International Journal of Research in Education Humanities and Commerce

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

A HOLISTIC ONLINE RESULT PROCESSING: USING ROLE-BASED ACCESS CONTROL

OLABISI MATEMILAYO DADA[1], FEMI SAMSON OYEDEPO[2], KOLAWOLE ABUBAKAR SADIQ[2] & SIKIRU SULIMAN[2B]

[1,2]Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria

[2b]Department of Statistics, Kwara State Polytechnic, Ilorin, Nigeria

https://doi.org/10.37602/IJREHC.2025.6424

ABSTRACT

The security surrounding Result Processing in an online environment necessitates swift intervention, given the rapidly evolving technology that is now crucial for both students and Staff, as thoroughly examined in this work. Access Control presents serious security risks that require careful attention. Despite numerous researchers discussing various measures to address the overall system, the findings highlight the importance of prioritising data security, integrity, and user experience to uphold academic confidentiality in a digital world. With the transformation in the digital world, educational institutions should endeavour to manage student records effectively while maintaining data security. This work examined the security and safety of student results and transcripts in an online environment. An Agile methodology was employed, which supports Iterative development and flexibility, allowing for constant feedback and quick adjustments to requirements. This approach ensures data integrity, confidentiality, and accessibility. The system is designed to simplify the management of academic records. It has a well-defined interface for administrators, Exam Officers, the Academic Planning Unit, and students, with role-based access control, to ensure a holistic online result processing system that secures authentication and data encryption for non-illegal access and data breaches, which are essential in good system development. This work covers the system's design, implementation, and holistic data security and operational efficiency. The systems that were successfully implemented also indicate that they can be used to meet the needs of educational institutions that are willing to improve their result-processing procedures.

Keywords: holistic, result processing, transcript, authentication, agile software development methodology.

1.0 INTRODUCTION

In today's educational environment, effective academic record management is crucial for both schools and students. The manual processes and paper-based systems frequently used in the traditional methods of handling transcripts and results present several problems, such as inefficiency, a high risk of data loss, and susceptibility to unauthorised access. There is a need for reliable and secure systems that can effectively manage academic records while ensuring data security and integrity as educational institutions transition to digital platforms. This work has identified the need to upgrade to a more reliable, efficient, and secure platform for its academic records management system. The goal is to create a safe and enhanced system, adopting a holistic approach, that secures sensitive data used in these procedures while automating the computation of student results and transcript generation. The need to reduce the

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

risks of data breaches, unauthorised access, and data manipulation, all of which are common in traditional systems, motivated this shift to a digital system. To enhance the security of the data, this lead to the use of Role Based Access Control (RBAC) is an access control That ensures data security by protecting assets and private information against unauthorized access by defined subjects' Role (Ferraiolo et al. (2016); Sandhu et al. (1996)).in this system users can be granted access based on their Role with the assurance that users are using the system for the same purpose and this will require access to the same resources. It helps prevent information leaks or unauthorised modifications by potentially malicious parties.

2.0 LITERATURE REVIEW

Academic institutions are responsible for the creation, management, computation, and processing of examination records of past and present students of the institution. An efficient result and transcript processing system should be able to handle result computation and transcript processing quickly and with a very high degree of accuracy. Result computation and transcript processing systems provide functionalities that enable the academic institution to render efficient services in monitoring academic progress and provide a reliable avenue for students to access their results and transcripts promptly. Diverse researchers contributed to the research process and arrived at a result. Harsha and Thyagaraja (2016) described a school management system designed to automate, integrate, and oversee all tasks related to student data in an academic proceeding. Their work used a SQLite database at the back end and NetBeans IDE 8.1 at the front end for the system development. To enhance system security, a symmetric data encryption model is employed. Also, the integrity and authenticity of information are significantly influenced by who has access to it.

Furthermore, Edison et al. (2021) conducted a comparison of large-scale agile approaches, including SAFe, LeSS, Scrum at Scale, DAD, and the Spotify model. Their work consistently analysed and evaluated all the tools, measurements, practices, and principles of the method. The system is subject to changes due to further empirical study in addition to the original method specifications. The survey also identifies several research gaps that need to be filled using various approaches.

Ufuoma et al.,2024. Ensured Data Integrity in API-Enabled Student Transcript and Result Management Systems. Their work adopted a Rapid Application Development (RAD), which is an iterative and incremental software development methodology that prioritises quick development and iteration. The use of this method for developing Student Transcripts and Result Management with an API (Application Programming Interface) offers several advantages. Additionally, Simon and Saad's (2022) study is grounded in an empirical perspective, examining the techniques and ability to identify problems when implementing access-control policies. The motivation extended beyond the academic view, helping to gain an understanding of how analysis techniques can be applied in the real world. This requires considering the difficulty of comparability, as techniques are often tested against different policies and conditions. However, policy size and processing time are considered suitable criteria, as they indicate how appropriate the technique is for analysing real-world policies. If the analysis technique requires too long, then it would be problematic for the end-user. If the analysis technique has only been evaluated on small policies, then it may not yet be ready to scale to handle real-world policies. better still

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

Bian et al. (2022) worked on certificate-less remote data integrity auditing. The scheme, which considers both data privacy and storage burden issues when ensuring the correctness of the data audit results, utilises the certificate-less design concept to avoid the burdens associated with certificates. The scheme provides a data access control function for authorised users to generate a valid token and access the target data from the cloud.

Megouache et al. (2020) proposed a model that provides authentication and data integrity in a distributed and interoperable environment. They analysed various security models for addressing security issues in large and distributed environments. Their approach involved several steps; step one was about a private virtual network for secure data in transit. The second step utilised an authentication method based on data encryption to safeguard the user's identity and data. The final step involved developing an algorithm to verify the integrity of data distributed across the system's various clouds. The model achieves both identity authentication and the ability to interoperate between processes running on different cloud providers.

