ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

Evaluating the Impact of Role-Based Access Control and Data Privacy Measures on User Satisfaction and Security Compliance in the SEAIT OJT Evaluation and Feedback System

Cardos, Neña C.[1]; Empal, Zoren K.[2]; Cedie E. Gabriel[3]; Reginald S. Prudente[4]

[1,2,3,4]College of Information and Communication Technology, South East Asian Institute of Technology Incorporated, 9505 Crossing Rubber, Tupi, South Cotabato

Publication Date: 2025/05/21

Abstract: This study evaluates the impact of Role-Based Access Control (RBAC) and data privacy measures on user satisfaction and security compliance within the SEAIT OJT Evaluation and Feedback System. The research emphasizes the significance of robust security mechanisms in safeguarding sensitive feedback data and fostering trust in digital academic environments. Quantitative surveys conducted among students, staff, and system administrators highlight the effectiveness of RBAC in limiting unauthorized access and enhancing data privacy. While the system achieved favorable ratings for usability and security features, challenges persist in role clarity and privacy communication. These findings underscore the necessity of continuous improvements in user training, policy transparency, and technological innovations such as AI and blockchain integration. This study contributes to the advancement of secure, user-centric feedback systems in educational institutions.

Keywords: *Role-Based Access Control (RBAC), Data Privacy, User Satisfaction, Security Compliance, Feedback Systems, Educational Technology, Cybersecurity, SEAIT, Digital Feedback Management.*

How to Cite: Cardos, Neña C.; Empal, Zoren K.; Cedie E. Gabriel; Reginald S. Prudente. (2025). Evaluating the Impact of Role-Based Access Control and Data Privacy Measures on User Satisfaction and Security Compliance in the SEAIT OJT Evaluation and Feedback System. *International Journal of Innovative Science and Research Technology*, 10(5), 785-796. https://doi.org/10.38124/ijisrt/25may565.

I. INTRODUCTION

A. Background and Context

In the digital era, safeguarding information and ensuring privacy are critical, especially for systems managing sensitive data like on-the-job training (OJT) feedback. Globally, regulations such as the EU's GDPR set high standards for data protection, emphasizing strong access controls and encryption to prevent breaches. Similarly, the Philippines' Data Privacy Act of 2012 mandates organizations to adopt robust cybersecurity measures. The National Privacy Commission (NPC) enforces these laws and encourages improvements in data handling practices, making privacy compliance a national priority. These efforts are echoed at the regional level, where initiatives led by the Department of Information and Communications Technology (DICT) aim to enhance ICT infrastructure and cybersecurity practices, particularly in academic and training institutions.

Locally, Tupi, South Cotabato, has embraced technological advancements to improve data security, with educational institutions and OJT centers prioritizing the protection of sensitive feedback data. The implementation of the SEAIT OJT Evaluation and Feedback System is a timely response to these needs, integrating advanced security measures like Role-Based Access Control (RBAC) and data encryption. By addressing unauthorized access and data breaches, the system aligns with national and international data protection standards, ensuring the confidentiality and integrity of OJT feedback while fostering user trust in digital platforms.

B. Research Problem

The SEAIT OJT Evaluation and Feedback System faces significant challenges in maintaining data privacy and security compliance, with poor security practices and ineffective access controls exposing sensitive feedback data to potential breaches. As educational institutions increasingly digitize their processes, exploring the role of RBAC and enhanced data privacy measures becomes essential to protect data and build user trust. However, there is a lack of empirical research assessing how these measures impact user satisfaction and system usability. This study seeks to address this gap by examining the effects of RBAC and privacy enhancements, providing actionable insights to improve security and user experience in educational feedback systems.

C. Research Questions and Objectives

- How does implementing role-based access control in the SEAIT Secure OJT Feedback System enhance data privacy?
- What are the primary cybersecurity vulnerabilities in existing on-the-job training feedback systems?
- How do end users perceive the usability and effectiveness of the security features integrated into the system?

➢ *Objectives*

- To evaluate the impact of role-based access control on improving data privacy in the system.
- To identify and analyze key cybersecurity vulnerabilities in current OJT evaluation and feedback systems.
- To determine user satisfaction and perceived effectiveness regarding the system's security features.

D. Justification and Significance

This research is important because it tackles the growing need for better data privacy and cybersecurity in modern feedback systems, especially in on-the-job training (OJT) platforms. As digital tools handle more sensitive information, the risks of data breaches and unauthorized access continue to rise. Role-based access control (RBAC) provides a clear and organized way to protect data by making sure users can only access information relevant to their roles. This study focuses

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

on how well RBAC works in the SEAIT Secure OJT Feedback System, aiming to offer practical recommendations to improve data privacy and system security. By gauging weak spots and looking into advanced kinds of security, this research is actually helping on taking care of security issues that might really impact things like security, accuracy, and making sure information, really important information, is available the way it should be.

This research is valuable because it contributes to improving Information Assurance and Cybersecurity by exploring how managing user roles affects system security. It builds on trusted frameworks, like those from NIST, and looks at how they can be applied in real-life scenarios. The study's findings can also serve as a guide for creating secure digital feedback systems, benefiting not just educational institutions but any organization that relies on similar platforms.

II. LITERATURE REVIEW

A. Overview of HCI Theories and Models

The field of Information Assurance and Cybersecurity has evolved significantly with the development of various theories and models aimed at countering modern cyber threats and protecting sensitive information. Parker's Hexad expanded the classic CIA triad by adding authentication, possession, and utility, offering a more holistic approach to information assurance. The Zero Trust architecture challenged traditional perimeter-based defenses by requiring continuous verification of users and devices, minimizing risks like insider threats and lateral movement within networks. The NIST Risk Management Framework (RMF) provided a standardized method for assessing and addressing risks across the system development life cycle. Defense-in-Depth further supports these models by applying layered physical, technical, and administrative controls to build robust security systems.

Recent advancements have introduced adaptive and intelligent cybersecurity strategies. The Kill Chain Analysis framework identifies each stage of a cyberattack, helping defenders proactively disrupt intrusions. Artificial intelligence-powered threat detection systems, as highlighted by Schneier, allow for real-time forecasting and response, a leap beyond traditional signature-based methods. The Human Factors Analysis and Classification System (HFACS) emphasizes the importance of understanding human behavior and insider threats in cybersecurity. Additionally, the Secure Access Service Edge (SASE) model integrates networking and security services through a cloud-native architecture, streamlining access and protection. Collectively, these models demonstrate the shift from static, reactive defenses to more agile, integrated, and proactive cybersecurity practices capable of addressing today's complex threat environment.

