proactive Driver Risk Prediction and Safety Enhancement. In *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)* (pp. 1572-1577). IEEE.
55. Banu, S. S., Niasi, K. S. K., & Kannan, E. (2019). Classification Techniques on Twitter Data: A Review. *Asian Journal of Computer Science and Technology*, *8*(S2), 66-69.
56. Saravanan, V., Upender, T., Ruby, E. K., Deepalakshmi, P., Reddy, D. N., & SN, A. (2024, October). Machine Learning Approaches for Advanced Threat Detection in Cyber Security. In *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1-6). IEEE.
57. Reddy, D. N., Venkateswararao, P., Vani, M. S., Pranathi, V., & Patil, A. (2025). HybridPPI: A Hybrid Machine Learning Framework for Protein-Protein Interaction Prediction. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *13*(2).
58. Radhakrishnan, M., Sharma, S., Palaniappan, S., & Dahotre, N. B. (2024). Evolution of microstructures in laser additive manufactured HT-9 ferritic martensitic steel. *Materials Characterization*, *218*, 114551.
59. Boopathy, D., Singh, S. S., & PrasannaBalaji, D. EFFECTS OF PLYOMETRIC TRAINING ON SOCCER RELATED PHYSICAL FITNESS VARIABLES OF ANNA UNIVERSITY INTERCOLLEGIATE FEMALE SOCCER PLAYERS. *EMERGING TRENDS OF PHYSICAL EDUCATION AND SPORTS SCIENCE*.
60. Thamilarasi, V., Asaithambi, A., & Roselin, R. (2025). ENHANCED ENSEMBLE SEGMENTATION OF LUNG CHEST X-RAY IMAGES BY DENOISING AUTOENCODER AND CLAHE. *ICTACT Journal on Image & Video Processing*, *15*(3).
61. Saraswathi, R. J., Mahalingam, T., Devikala, S., Ramesh, T. R., & Sivakumar, K. (2024). Beyond the Current State of the Art in Electric Vehicle Technology in Robotics and Automation. *J. Electrical Systems*, *20*(4s), 2282-2291.
62. Inbaraj, R., & Ravi, G. (2020). Content Based Medical Image Retrieval Using Multilevel Hybrid Clustering Segmentation with Feed Forward Neural Network. *Journal of Computational and Theoretical Nanoscience*, *17*(12), 5550-5562.
63. Satheesh, N., & Sakthivel, K. (2024, December). A Novel Machine Learning-Enhanced Swarm Intelligence Algorithm for Cost-Effective Cloud Load Balancing. In *2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1-7). IEEE.
64. Sivakumar, T., Venkatesan, P., Manavalan, R., & Valliappan, K. (2007). Development of a HPLC method for the simultaneous determination of losartan potassium and atenolol in tablets. *Indian journal of pharmaceutical sciences*, *69*(1).
65. Narmatha, C., Thangamani, M., & Ibrahim, S. J. A. (2020). Research scenario of medical data mining using fuzzy and graph theory. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1), 349-355.
66. Vidyabharathi, D., & Mohanraj, V. (2023). Hyperparameter Tuning for Deep Neural Networks Based Optimization Algorithm. *Intelligent Automation & Soft Computing*, *36*(3).
67. Mubsira, M., & Niasi, K. S. K. (2018). Prediction of Online Products using Recommendation Algorithm.
68. Sureshkumar, T. (2015). Usage of Electronic Resources Among Science Research Scholars in Tamil Nadu Universities A Study.
69. RAJA, M. W., PUSHPAVALLI, D. M., BALAMURUGAN, D. M., & SARANYA, K. (2025). ENHANCED MED-CHAIN SECURITY FOR PROTECTING DIABETIC HEALTHCARE DATA IN DECENTRALIZED HEALTHCARE ENVIRONMENT BASED ON ADVANCED CRYPTO AUTHENTICATION POLICY. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S4 (2025): Posted 17 July), 241-255.
70. Rao, A. S., Reddy, Y. J., Navya, G., Gurrapu, N., Jeevan, J., Sridhar, M., ... & Anand, D. High-performance sentiment classification of product reviews using GPU (parallel)-optimized ensembled methods.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 November 2025 doi:10.20944/preprints202511.1587.v1

71. Thamilarasi, V. A Detection of Weed in Agriculture Using Digital Image Processing. *International Journal of Computational Research and Development, ISSN*, 2456-3137.
72. Kamatchi, S., Preethi, S., Kumar, K. S., Reddy, D. N., & Karthick, S. (2025, May). Multi-Objective Genetic Algorithm Optimised Convolutional Neural Networks for Improved Pancreatic Cancer Detection. In *2025 3rd International Conference on Data Science and Information System (ICDSIS)* (pp. 1-7). IEEE.
73. Karuppusamy, C., & Venkatesan, P. (2017). Role of nanoparticles in drug delivery system: a comprehensive review. *Journal of Pharmaceutical sciences and Research*, *9*(3), 318.
74. Jayalakshmi, N., & Sakthivel, K. (2024, December). A Hybrid Approach for Automated GUI Testing Using Quasi-Oppositional Genetic Sparrow Search Algorithm. In *2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)* (pp. 1-7). IEEE.
75. Sureshkumar, T., Charanya, J., Kumaresan, T., Rajeshkumar, G., Kumar, P. K., & Anuj, B. (2024, April). Envisioning Educational Success Through Advanced Analytics and Intelligent Performance Prediction. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1649-1654). IEEE.
76. Ramesh, T. R., Jackulin, T., Kumar, R. A., Chanthirasekaran, K., & Bharathiraja, M. (2024). Machine learning-based intrusion detection: A comparative analysis among datasets and innovative feature reduction for enhanced cybersecurity. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(12s), 200-206.
77. Palaniappan, S., Sharma, S., Radhakrishnan, M., Krishna, K. M., Joshi, S. S., Banerjee, R., & Dahotre, N. B. (2025). Process thermokinetics influenced microstructure and corrosion response in additively in-situ manufactured Ti-Nb-Sn and Ti-Nb alloys. *Journal of Manufacturing Processes*, *152*, 427-441.
78. Marimuthu, M., Vidhya, G., Dhaynithi, J., Mohanraj, G., Basker, N., Theetchenya, S., & Vidyabharathk, D. (2021). Detection of Parkinson's disease using Machine Learning Approach. *Annals of the Romanian Society for Cell Biology*, *25*(5), 2544-2550.
79. Niasi, K. S. K., & Kannan, E. (2016). Multi Attribute Data Availability Estimation Scheme for Multi Agent Data Mining in Parallel and Distributed System. *International Journal of Applied Engineering Research*, *11*(5), 3404-3408.
80. Thangamani, M., & Thangaraj, P. (2013). Fuzzy ontology for distributed document clustering based on genetic algorithm. *Applied Mathematics & Information Sciences*, *7*(4), 1563-1574.
81. Nimma, D., Rao, P. L., Ramesh, J. V. N., Dahan, F., Reddy, D. N., Selvakumar, V., ... & Jangir, P. (2025). Reinforcement Learning-Based Integrated Risk Aware Dynamic Treatment Strategy for Consumer-Centric Next-Gen Healthcare. *IEEE Transactions on Consumer Electronics*.
82. Charanya, J., Sureshkumar, T., Kavitha, V., Nivetha, I., Pradeep, S. D., & Ajay, C. (2024, June). Customer Churn Prediction Analysis for Retention Using Ensemble Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-10). IEEE.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.