Otu (2020) researched a secure program development approach to generate reliable data for student registration in tertiary institutions. The data is transformed using an object-oriented approach (OOP) based on software development principles that employ a modular design. OOP class construct, decision structure, loop, inheritance and interface were used to build the module. The interface was implemented to ensure compliance with the data specification and to ensure that the data passes through a carefully formulated system that will ensure it conforms to the laid-down guidelines and format. Additionally, the module's output demonstrates a range of references, including both valid and invalid data.

Damasevicius et al. (2019) developed a student clearance system that reduces costs, processing time, and overall time. Their architectural design was based on the Unified Modelling Language (UML), which is used in system processing and defining the system's functionality and requirements. The method reduces the tediousness and stress of manual clearance during result generation. The digital platform speeds up information processing and reduces costs associated with labour and processing in an educational environment.

Ekanem et al. (2017) presented a paper that addresses a requirement for a robotic platform, enabling the smooth and interactive organisation of student results across all categories. It also resolves the problems of handling test and exam outcomes for students by creating transcripts, scheduling classes and due dates, and granting secure access to authorised users.

Abah et al. (2022) aimed to design a computerised examination system that some Senior Secondary Schools in Nigeria would use. Developed in single-user mode on a Windows 10 machine, the system was based on SSADM. The programming end utilised PHP, HTML, CSS, and MySQL technologies. This system was used to solve problems on paper-based tests. They aim to eliminate examination misconduct, impersonation, and result compilation delays; however, the system's lack of networking features restricts its scalability and usage in larger educational environments.

Mishra and Alzoubi (2023) conducted a comparative analysis of agile software development versus structured software development, aiming to design a decision tree to determine which method, between Waterfall and Agile, is most suitable for a given software development project. In this case, most researchers used a hybrid development methodology. It was revealed

that the Agile method has several benefits; in some projects, Phases may require a mixed strategy because the Waterfall approach is sometimes important. The feasibility of integrating Waterfall and Agile methods in software development management was investigated in their study. Moreover, Onibere (2013) used a fuzzy logic technique in developing a decision support system for tracking and assessing academic program achievement in Nigerian schools. Fuzzy ideas are integrated into the multidimensional data schema created by the model, along with a meta-table structure for categorisation. He discusses issues with data inconsistency and offers helpful advice via a case study.

Osunade et al. (2019). The system ensured the avoidance of mistakes and delays in transcript generation and result processing, which can lead to students missing out; this system was developed as a pilot project using one faculty because manual processes might lead to computation errors and delays in producing accurate transcripts or results, which can negatively impact students by depriving them of possibilities.

Okikiola and Samuel (2016) developed a web-based system and restructured the generation of transcripts and results in educational institutions. They utilised WAMP (Windows, Apache, MySQL, PHP) and HTML and JavaScript as Software development tools to enhance accessibility for students and optimise result and transcript generation in certain institutions. Their research, Olamide and Joshua (2012), proposes a web-based approach. Also discussed was the issue of students having easy access to their exam results through the Result Alert System, which utilises SMS and email technology.

Akputu et al. (2020) researched Policy-Driven Academic Result Computation and Transcription. Aimed to resolve incompetence in academic result computation and transcript due to an expanding student population and dynamic curriculum. The system aims to automate processes, significantly reducing processing time and errors while ensuring robust data integrity and security measures. It also attempts to provide access control based on the roles of individual participants, which determines their permissions. Additionally, the study employs the Rational Unified Process (RUP) and a multi-tier architecture to develop a policy-driven system that adapts to departmental policies, enhancing flexibility and compliance by utilising technologies such as Apache, MySQL, PHP (via XAMPP), HTML, CSS, and JavaScript.

3.0 TYPES OF ACCESS CONTROLS

This paper discusses an access-control model to enhance understanding and review of its differences, highlighting that all access-control systems share common and primary components.

Role-Based Access Control (RBAC) Model: enables the restriction of access based on subject Role (Ferraiolo et al., 2003; Sandhu et al., 1996), which users can be granted access based on their Role, under the believe that users using the system for the same purpose and require access to the same resources. RBAC is precise, and a series of accepted models exists. The RBAC96 family of modewidelyidely adopted and cites the first formalised and normalised RB (AC model (Sandhu, 1995). The model implements the needed security principles of RBAC systems (least privilege and separation of duties), but it also includes constraints to handle mutual exclusion and cardinality on user-role and permission-role assignment. ARBAC97 serves as an extension of RBAC96 to account for the formalisation of administration in RBAC models

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

(Sandhu et al., 1999). The formalisation of an administration model is necessary, as a single central authority does not administer RBAC models, and it is required to distribute administrative control to sub-areas of activity.

Discretionary Access Control (DAC): In discretionary access control, the subject can grant permission to others at their discretion. That is, a user owning a resource can grant or deny access to other subjects. From previous studies, an algorithm was developed to determine and ensure the safety and complexity of DAC systems. (Dranger et al., 2006; Li et al., 2005). Unix permissions are a good example of DAC, with usread, write, and execute permissions (read, write, and execute). However, a more recent version was allowing for recently introduced, all permissions, owing to either positive/n (negative permissions, or strong introduces the possibility of conflicts. Klael (2014) presents the possibility of conflicts. Resolution strategies are often needed to determine whether negative or positive permissions should take precedence. Discretionary access-control systems have been used in the past to configure organisations in a way that implements role-based access controls, specifically the administration of user roles and permissions.

Mandatory Access Control (MAC) is a variation of the access-control model whereby a central authority enforces a security policy, constraining a subject's ability to access resources and making it different from other access-control mechanisms, such as DAC. The MAC operating system enforces the policy set by the Administrator, whereas in DAC, the owner can control access. MAC has a history of being used in highly sensitive environments, such as those in military systems (Kumar, 2006). A typical representation of MAC is the Bell-LaPadula model (McLean (McLean, 1985), which employs aviewedtice model to govern access. MoreMore specifically, the lattice can be viewed as a hierarchy of access levels, where restrictive information can only flow upward (from least restrictive to most restrictive).