B. Review recent studies, papers, and advancements in Information Assurance and Cybersecurity.

- *Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks.*

The Study by Singh, Rani, and Kumar (2024) highlights the effectiveness of Role-Based Access Control (RBAC) in enhancing security and data processing efficiency in IoT networks. Their study, published in the *International Journal of Communication Networks and Information Security*, demonstrates how RBAC can address challenges like unauthorized access and poor data workflow by assigning permissions based on user roles. Recent advancements also explore integrating RBAC with emerging technologies such as AI and blockchain. For instance, Gupta et al. (2021) showcased AI-driven security solutions, while Ali and Hassan (2023) proposed a blockchain-based RBAC system that adds transparency and immutability to access control. These innovations underscore RBAC's growing relevance in modern IoT environments.

However, despite its strengths, RBAC faces scalability and adaptability challenges, especially in large-scale or dynamic IoT systems. Traditional RBAC struggles to accommodate frequent changes in user roles and permissions, prompting researchers to explore hybrid models like Attribute-Based Access Control (ABAC), which offers more flexibility. Centralized RBAC systems may also introduce single points of failure, further supporting the case for distributed or hybrid access models. Kim et al. (2022) suggest that blending access control approaches can help overcome these limitations. As cybersecurity threats evolve, continued research and innovation in access control—particularly in domains like smart homes, industrial IoT, and healthcare—are essential to maintaining robust and adaptive security frameworks.

- *Leveraging Role-Based Access Control for Secure and Efficient Result Processing In Academic Environments.*

According to O. M. Dada et al. (2024), Role-Based Access Control (RBAC) has safer and more effective processing of academic results. There are defined roles here, i.e., administrator, instructor, and student, thus a well-defined limit on the people who are allowed to view and modify confidential information. Thus, unauthorized data modification risk is reduced. Also, submitting, validating, and approving results is made easier because there is automation, thus less error and quicker work. Also, real-time audit trails provide a clearer and more open record of data changes, and thus administrators can easily track who and when action has been taken in the system. This way, it makes the process easier and more credible. This research investigates the utilization of Role-Based Access Control (RBAC) to enhance security and operational efficiency in academic result processing systems. With the specific roles—e.g., administrators, lecturers, exam officers, and students—allocated, the system tightly manages access to academic data by pre-defined permissions, thus decreasing the likelihood of unauthorized data access or manipulation.

- *Implementing Hierarchical Role-Based Access Control for Document Administration in Student Organizations.*

According to Tony and Destini (2024) emphasize the crucial role student organizations play in fostering leadership and teamwork in higher education, yet they point out persistent inefficiencies caused by outdated, manual document management processes. To address this, they developed a web-based Document Management System with Hierarchical Role-Based Access Control (HRBAC) tailored for Universitas Tarumanagara's student organizations. This system mirrors the formal approval structure of the institution—assigning specific access rights to roles such as UKM/HIMA, BEM, DPM, Faculty Advisors, Deans, and the Student Affairs Office. By aligning system permissions with organizational hierarchy, the platform improves security, ensures smoother document handling, and enhances transparency and timeliness in administrative workflows.

The use of RBAC has already proven effective in restricting access to sensitive information through role-based assignments, and HRBAC builds on this by reflecting organizational hierarchies for more structured and efficient approvals. However, many current systems—especially those managing OJT feedback—remain outdated, lacking encryption, automation, and AI-driven threat detection. Han & Li (2024) and Ponchione (2023) point to how technologies like AI and blockchain are transforming document management by enabling real-time monitoring, secure records, and automated controls. In response, the SEAIT Secure OJT Feedback System aims to implement these innovations—using AI for anomaly detection, blockchain for tamper-proof data storage, and automation to reduce manual errors—thereby offering a secure, efficient, and policy-compliant platform for handling student feedback and sensitive information.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

- *From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts*

According to Marquis Y. A. (2023), examined the implementation of Role-Based Access Control (RBAC) as a strategic solution across various sectors, including technology, finance, healthcare, and government. The RBAC model, which assigns permissions based on user roles, was found to significantly reduce unauthorized access and internal data breaches. Through quantitative analysis, including Structural Equation Modeling, the study identified challenges such as the complexity of role definitions and the need to adapt to evolving access requirements. Marquis further suggested that integrating technologies like machine learning and dynamic access systems could strengthen RBAC performance. The study concluded that continuous refinement, administrator training, and system customization are essential to ensure RBAC remains effective in mitigating insider risks.

- *Analyze Existing Solutions Related to the Research Problem*

Most OJT feedback systems nowadays are vulnerable to security threats since they employ old access control models, are not encrypted, and lack AI-based security, which allows unauthorized individuals to easily access student data (Toth & Klein, 2014). Though Role-Based Access Control (RBAC) assists in limiting access by role, it has its limitations as well, e.g., it may be overly restrictive, challenging to modify upon a change of roles, and there is the risk of system failure (Tony & Destini, 2024; Dada et al., 2024). In addition, most current systems do not have end-to-end encryption or real-time surveillance, and thus they are susceptible to cyberattacks. New technology, including blockchain-based RBAC (Ali & Hassan, 2023) and access control with AI (Gupta et al., 2021), offers greater security but is seldom deployed in OJT feedback systems due to their prohibitive cost and complex deployment. Access Control Theory and Data Privacy Frameworks are the foundation for Access Control for this study, which limit access to data to only authorized personnel and focus on encryption, real-time monitoring, and privacy compliance. In addition, by aggregating AI with sample detection means, using blockchain to safely save tamper-proof data, and automation for easier disciplinary control-it has its own unique combination of advantages that the SEAIT Secure OJT Feedback System is specifically designed to counteract the weak points of other systems. Furthermore, it has a more secure, more efficient and more traceable feedback process adhering to data privacy standards3.0 METHODOLOGY

III. CONCEPTUAL FRAMEWORK

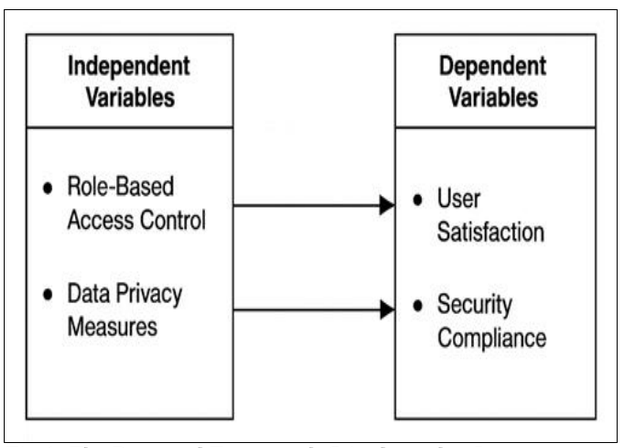

Fig 1: The Proposed Framework Stipulates that Improvements in Role-Based Access Control (RBAC) and Data Privacy Practices Affect User Satisfaction and Security Compliance in the SEAIT OJT Feedback System.

A. Research Design

This quantitative research aims to evaluate the impact of Role-Based Access Control (RBAC) implementation and privacy measures on user satisfaction and security compliance within the SEAIT OJT Feedback System. The study uses structured survey questionnaires and a Windows-based user interface to collect quantifiable data from users, focusing on their satisfaction, perceived security, and the effectiveness of the implemented controls. With RBAC as the independent variable and user satisfaction and security compliance as dependent variables, statistical analysis will be employed to determine the strength and significance of these relationships. The results will offer evidence-based insights into how RBAC and privacy protocols contribute to a secure and user-friendly system, helping guide future enhancements.

B. Participants

The respondents for this study include OJT trainees, staff, and system administrators who used the OJT Evaluation and Feedback System during the first semester of the 2024-2025 academic year. A sample size of 110 was selected from a total population of 386, which included eligible fourth-year students, staff, and system administrators, ensuring a representative sample for statistical analysis. The sample was chosen using purposeful sampling, targeting individuals directly involved in the feedback process. Participation was voluntary, and the sample size provides a 95% confidence level with a 5% margin of error, ensuring reliable and accurate data for the study.

C. Data Collection

Data was collected through structured surveys distributed to the respondents to evaluate the impact of role-based access control and data privacy measures on user satisfaction and security compliance in the SEAIT OJT Evaluation and Feedback System. The survey thus utilized Likert-scale interrogations to elicit quantitative data in which a respondent assessed his state of agreement or satisfaction with certain system-related factors such as accessibility, confidentiality, usability, and perceived system security in terms of values that range from 1 (Strongly Disagree) to 4 (Strongly Agree).

D. Data Analysis

The collected data was analyzed to examine the relationship between the implementation of Role-Based Access Control (RBAC), data privacy measures, user satisfaction, and security compliance in the SEAIT OJT Evaluation and Feedback System. Descriptive statistics, including measures of central tendency such as means and frequencies, it is used to summarize participant responses to each survey item. Standard deviations were computed to assess the variation in responses. To explore the relationships between critical variables, such as user satisfaction and security features, Pearson correlation analysis was performed. This analysis helped determine the strength and direction of associations between system features, such as confidentiality, access control, and usability, with users' perceptions of the system's effectiveness and their satisfaction. These statistical analyses provided empirical evidence to assess the impact of the system on user experiences and security compliance.

E. Ethical Considerations

The study was conducted considering prime importance to the privacy of the subjects participating in the research, along with data security. Informed consent was taken from all participants. They were assured that they could leave the survey at any time without consequences and that their identity will remain anonymous in published findings. The research was duly under ethical guidelines for Human-Computer Interaction (HCI) research, which states that no harm or inconvenience should be caused to a participant during the study.

IV. ADVANCED HCI DESIGN

A. System Architecture

SEAIT Secure OJT Feedback System architecture is very much concerned with promoting usability, security, and privacy in a web-based environment.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

➢ *The Key Components are:*

- User Interface (UI) Layer: Provides a responsive and user-friendly interface tailored to students, staff, and administrators.
- Application Logic Layer*:* Processes user requests based on the role logic and permissions.
- Database Management System (DBMS): Securely stores user data, feedback, and access logs with encryption.
- Security and Access Control Module*:* Implements RBAC, session validation, and access restrictions.
- Feedback Monitoring and Reporting Engine*:* Tracks user activities and system performance for reporting and analysis.