Attribute-Based Access Control (ABAC) is an access-control paradigm whereby policies are defined in terms of attributed types (e.g., users, resources, objects, environment). ABAC allows for a greater degree of flexibility by enabling a greater number of discrete inputs into access control decisions (Hu et al., 2015; Zhang et al., 2018). In ABAC systems, subjects and objects have a series of attributes, which are subsequently utilised in rules created by the Administrator or owner to govern the set of allowable capabilities. Furthermore, ABAC can account for risk-intelligent access control by considering subject risk and resource sensitivity (Xin et al., 2012). Figure 1 provides a graphical overview of how ABAC differs from more traditional access-control models, which have been previously discussed (DAC, MAC, and RBAC). ABAC systems introduce the additional components of Subject Attributes and Object Attributes, which are essential axioms used in access-control policies. This significantly increases the flexibility of access control systems, which were previously centred on granting permissions to subjects based on rules that tied the subject and object together. The use of attributes for the subject and object allows the Administrator to implement an ever-increasing variety of access controls, which, using more RBAC, MAC, and DAC systems, would be exhaustive and cumbersome to manage. Furthermore, ABAC eliminates the need to modify the central policy rule set, as changing the subject and object attributes alone will enable the application or revocation of policies that are currently in place.

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

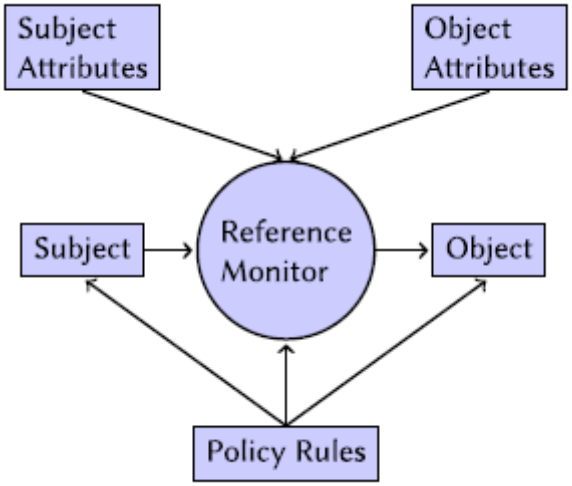


Figure 1. Primitive access-control abstract model. (Simon and Saad, 2022)

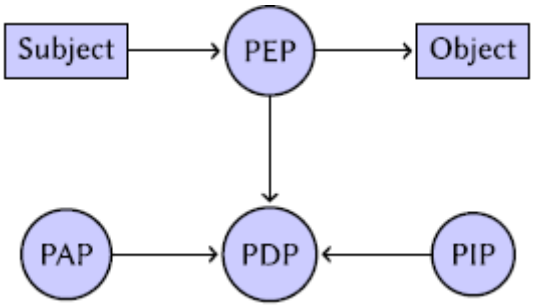


Figure 2. Primitive attribute-based access control. (Simon and Saad, 2022)

The development of the language is largely motivated by the need to deliver standardisation across the implementation of different ABAC systems. XACML provides a standard architecture and process model to describe the flow of information through the access-control system. The standard goes beyond the abstraction provided in Figure 1 and introduces standardised notation and information flow process. Figure 2 presents the standardised information flow and system architecture. The components of the XACML standard are as follows:

1) Policy Enforcement Point (PEP): interrupts the requests from the subject and translates them into an XACML authorisation request.
2) Policy Decision Point (PDP): accepts and assesses the XACML request based on its policies.
3) Policy Administration Point (PAP): Policies are managed through the PAP.
4) Policy Information Points (PIP) are where attribute values are stored and retrieved.

Auditing of ABAC has been established as an open challenge by a recent study. The authors Note that performing analysis would be resource-intensive due to the distributed nature of ABAC, which is based on identity-less access-control policies (Servos & Osborn, 2017).

4.0 RESEARCH METHODOLOGY

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

4.1 Research Design

In this research, both qualitative and quantitative approaches were integrated to design a comprehensive analysis of a holistic, secure online result processing system. This design eased the survey of user experiences, data integrity, and security measures from multiple perspectives.

Qualitative Methods: Semi-structured interviews and discussions were conducted with participants, including administrators, HODs, and Exam Officers. The eligible members of the academic planning unit and students. These provided an understanding of user needs and expectations concerning the system's functionality and security features.

Quantitative Methods: Surveys were administered by every institute stakeholder and to every student at all levels of studies, which allowed for statistical analysis of user satisfaction and system performance metrics.

System Development Process: An agile software development model was employed in this work, which supports iterative design and continuous feedback from the participants. The key stages of the development process are outlined below:

Requirements Gathering: Initial requirements were identified through past work on online result processing (Dada, 2017; Dada, 2024); the participant was interviewed, and surveys were conducted to capture user expectations and critical functionalities needed in the system.

Design: A system architecture was designed, incorporating RBAC to ensure holistic and secure access based on user roles (e.g., administrators, HOD, Exam Officer, APU staff and students). Role-based access control (RBAC) policies regulate user access to information based on the activities they perform. Role-based policies require the identification of roles in the system. A role is a collection of permissions to use resources appropriate to a person's job function; thus, it is defined as a set of actions and responsibilities associated with a particular working activity. Instead of specifying all the accesses each user is allowed to execute, access authorisations on objects are defined for roles. Users are given authorisation to adopt roles. The design also included user interface (UI) models to show the system's functionality, as shown in Figure 3.