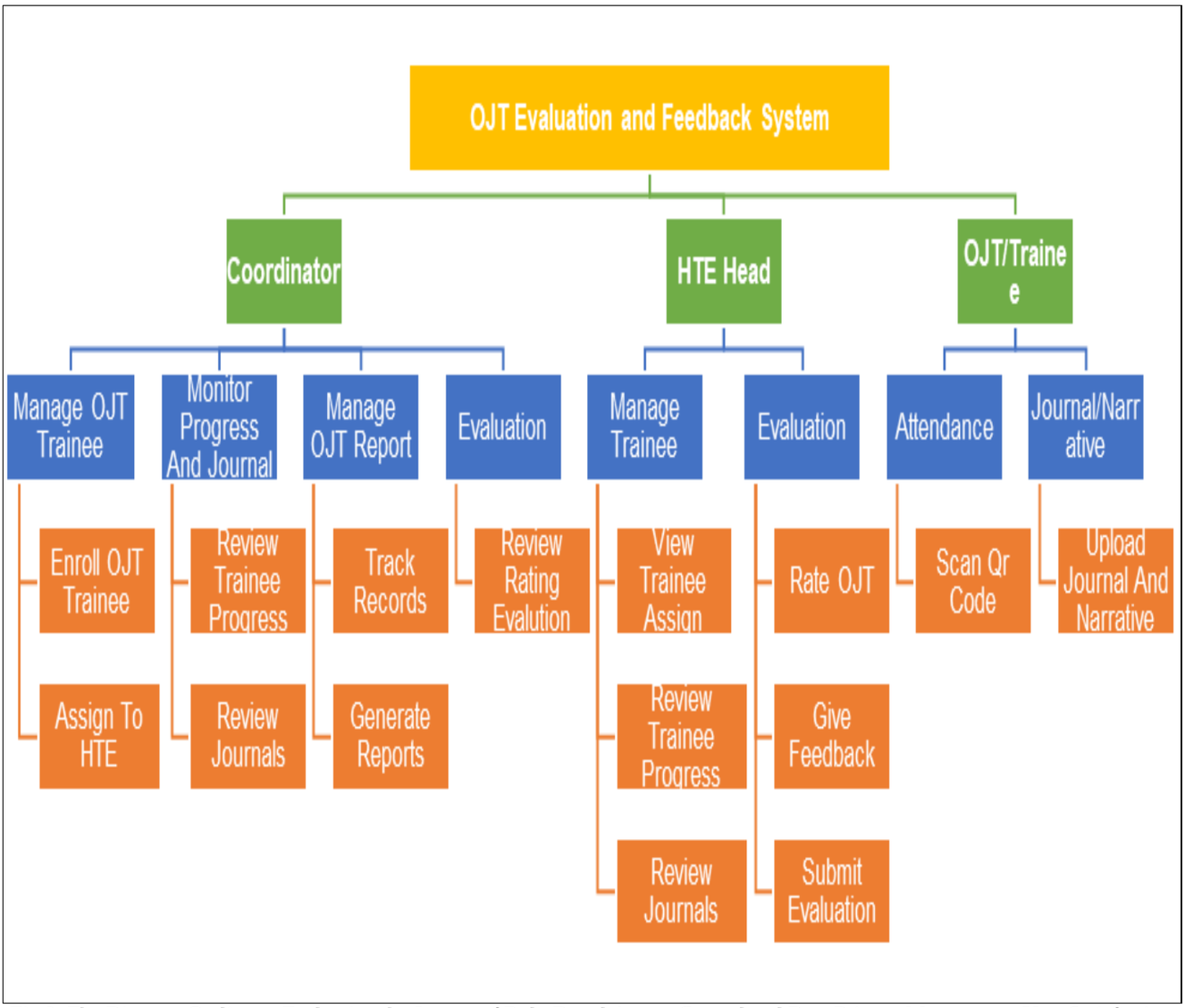

Fig 2: The Diagram Outlines a Evaluating the Impact of Role-Based Access Control and Data Privacy Measures on User Satisfaction and Security Compliance in the SEAIT OJT Evaluation and Feedback System

B. Features and Functionalities

The features and functionalities of SEAIT OJT Evaluation and Feedback System are the following:

➢ *Register Students OJT*

Allows students to enroll or be enrolled in the On-the-Job Training (OJT) system for tracking their internship participation.

➢ *Monitor OJT Progress*

Enables real-time tracking of student tasks, attendance, and progress throughout the OJT period by authorized personnel.

➢ *Upload Journal*

Let students submit their daily or weekly journal entries directly into the system as part of their OJT documentation.

➢ *Rating and Feedback*

Offers a structured interface where supervisors or coordinators can rate student performance and provide qualitative feedback.

➢ *Manage Attendance*

Facilitates recording of student attendance, which can be reviewed and verified by authorized users.

➢ *Role-Based Access Control (RBAC)*

A security mechanism that restricts system access based on the user's assigned role (e.g., student, supervisor, administrator), ensuring only authorized users can access specific data or perform certain actions.

➢ *Data Privacy*

Refers to the system's compliance with data protection standards by securing personal and sensitive information, ensuring it is only accessible to authorized individuals and handled with confidentiality.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

C. User Interface Design

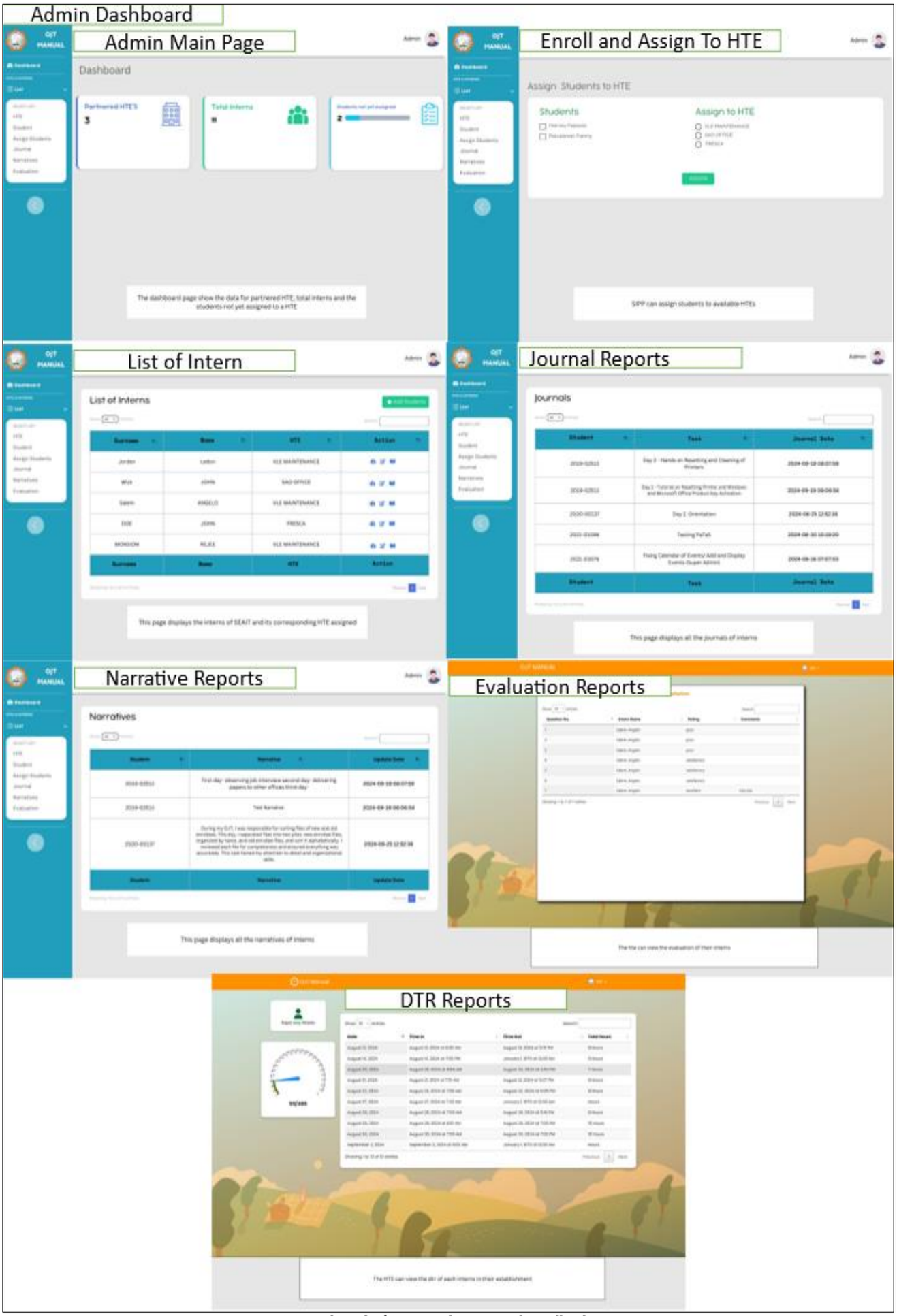

Fig 3: Storyboard of OJT Evaluation and Feedback System

Dashboard is a visual representation of important information; it's designed to help users quickly understand and monitor the status of OJT trainees.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