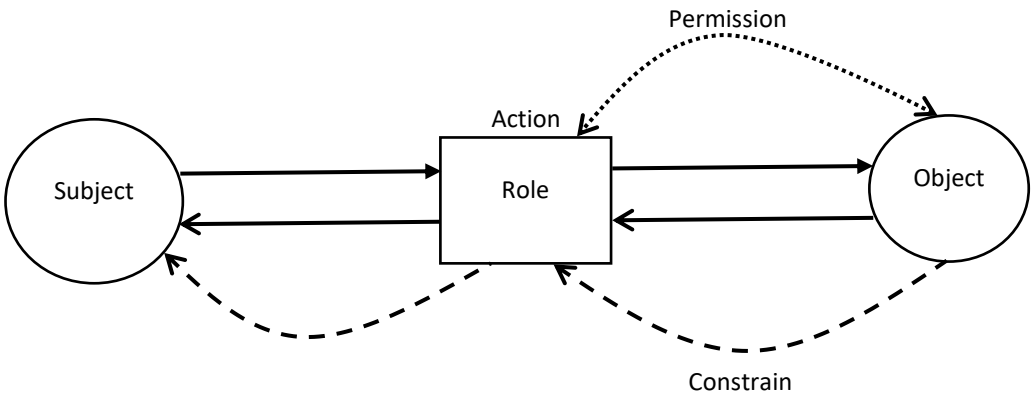


Figure 3: A System Architecture: Designed, Incorporating RBAC to Ensure Holistic and Secure Access Based on User Roles

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

The development of a Holistic Data Integrity for an online Result Processing System, utilising a role-based Access Control (RBAC) Framework, involves a staged and iterative approach. A thorough review of existing online result-processing frameworks, standards, and user-centric design principles is conducted to provide a basis for the development of the proposed system. The standardisation process involves defining a set of subjects, Objects, and Actions with constraints that ensure compatibility and interoperability across diverse environments within the result-processing platform. Concurrently, the Administrator and user-centric design were incorporated to prioritise ease of use, transparency, and user satisfaction. The results from our institution demonstrate the iterative nature of the development process, which enables continuous refinement based on emerging threats and technological advancements. Feedback loops, involving the use of RBAC, ensure the right permissions are given to authorised users based on their Role and for every object they need to act on. In this work, Figure 4 shows the entities involved and their attribute, which are:

The Subjects are the users, including the Administrator, the Head of the Department, Various Exam officers in each department, and the Approved authority from the Management and Academic Planning Unit, who utilise the proposed system.

The Objects are the resources, including the System, student records, files, and database.

Actions: Actions refer to the roles users perform based on their permissions while running the application, either granting or denying access to resources by the subject.

Permissions (privilege): An authorisation to perform some action on the system. Permission refers to some combination of object and operation. A particular operation used on different objects represents different distinct permissions, and similarly, if two different operations applied to a single object represent two distinct permissions, this is about the specification of access rights and combines the Permission strategy, the permission model and the permission policy, including their components (i.e., subject, object and action). It also considers the process of defining the permission policy about the selected model, as framed by its strategy.

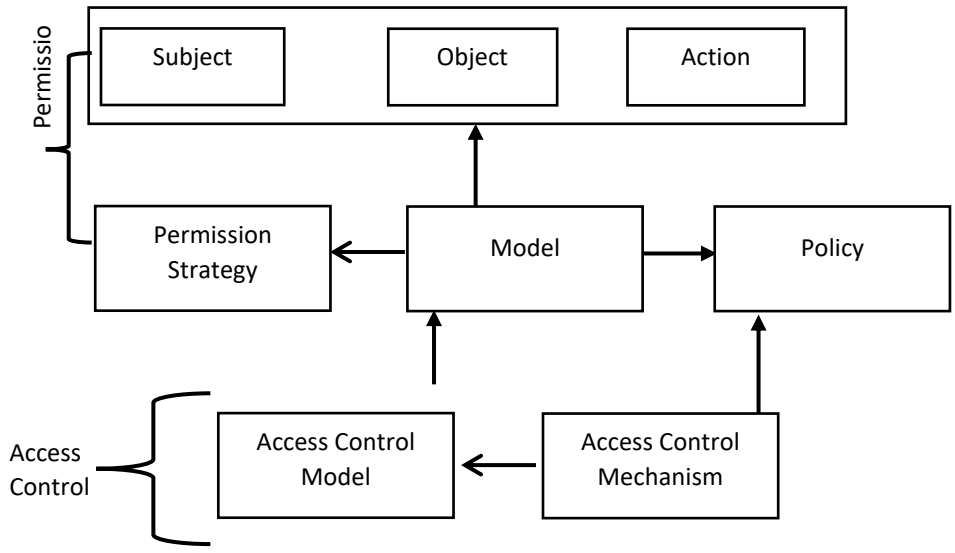


Figure 4: Access Control and Permission for a Holistic Online Result Processing

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

Permission Strategy: This outlines the overall perspective on specifying permissions, focusing on an administrative-centric approach and setting the framework for the Permission models.

Permission Model: The permission model used in this work is RBAC, which defines access rights through three main attributes: subject, object, and action. However, concerning the access control model, which enforces the permission model, the additional components can also be relevant, such as Role and session with RBAC or environmental variables with Role-based access control (RBAC):

Subject: is the active entity, which includes (the user, group, organisational Role, process, and application program)

Users: are the exam officer, HOD, the Academic Planning Unit, and students of each department

Group: is the Administrator, Staff, and Student. Organizational Roles are those who are granted or denied permissions based on their responsibilities.

Process: are the activities that need to be performed by the users based on their Role. An application program is a software developed.

Object: These are resources that are passive entities and require protection, such as a system, including a file, a database table, or a record.

Action: states what privilege, (access) right or type of operations the subject can perform on the object.

Permission Mode: This defines the model for specifying the access Rights of the subject, specifically the actions between the subject and the object, and their interactions concerning the core authorisation strategy.

Permission policy: describes access control policies at a high-level requirement that specify how access is managed and who may access information under what circumstances.

Access control is about enforcing the subject's right over the object during processes, determining who does what to what based on a defined permission policy.

Access control model: Defines the enforcement of the permission model, i.e., what needs to be checked to determine whether to allow or deny access for a subject to a protected resource.

Access Control Mechanism: Is it an implementation of an access control model and, thus, an instance-level artefact? It enforces a permission policy which fits the access control model of the mechanism. The mechanism determines whether an access request evaluation allows or restricts access.

Development: The development stage involved coding the system using modern programming languages and frameworks, with a focus on performance, security, and user experience. Several

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

testing procedures were implemented to identify weaknesses and ensure system robustness. This included user acceptance testing (UAT), unit testing, and integration testing.

4.2 Data Collection techniques:

A multi-faceted approach was employed to gather data from various participants. Surveys were distributed online to staff involved and students, incorporating Likert scale questions to quantify satisfaction levels and open-ended questions for qualitative feedback. The survey on user satisfaction is illustrated in the figure.5

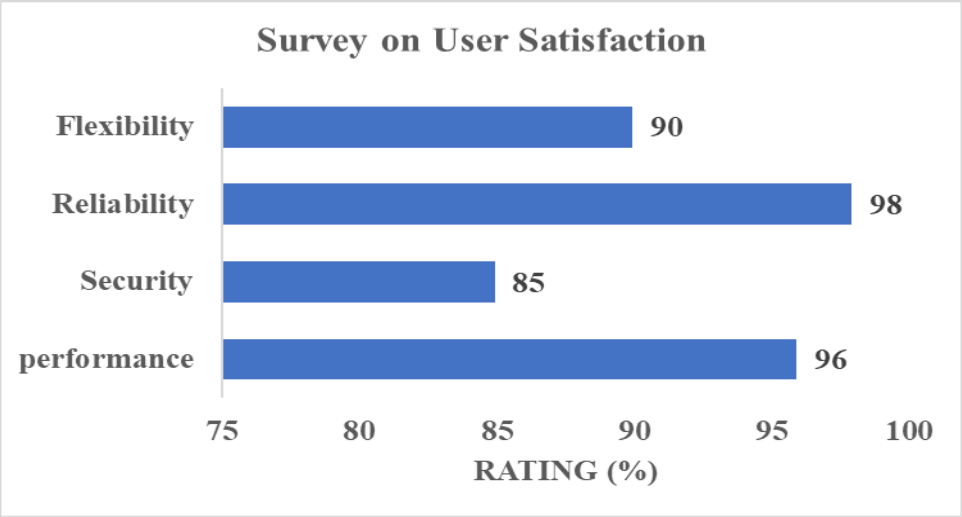


Figure 5. Distribution of user ratings on the System

Semi-structured interviews were conducted with key participants, including administrators, HODs, Exam Officers, APU staff, and students, to gather data. This approach provided a qualitative understanding of their insights into the system's usability and security measures.

System usage: During the system's utilisation, it was examined to track user access and evaluate its throughput, identifying any security vulnerabilities.

Evaluation Techniques: The efficiency of the holistic, secure online result processing system was evaluated through various quantitative and qualitative metrics:

4.3 The Distribution of User Ratings on the System

Data was analysed to confirm user satisfaction based on the flexibility, security, reliability, and overall performance of the system. Descriptive statistics were used to classify trends.

Security Assessment: A security assessment was conducted to evaluate the Role and permissions between the subject and object during RBAC model implementation, focusing on each user's roles and permissions. Figure 6 illustrates the security assessment.

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

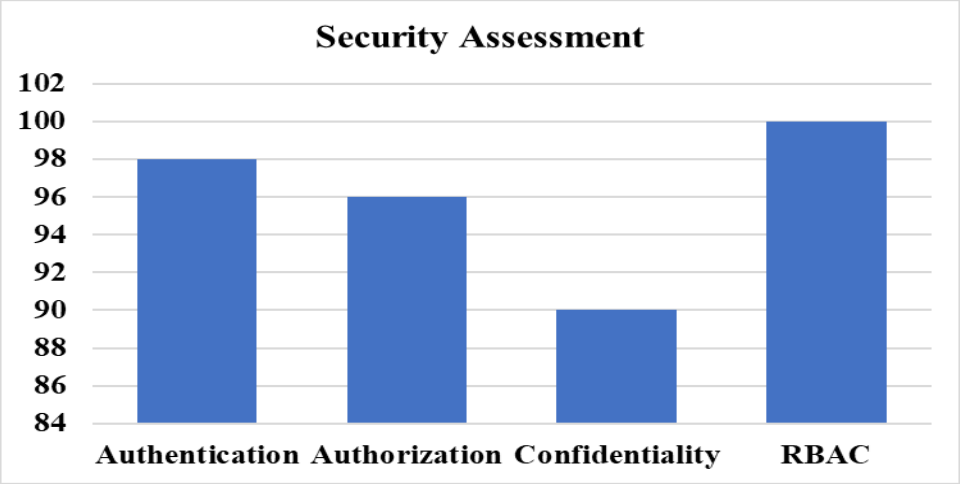


Figure 6: Distribution of Security Assessment

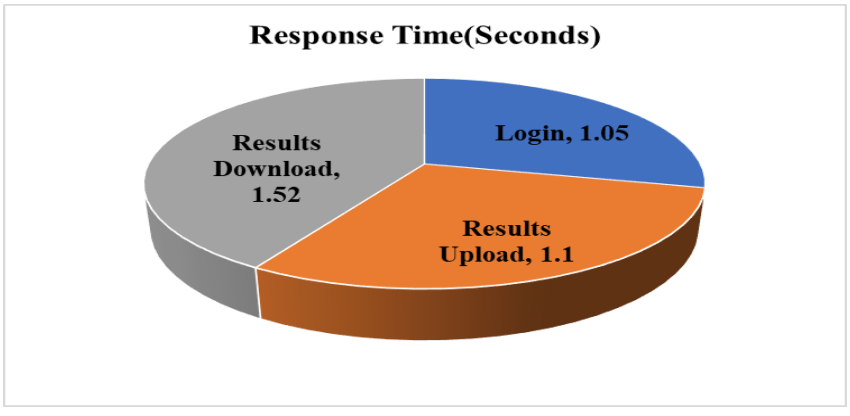
Figure 6 shows the distributions of security performance on authentication of the system, how it authorises the Role to a subject, either to be permitted or denied access to the resources available on the system, the confidentiality of the system to the users and how compliance of the system is developed to the RBAC framework

4.4 Performance Evaluation

System evaluation was conducted on a holistic Secure Online Result Processing with Role-Based Access Control (RBAC) through various parameters, including security assessments, response time, user satisfaction, and. system throughput. The evaluation aims to establish how efficiently the system meets its objectives of enhancing security, user experience, and data integrity within academic environments.