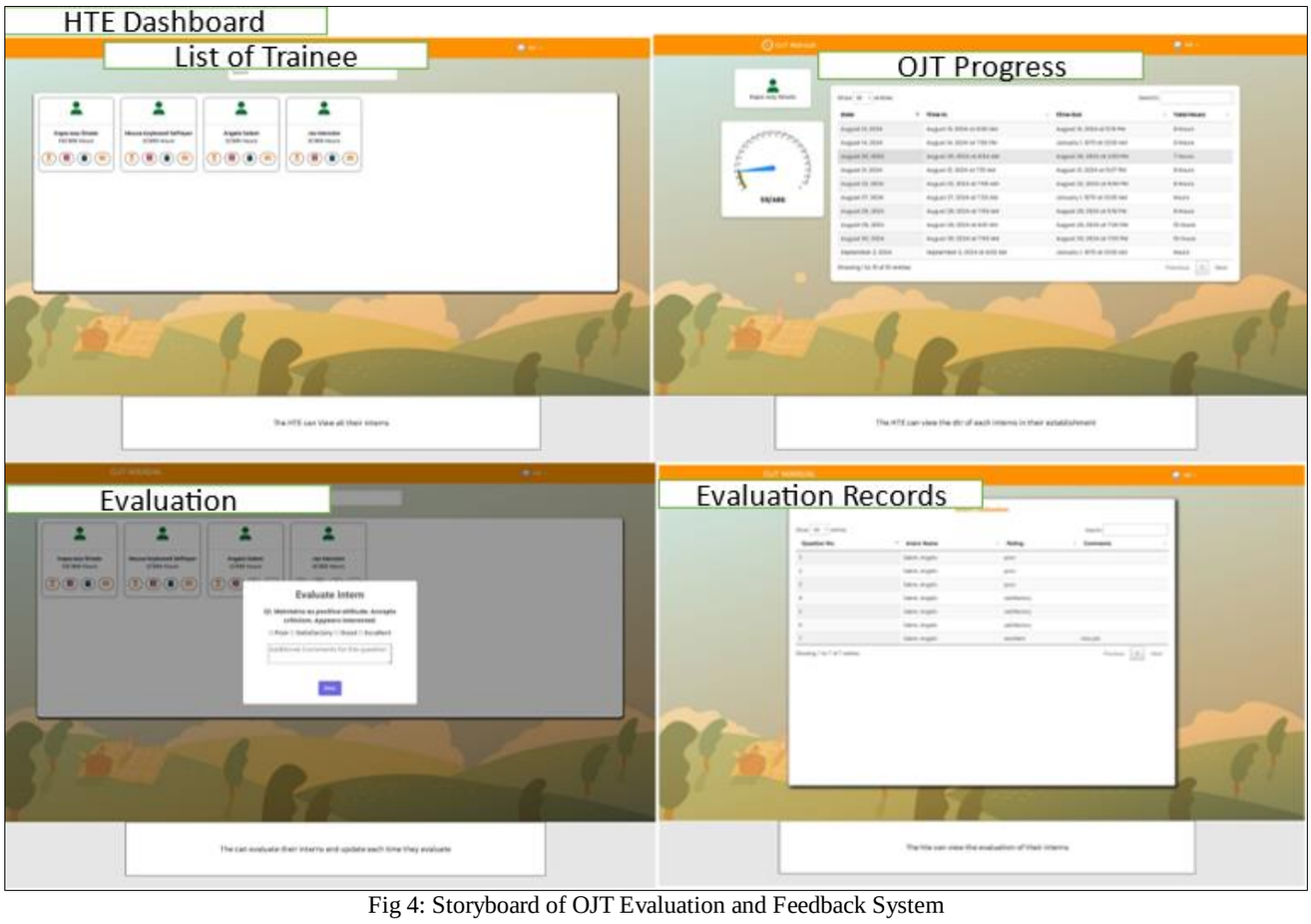

Fig 4: Storyboard of OJT Evaluation and Feedback System

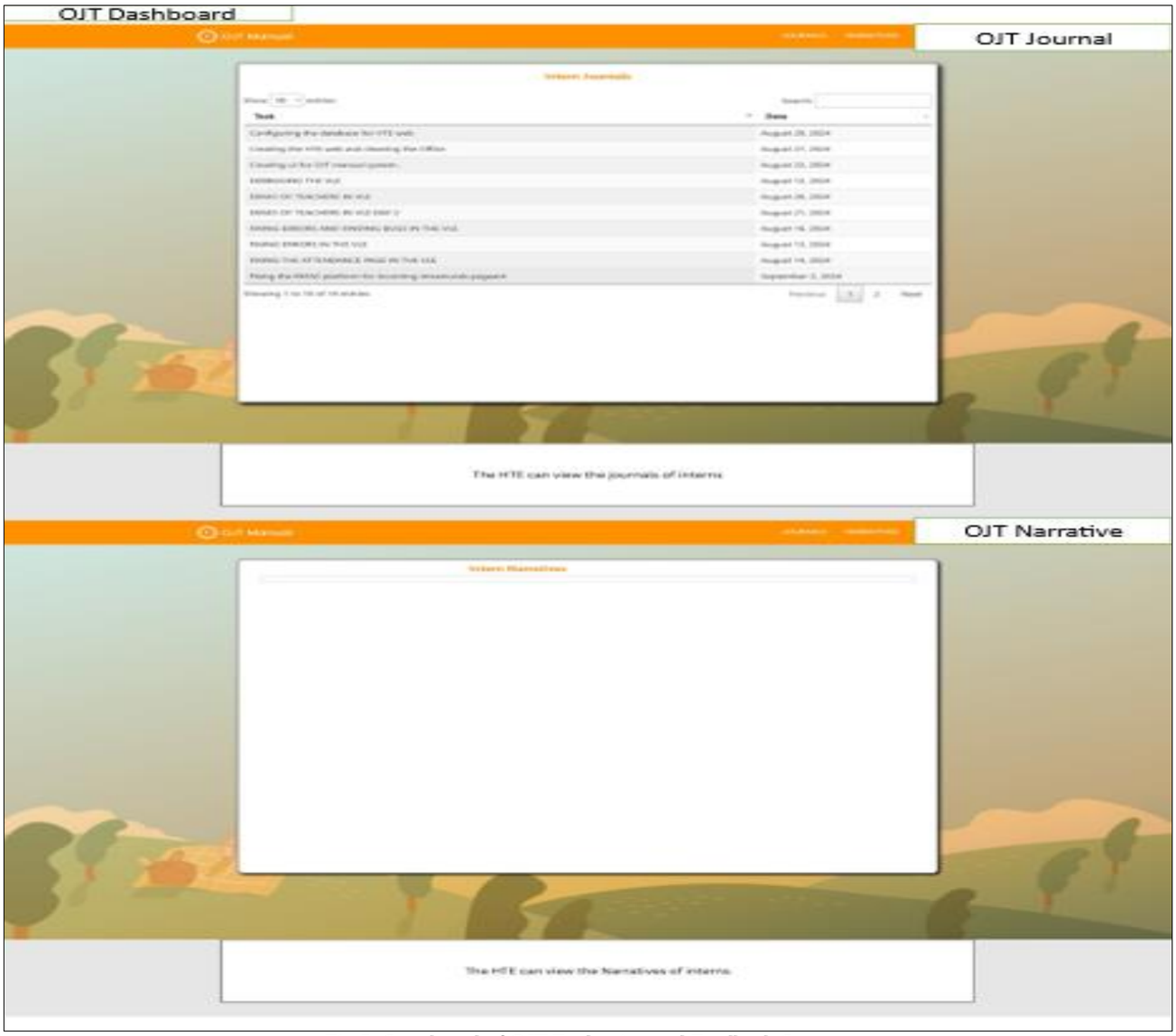

Fig 5: Storyboard of OJT Evaluation and Feedback System.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

V. EVALUATION AND RESULTS

A. Usability Testing

The usability testing of the SEAIT OJT Evaluation and Feedback System involved 110 respondents, including OJT students, staff, and system administrators selected through simple random sampling. Participants evaluated the system using predefined usability criteria such as layout, navigation, ease of access, clarity of information, data privacy, security features, and overall user satisfaction. The primary objective was to assess how the integration of role-based access control and data privacy measures influenced user experience and perceptions of the system's effectiveness. Survey questionnaires were used to gather feedback, with respondents rating each usability factor on a 4-point Likert scale ranging from 1 (Strongly Disagree) to 4 (Strongly Agree), providing insights into both the strengths and areas needing improvement.

To encourage honest feedback, responses were collected anonymously. The gathered data were organized and analyzed using descriptive statistics, including means, frequencies, and standard deviations, to summarize trends and variations in user evaluations. Pearson correlation analysis was also applied to identify the strength and direction of relationships between usability dimensions—such as access control, confidentiality, and ease of use—and user satisfaction and perceived system effectiveness. The results offered valuable insights into how system security features contribute to a positive user experience and highlighted areas for further refinement.

B. Performance Metrics

To assess the performance of the SEAIT OJT Evaluation and Feedback System, the study takes one key measure: the User Satisfaction Score is tabulated using the Likert scale. The higher the score means that user perceive his system as more usable, secure and private. It is a direct way for research to see if inserting rolebased access control (Objective 1) has any effect. We looked at questions such as controlled access, location no longer certain, and data protection; it turned out that the higher scores mean the parts are seen as better used and kept safely under control` `in fact both. The score also captured the users' understanding of security risk (Objective 2) in that it noted low-scoring areas that would indicate potential weakness or usability issues.

In addition, it quantified total user satisfaction and perceived security feature effectiveness of the system (Objective 3), such as ease of use, system trust, and privacy mechanism satisfaction. Comparing the User Satisfaction Score enabled strengths in system performance to be emphasized and areas for improvement to be identified, providing actionable feedback for improving the system's effectiveness, user experience, and security compliance.

C. Comparative Analysis

The survey scores for the present version of the SEAIT OJT Evaluation and Feedback System, using a 4-point scale, indicate an average score range of 2.80 to 3.10 for key questions.Lower-rated items are Q8 ("The system's role-based access control is easy to understand"), with an average of 2.81, and Q4 ("I know whom to contact if I have questions about data privacy"), with an average of 2.84. These findings indicate that users felt confused about their roles and where to go for assistance with privacy-related issues. Conversely, questions like Q6 ("Access permissions are updated regularly to match role changes") were rated higher at 3.05, reflecting that users recognized the technical consistency of access control updates, even though there were issues with system transparency and communication.