4.5 Response Time

This Response time is one of the important parameters used in measuring the efficiency of a holistic, secure online result processing system. This shows the time taken for the system to process user requests, upload requests and downloads. However, the evaluation focuses on the response times for several processes, including login, uploading results, and downloading results.



Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

Figure 7. Distribution of System response time per second

Figure 7 shows that the average response time for user logins was approximately 1.05 seconds, while result upload and download operations averaged around 1.1 and 1.52 seconds, respectively. This remains within acceptable limits, providing a satisfactory user experience.

4.6 System Output

This measures the number of transactions processed per unit of time. High throughput shows a system's ability to handle several user requests concurrently. During the evaluation, we conducted several tests by simulating multiple users accessing the system simultaneously.

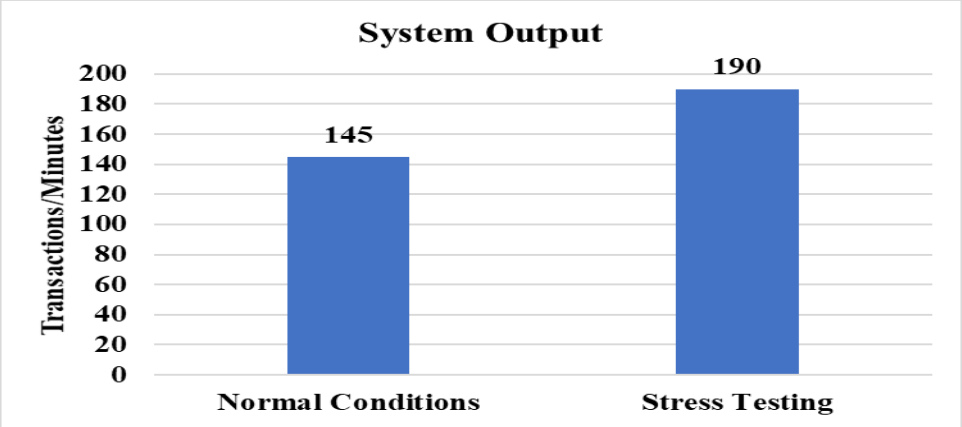


Figure 8. System Outputs per Minute

Figure 8 shows that the system achieved a throughput of approximately 145 transactions per minute under normal conditions, with a peak of 190 transactions per minute during several tests. This demonstrates the system's capacity to manage high volumes of simultaneous user requirements competently.

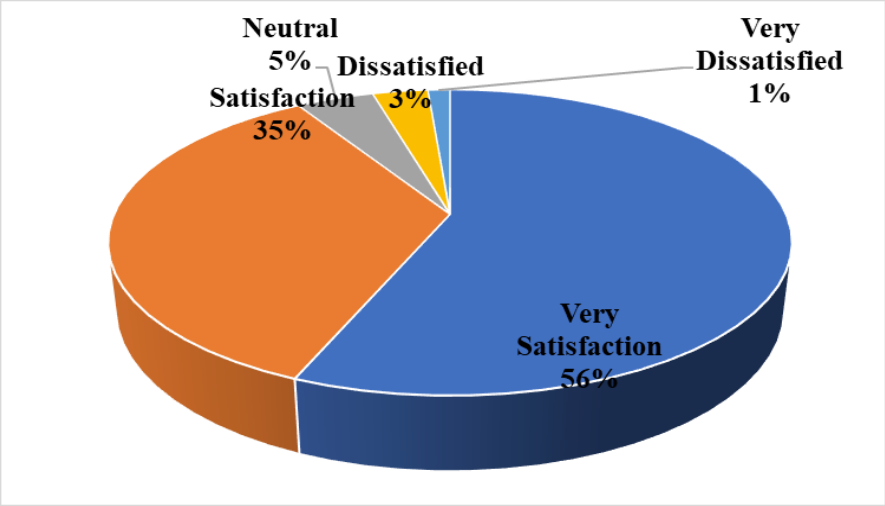


Figure 9. User Satisfaction Evaluations

Volume 06, Issue 04 "July - August 2025"

ISSN 2583-0333

4.7 User Satisfaction Evaluation

User satisfaction was evaluated through an appraisal conducted on all participants. The appraisal included questions regarding accessibility, overall satisfaction, and usability of the system. Figure 9 illustrates the appraisal results, revealing that 91% of users rated their experience as satisfactory or very satisfactory. The feedback highlighted the effectiveness of the RBAC system in providing secure access while maintaining ease of use.

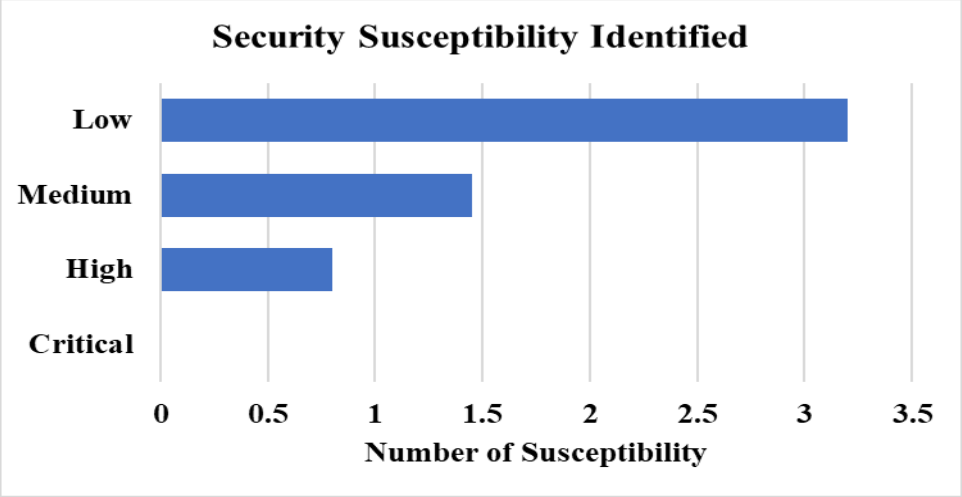


Figure 10. Security Susceptibility Identified

Security Susceptibility: A security evaluation was conducted to assess the effectiveness of the RBAC implementation in securing sensitive data and preventing unauthorised access. This evaluation included penetration testing and vulnerability scanning. This assessment identified a minimal number of vulnerabilities, all of which were promptly addressed. The RBAC implementation effectively restricted access based on user roles, contributing to a robust security posture.