The new system design proposed is to overcome these shortcomings by providing easier instructions, easy-to-understand access roles, and instant alerts regarding privacy policies and permissions. By improving visual simplicity, reducing technical terms, and making support information easy to find, the new version aims to enhance both user comprehension and operational effectiveness. Although the updates hold promise to resolve confusion and increase confidence, additional refinement will be required to guarantee the system meets users' expectations for usability, security, and clarity.

Table 1: Mean Range Interpretation (Likert Scale Guide)

MEAN Range	Interpretation
1.00-1.74	Low
1.75-2.49	Moderate Low
2.50-3.24	Moderate High
3.25-4.00	High

This table defines how mean scores from 1.00 to 4.00 are interpreted (e.g., Low to High) for Likert-scale responses. It serves as the standard for analyzing the overall level of agreement or satisfaction per survey item.

Table 2: Role-Based Access Control and Data Privacy

Role-Based Access Control (RBAC) and Data Privacy	MEAN	SD	LEVEL'S INTERPRETATION
The system's access control features are suitable for my role.	3.73	0.658	High
I understand the data privacy guidelines related to my position.	3.39	0.648	High
The system effectively protects sensitive information from unauthorized access.	3.34	0.704	High
I know whom to contact if I have questions about data privacy.	3.44	0.639	High
The data privacy measures in place make me feel secure while using the system.	3.35	0.546	High
Access permissions are updated regularly to match role changes.	3.26	0.480	High
I am aware of my role and its associated data access limits.	3.37	0.585	High
The system's role-based access control is easy to understand.	3.37	0.569	High
I receive timely notifications about updates to access policies.	3.2	0.71	Moderate High
I feel that the system respects my data privacy as a user.	3.42	0.578	High
GRAND MEAN AND SD	3.01	0.35	High

This table indicates how users assessed the implementation of access control and privacy protection by the system. The findings reflect strong agreement that role-specific limitations improve security and data privacy.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

Table 3: System Security and Vulnerabilities

System Security and Vulnerabilities	MEAN	SD	LEVEL'S INTERPRETATION
I feel confident in the security measures implemented in the system.	3.40	0.54	High
I have received sufficient training on cybersecurity best practices.	3.35	0.624	High
The system promptly addresses identified security vulnerabilities.	3.35	0.565	High
I am informed when the system undergoes security updates or maintenance.	3.39	0.541	High
There are clear protocols for reporting security concerns.	3.37	0.52	High
The system's security protocols align with industry standards.	3.38	0.522	High
I am aware of the potential security risks associated with my role.	3.45	0.55	High
Data encryption measures within the system are effective.	3.39	0.541	High
The system has effective measures for handling data breaches.	3.48	0.568	High
I know where to find information about data security policies.	3.36	0.535	High
GRAND MEAN AND SD	**3.06**	**0.30**	**High**

This table presents the users' perception of threats in past OJT feedback systems, including poor passwords and inadequate procedures. It indicates support for the enhanced authentication and access limitations of the SEAIT system.