The performance evaluation of a Holistic, Secure Online Result Processing System demonstrates its efficiency in enhancing data integrity, user experience, and security within academic environments. The system's response times, throughput, user satisfaction levels, and holistic security measures show that it meets the research objectives, providing a reliable and secure platform for managing academic results.

5.0 DISCUSSION OF RESULTS

The analysis of the holistic secure online result processing system with role-based access control (RBAC) has proven important and effective in securing overall system performance, data integrity, and user experience within academic environments. The application of RBAC has enabled the specification of user roles, ensuring that maintainers of data integrity, including administrators, HOD, Exams Officers, and students, are assigned based on their permissions. This reduced the risks of data manipulation and unauthorized access, as seen in previous research works that demonstrate the effectiveness of RBAC in ensuring the security of sensitive information (Alshaikh et al., 2021). Also, the delegation of roles and permissions that

characterise RBAC enables automated data entry mechanisms and authentication protocols, which ensure consistency and accuracy in data entry and reduce human errors. Constant, regular audit trails enable accountability, assist in tracking data alterations, strengthen the importance of monitoring, and ensure data integrity (Nguyen et al., 2022).

Based on user experience, the application, designed with user-centred values, shows meaningful gratification among users. Usability testing revealed that stakeholders appreciated the ease of navigation and user interface, which demonstrated the workflow's efficiency in uploading and downloading records, registering courses, and verifying results. The opportunities for comprehensive training on the use of resources gave and bolstered users' confidence in working on the system effectively. The system's Performance evaluation demonstrates its capability to handle concurrent user demands. Notably, average response times for main operations remained within acceptable limits, and system throughput confirmed the system's ability to support a high volume of transactions. All these tests are significant in academic settings, where timely result processing is essential. For the system to enhance user trust, data synchronisation is necessary to ensure that all records are updated simultaneously, thereby preventing inconsistencies within the system.

During the implementation of the online result processing system developed by Dada et al. (2024) to enhance the work of Dada et al. (2017), several challenges arose during the implementation stage. There were a few difficulties that occurred when integrating with existing systems, most especially with data format alignment and compatibility. Additionally, user training sessions revealed some conflict in adapting to the new process, highlighting the need for ongoing transformation in IT support and encouragement. The findings from this research demonstrate the potential of a holistic, secure online result processing system utilising RBAC to streamline academic workflows, enhance data integrity, and improve user experience and confidentiality, while also addressing the challenges inherent in implementing previous result processing systems.

6.0 CONCLUSION

This research presents a holistic, secure online result processing system using role-based access control (RBAC) to ensure data integrity in academic institutions. This paper builds upon the work of Dada et al. (2024). By defining user roles clearly, the system effectively minimised unauthorised access and enhanced data integrity. This system minimises manual errors, streamlines processing results, and establishes audit trails, promoting accountability and transparency. User-centred design principles enhance usability, leading to consistently high user satisfaction ratings. Performance evaluations indicate that the system efficiently manages high transaction volumes, which is essential for timely result processing in academic settings. While the implementation faced challenges, such as integrating with legacy systems and network scalability, the research provides valuable insights into the technology's Role in improving educational procedures. The global findings highlight the importance of data security, integrity, and user experience in upholding academic confidentiality in a digital world. However, educational institutions can ensure that their academic record management systems are reliable, secure, and capable of handling the evolving demands of the digital age by staying current with innovations and adapting to new needs.

REFERENCES

Abah, J. A., Honmane, O., Age, T. J., and Ogbule, S. O. (2022). Design of Single-User-Mode Computer-Based Examination System for Senior Secondary Schools in Onitsha North Local Government Area of Anambra State, Nigeria. VillageMath Educational Review (VER), 3(1).

Akputu, O. K., Attai, K. F., Usoro, A., & Abiodun, A. O. (2020). Policy-Driven Academic Result Computation and Transcription: Ritman University Case. Policy, 9(1).

Bian, G.; Zhang, F.; Li, R.; Shao, B. (2022). Certificateless Remote Data Integrity Auditing with Access Control of Sensitive Information in Cloud Storage. Electronics 2022, 11, 3116. https://doi.org/10.3390/ electronics11193116

DADA O. M., ADEDOTUN K. J., OYEDEPO F. S. & RAJI A. K. (2024). Leveraging Role-Based Access Control for Secure and Efficient Result Processing in Academic Environments. (JESTP); Journal of Educational Studies, Trends & Practice October, 2024 www.ssaapublications.com S

Dada O. M., Raji A. K., Oyedepo F. S., Yusuf I. T. & Saka T. O (2017). Design and Implementation of an Integrated Result Processing System in a Networked Environment. Published in Biomedical Statistics and Informatics, September 2017; Vol. 2 No. 5, 131–137. Available at http://www.sciencepublishinggroup.com/j/bsi.

Damasevicius, R., Maskeliunas, R., & Leon, M. (2019). Development of an Online Clearance System for an Educational Institution. In Applied Informatics: Second International Conference, ICAI 2019 (p. 327).

Daniel. S, and Sylvia L. O. (2017). Current Research and Open Problems in Attribute-Based Access Control ACM Comput. Surv. 49, 4 (2017), 65.