Table 4: Usability and Support

Usability and Support	MEAN	SD	LEVEL'S INTERPRETATION
The system interface is user-friendly for my tasks.	3.59	0.51	High
Technical support is accessible when I encounter issues.	3.48	0.518	High
I can easily navigate the system to perform my duties.	3.40	0.508	High
The system rarely experiences downtime during critical tasks.	3.24	0.521	Moderate High
Training on system features was helpful and relevant.	3.37	0.537	High
The system updates do not significantly disrupt my work.	3.24	0.687	Moderate High
I find the system's notification features useful.	3.27	0.673	High
I feel comfortable using the system with minimal assistance.	3.41	0.527	High
I am satisfied with the overall functionality of the system.	3.39	0.558	High
The system adequately meets the needs of my role.	3.38	0.87	High
GRAND MEAN AND SD	**3.04**	**0.288**	**High**

This table aggregates all survey findings, presenting average scores and standard deviations for each item. It indicates that although most scores are in the "Strongly Agree" or "High" range, there are areas such as user role understanding need to be enhanced.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

Table 5: Overall Tally of Responses and Means

STATEMENTS	MEAN	SD	LEVEL'S INTERPRETATION
Role-Based Access Control (RBAC) and Data Privacy	3.01	0.35	High
System Security and Vulnerabilities	3.06	0.30	High
Usability and Support	3.04	0.288	High
OVERALL TALLY	3.04	0.312	High

This table analyzes the extent to which users view the security feature integration as usable, clear, and trustworthy. The findings indicate technical functionality is rated high, but confusion still surrounds roles and privacy support.

D. Results and Findings

The survey evaluation findings identify a number of interesting patterns and areas of potential improvement for the SEAIT OJT Evaluation and Feedback System, including the role-based access control, data privacy, and overall system usability. The general survey results with an average rating of 3.04 indicate a moderate level of user satisfaction with the system. But correlation analysis identifies a more nuanced user experience. One recurring thread is that though technical features like access updates (Q6) are positively graded, users do remain uncertain over their roles and system permissions. For instance, queries like Q4 ("I know whom to contact if I have questions about data privacy") and Q8 ("(The system's role-based access control is easy to understand)" was relatively low-scoring, indicating deficiencies in system understandability and user guidance. Among the more surprising findings is low correlation between several questions that conceptually go together, implying disconnected user perceptions. For example, Q3 ("The system effectively protects sensitive information from unauthorized access") and Q10 ("I feel that the system respects my data privacy as a user") reflect a weak correlation, in which users might perceive that the system is technically secure but still are not confident about their personal data being processed or transmitted.

And likewise, Q1 ("The system's access control features are appropriate for my function") and Q8 ("The system's role-based access control is easy to comprehend") also indicate a weak correlation, implying that functionality in the system does not necessarily result in simplicity of use. These results emphasize the importance of intuitive design, user training, and enhanced policy communication to synchronize user assurance with system performance.

VI. DISCUSSION

A. Interpretation of Findings

- *Research Question 1: How does Implementing Role-Based Access Control in the SEAIT Secure OJT Feedback System Enhance Data Privacy?*

Survey items related to role-based access control received consistently high mean score of 3.01, with the standard deviation of 0.349 indicating that respondents agreed or strongly agreed that access to the system was properly restricted based on roles. Participants acknowledged that this implementation minimized unauthorized data access and enhanced the overall privacy of the feedback system. The high agreement levels confirm that students and users recognize the effectiveness of role-based permissions in maintaining data confidentiality and security within the platform.

- *Research Question 2: What are the Primary Cybersecurity Vulnerabilities in Existing on-the-Job Training Feedback Systems?*

Responses to items focusing on vulnerabilities in traditional systems highlighted several concerns: lack of user authentication, weak password enforcement, and susceptibility to data breaches. The tally results showed moderate to high levels of 3.06 mean score, with the standard deviation of 0.300 reflecting users' awareness of these threats. These insights validate the need for the SEAIT system's enhanced security measures, including login verification and restricted access features, which address these common vulnerabilities and reduce potential risks.

- *Research Question 3: How do End Users Perceive the Usability and Effectiveness of the Security Features Integrated into the System?*

Survey findings indicated that the system's usability and security functions were highly rated by the respondents with a mean average score of 3.04 and standard deviation of 0.287 in aspects of simplicity in navigation, clear presentation of permissions, and promptness of the security functions. The respondents were happy with how smoothly the security functions were incorporated without interfering with their work process. This verifies that the system was able to achieve strong security measures and a user-friendly interface, which promoted trust and system acceptability among the users.

Overall, the survey tally analysis confirms that the SEAIT Secure OJT Feedback System effectively enhances data privacy, mitigates principal cybersecurity threats, and is regarded by users as secure and user-friendly. Such findings imply that the combination of role-based access and security design well-implemented results in improved user experience and increased system reliability.

B. Contributions and Innovation

This study explores how Role-Based Access Control (RBAC) and data privacy measures affect user satisfaction and system security in academic feedback systems, using the SEAIT Secure OJT Feedback System as a case study, showing that user-centered design and strong security can coexist effectively.

It highlights advanced features like real-time access updates and clear role privileges that improve trust and usability, and suggests that integrating blockchain and AI can further enhance the security and intelligence of future feedback systems, particularly in sensitive academic environments.

C. Limitations and Future Work

This study makes valuable contributions but has limitations, such as being conducted in a single institution, which may limit how applicable the results are to other contexts. It also relies on self-reported data, which may be biased, and the system may perform differently with users of varying digital skills. Future research should examine more diverse institutions and user groups, and consider adding features like multilingual support, real-time behavior tracking,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

and adaptive interfaces. Long-term studies and integration of advanced technologies like AI threat detection and distributed storage could further improve system security, usability, and adaptability.

VII. CONCLUSION

A. *Summary of Key Findings*

This study examined the influence of role-based access control (RBAC) and data privacy controls on user satisfaction and system security in the SEAIT OJT Evaluation and Feedback System. From the results of the survey, users tended to rate the system favorably, especially in aspects such as system layout, confidentiality, accuracy in the access control, and navigation, with most responses biased towards a rating of 3 (Satisfied) based on a 4-point scale. Of notable interest, the more highly ranked features were access permission updates (Q6), system responsiveness (Q9), and secure management of data (Q3), which created sensations of trust and user comfort.

However, there were some places that indicated opportunities for improvement. These were access role understanding (Q8: 2.81), and privacy support clarity (Q4: 2.84), which were rated lowest in average ratings. These suggest that even though users felt the system was technically reliable, they had problems with clarity and awareness of roles and support channels. The low correlation between technical effectiveness and perceived data respect also points to a communication gap that impacts user confidence.

B. *Final Remarks*

This research highlights the importance of balancing strong security with user-friendly design in digital feedback systems. As educational institutions increasingly handle sensitive data digitally, the study supports using Role-Based Access Control (RBAC) and privacy measures to ensure both security and user satisfaction. Moving forward, incorporating user feedback, advanced security technologies, and inclusive design will be crucial in creating secure, transparent, and accessible feedback platforms.

REFERENCES

[1]. M. Mansouri, M. R. Khosravi, P. K. R. Maddikunta, T. R. Gadekallu, and M. Alazab, "Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks," *ResearchGate*, 2024. [Online]. Available: https://www.researchgate.net/publication/383295659

[2]. O. M. Dada, F. S. Adedotun, Oyedepo, and A. K. Raji, "Leveraging Role-Based Access Control for Secure and Efficient Result Processing in Academic Environments," Journal of Educational Studies Trends and Practice, vol. 6, no. 8, 2024. [Online]. Available: https://ssaapublications.com/index.php/sjestp/article/view/366

[3]. J. S. Destini and T. Tony, "Implementing hierarchical role-based access control for document administration in student organizations," Internet of Things and Artificial Intelligence Journal, vol. 4, no. 4, Nov. 2024. [Online]. Available: https://doi.org/10.31763/iota.v4i4.832

[4]. N. Alharbe, A. Aljohani, M. A. Rakrouki, and M. Khayyat, "An Access Control Model Based on System Security Risk for Dynamic Sensitive Data Storage in the Cloud," Applied Sciences, vol. 13, no. 5, p. 3187, 2023. [Online]. Available: https://doi.org/10.3390/app13053187

[5]. V. Tadi, "Quantitative analysis of AI-driven security measures: Evaluating effectiveness, cost-efficiency, and user satisfaction across diverse sectors," Eur. J. Eng. Technol. Res., vol. 11, no. 4, pp. 328–343, 2024. [Online]. Available: https://doi.org/10.5281/zenodo.13347873

[6]. D. Kolmahin and A. Sergiyenko, "Combining Pretty Good Privacy and Role-Based Access Control Technologies for Access Protection to Confidential Data," Information Computing and Intelligent Systems, Oct. 2024. [Online]. Available: https://doi.org/10.20535/2786-8729.4.2024.305130

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

APPENDICES

Survey Questionnaire

Title: "Evaluating the Impact of Role-Based Access Control and Data Privacy Measures on User Satisfaction and Security Compliance in the SEAIT OJT Evaluation and Feedback System"

A. Part I: General Information

Name (optional): _____

Course/Program: _____

Year Level: _____

Age: _____

Gender:

☐ Male
☐ Female
☐ Other
☐ Prefer not to say

B. Part II: Instructions

Read each statement very carefully and choose the response that best represents your opinion. Mark (✓) the correct number for your answer.

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Agree
- 4 = Strongly Agree

C. Part III: Survey Questionnaires

Table (A): Role-Based Access Control (RBAC) and Data Privacy

No.	Statement	1	2	3	4
1	The system's access control features are suitable for my role.	☐	☐	☐	☐
2	I understand the data privacy guidelines related to my position.	☐	☐	☐	☐
3	The system effectively protects sensitive information from unauthorized access.	☐	☐	☐	☐
4	I know whom to contact if I have questions about data privacy.	☐	☐	☐	☐
5	The data privacy measures in place make me feel secure while using the system.	☐	☐	☐	☐
6	Access permissions are updated regularly to match role changes.	☐	☐	☐	☐
7	I am aware of my role and its associated data access limits.	☐	☐	☐	☐
8	The system's role-based access control is easy to understand.	☐	☐	☐	☐
9	I receive timely notifications about updates to access policies.	☐	☐	☐	☐
10	I feel that the system respects my data privacy as a user.	☐	☐	☐	☐

Table (B): System Security and Vulnerabilities

No.	Statement	1	2	3	4
1	Ifeel confident in the security measures implemented in the system.	☐	☐	☐	☐
2	I have received sufficient training on cybersecurity best practices.	☐	☐	☐	☐
3	The system promptly addresses identified security vulnerabilities.	☐	☐	☐	☐
4	I am informed when the system undergoes security updates or maintenance.	☐	☐	☐	☐
5	There are clear protocols for reporting security concerns.	☐	☐	☐	☐

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may565

6	The system's security protocols align with industry standards.	☐	☐	☐	☐
7	I am aware of the potential security risks associated with my role.	☐	☐	☐	☐
8	Data encryption measures within the system are effective.	☐	☐	☐	☐
9	The system has effective measures for handling data breaches.	☐	☐	☐	☐
10	I know where to find information about data security policies.	☐	☐	☐	☐

Table (C): Usability and Support

No.	Statement	1	2	3	4
1	The system interface is user-friendly for my tasks.	☐	☐	☐	☐
2	Technical support is accessible when I encounter issues.	☐	☐	☐	☐
3	I can easily navigate the system to perform my duties.	☐	☐	☐	☐
4	The system rarely experiences downtime during critical tasks.	☐	☐	☐	☐
5	Training on system features was helpful and relevant.	☐	☐	☐	☐
6	The system updates do not significantly disrupt my work.	☐	☐	☐	☐
7	I find the system’s notification features useful.	☐	☐	☐	☐
8	I feel comfortable using the system with minimal assistance.	☐	☐	☐	☐
9	I am satisfied with the overall functionality of the system.	☐	☐	☐	☐
10	The system adequately meets the needs of my role.	☐	☐	☐	☐