David F. D., Richard K., and Ramaswamy C. (2003). Role-based Access Control. Artech House.

Dranger, S, Sloan, R. H, & Solworth, J. A. (2006). The complexity of discretionary access control. In Proceedings of the International Workshop on Security. Springer, 405–420.

Edison, H., Wang, X., & Conboy, K. (2021). Comparing methods for large-scale agile software development: A systematic literature review. IEEE Transactions on Software Engineering, 48(8), 2709–2731.

Ekanem, A. J., Ozuomba, S., & Jimoh, A. J. (2017). Development of Students' Result Management System: A case study of the University of Uyo. Mathematical and Software Engineering, 3(1), 26–42.

Ferraiolo, D., Chandramouli, R., Kuhn, R. & Hu, V. (2016). "Extensible access control markup language (XACML) and next generation access control (NGAC)", in Proceedings of the 2016 ACM International Workshop on Attribute-Based Access Control, pp. 13–24.

Klaedtke F, Ghassan O, Roberto B, & Heng C. (2014). Access control for SDN controllers. In Proceedings of the 3rd Workshop on Hot Topics in Software Defined Networking. 219–220.

Hu V.C., Kuhn R.D., Ferraiolo D.F., and Voas J. (2015). Attribute-based access control. Computer 48, 2 (2015), 85–88.

Indrakshi R, and Mahendra K.(2006). Toward an allocation-based mandatory access control model.Comput.Secure. 25, 1 (2006), 36–44

Indrakshi Ray and Mahendra

Kumar. (2006). Towards a location-based mandatory access control model.Comput.Secure. 25, 1 (2006), 36–

John M. (1985). A comment on the "basic security theorem" of Bell and LaPadula. Inform. Process. Lett. 20, 2 (1985), 67–70.

Klaedtke F, Ghassan O, Roberto B, & Heng C. (2014). Access control for SDN controllers. In Proceedings of the 3rd Workshop on Hot Topics in Software Defined Networking. 219–220.

Megouache..L, Zitouni. A., Djoudi, M. (2020). Ensuring user authentication and data integrity in a multi-cloud environment. Human-centric Computing and Information Sciences, 2020, 10 (1), 10.1186/s13673-020-00224-y. HAL-03125583 HAL Id: hal-03125583 https://hal.science/hal-03125583v1 Submitted on 29 Jan 2021

Mishra, A., & Alzoubi, Y. I. (2023). Structured software development versus agile software development: a comparative analysis. International Journal of System Assurance Engineering and Management, 14(4), 1504–1522.

Ninghui L., & Mahesh V. T. (2005). On safety in discretionary access control. In Proceedings of the IEEE Symposium on Security and Privacy (S&P'05). IEEE, 96–109.

Okikiola, M. A., & Samuel, F. (2016). Optimising the processing of results and generation of transcripts in Nigerian universities through the implementation of a friendly and reliable web platform. Imperial Journal of Interdisciplinary Research, 2, 12.

Olamide, O. O., & Joshua, A. O. (2012). Design and simulation of an SMS-driven microcontroller for home automation using the Proteus software. Journal of Computer Science Department. University of Lagos.

Onibere, E. I. (2013). Fuzzy logic modelling of a performance evaluation system for academic programmes in Nigeria's higher education. Data Management and Security: Applications in Medicine, Sciences and Engineering, 45, 113.

Osunade, O., Ayinla, I. B., & Aduroja, O. O. (2019). Design and Implementation of a Centralised University Result Processing and Transcript System: A case study of the

University of Ibadan. International Journal of Computing Sciences Research, 2(3), 89–101.

Otu. G.A., Iheagwara S.E., Okafor A.C. (2023), Enhancing Data Integrity of Student Registration Input Using Integration of Secure Program Development Technique. International Journal of Scientific Engineering and Research (IJSER) ISSN (Online): 2347-3878 Impact Factor (2020): 6.733 Volume 11 Issue 7, July 2023 www.ijser.in Licensed Under Creative Commons Attribution CC BY

Ravi S. S. (1995). Rationale for the RBAC96 family of access control models. In Proceedings of the First ACM Workshop on Role-Based Access Control (RBAC'95), C. E. Youman, R. S. Sandhu, and E. J. Coyne (Eds.). ACM Press, New York, NY.

Ravi S. S, Edward J. C, Hal L. F, and Charles E. Youman. (1996). Role-based access control models. Computer 29, 2 (1996), 38–47. [87]

Ravi S, Venkata B, and Qamar M. (1999). The ARBAC97 model for role-based access control administration. ACM Trans. Inf. Syst. Secur. 2, 1 (1999), 105–135.

Sandhu, R., Coyne, E.J., Youman, C.E. & Feinstein, H.L. (1996). "Role-based access control models", Computer, Vol. 29No.2, pp. 38-47, doi:10.1109/2.485845.

Simon P. and Saad K. (2022). A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective. ACM Comput. Surv. 55, 6, Article 123 (December 2022), 28 pages. https://doi.org/10.1145/3533703 Citation:

Ufuoma J. O, Edith O, Abel E. E. & Irene A. (2024). Ensuring Data Integrity in API-Enabled Student Transcript and Result Management System; International Journal of Trend in Research and Development, Volume 11(3), ISSN: 2394-9333 www.ijtrd.com IJTRD | May – Jun 2024 Available Online@www.ijtrd.com

Vincent C. Hu, D. Richard Kuhn, David F. Ferraiolo, and Jeffrey Voas. (2015). Attribute-based access control. Computer 48, 2 (2015), 85–88.

Wang, J. M., Ching-Kuang S., S. C., & Chaoli W. (2017). UNIXvisual: A visualisation tool for teaching UNIX permissions. In Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education. 194–199

Xin. J, Ram. K, and Ravi S. (2012). A unified attribute-based access control model covering DAC, MAC and RBAC. In Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy. Springer, 41–55.

Zhang Y, Zheng D, and Deng R.H. (2018). Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet Things J. 5, 3 (2018), 2130–2145.

