ISSN: 2581-1274

Development and Operational Evaluation of a Layered Authentication-Based Access-Control Framework for Secure Institutional EBook Distribution

Lingga Kurnia Ramadhani [a,1], Bajeng Nurul Widyaningrum [b,2*], Wahyu Wijaya Widiyanto [c,3]

[a] *Information Systems and Technology, Universitas Ivet, Semarang 50233, Indonesia*
[b] *Medical Records and Health Information, Politeknik Bina Trada, Semarang 50166, Indonesia*
[c] *Bachelor of Applied Health Information Management, Politeknik Indonusa Surakarta, Surakarta 57142, Indonesia*
[1] *Linggakurniaramadhani@unisvet.ac.id;* [2] *bnwidyani@gmail.com;* [3] *wahyuwijaya@poltekindonusa.ac.id*
** corresponding author*
Contact number/WA: +62 811-2755-919

ARTICLE INFO

Article history:
Published
August 28, 2026

Keywords:
Secure eBook distribution; Layered access control; Single-session enforcement; Transaction-gated authorization; Protected content delivery

ABSTRACT

Secure eBook delivery in educational institutions requires coordinated identity, session, entitlement, and content-delivery controls. Existing studies frequently evaluate these controls separately, leaving limited evidence on how they operate as a traceable decision chain in a lightweight institutional platform. This study develops and operationally evaluates a layered authentication-based access-control framework for secure web-based eBook distribution. The framework applies deny-by-default and complete-mediation principles through four enforcement layers: credential authentication, single-session validation, role-and-transaction authorization, and server-mediated eBook viewing. A design-and-evaluation approach based on the Waterfall model was used for requirements analysis, architecture design, PHP-MySQL implementation, control-validation testing, and operational deployment. Evaluation combined 18 black-box functional scenarios with 11 security-control decision cases covering invalid credentials, role violations, concurrent login, session expiry or reuse, pending transaction status, direct URL access, and download restriction. The deployed instance contained 153 registered users, 151 eBook transactions, 29 pending verifications, and six published eBooks. All 18 functional scenarios and all 11 security decisions matched the expected outcomes; nine prohibited or invalid requests were blocked or invalidated, while two authorized requests were permitted. The contribution is a context-specific, auditable policy-enforcement chain linking identity, session state, entitlement, and protected content delivery. The framework is not a substitute for cryptographic Digital Rights Management and was not evaluated for latency, throughput, penetration resistance, or large-scale load. It provides a lightweight baseline for institutions requiring controlled eBook access and a clear path toward watermarking, encryption, and performance benchmarking.

I. Introduction

Digital learning environments increasingly depend on eBooks because they reduce distribution constraints and allow students and educators to access learning materials across locations and schedules [1], [2]. This convenience, however, changes the protection problem. A digital file can be copied, forwarded, or redistributed at negligible cost, so institutions must control not only who enters a platform but also whether a particular user remains entitled to a specific resource throughout the access session [3], [4].

Digital Rights Management (DRM) can combine encryption, licensing, and usage restrictions, but comprehensive DRM commonly introduces implementation cost, infrastructure complexity, and administrative overhead [5]. For small educational institutions and independent publishers, a lighter

control architecture may therefore be preferable, provided that its security claims are limited to the controls actually implemented and tested.

Access-control engineering distinguishes identity verification from authorization and continuous enforcement. Role-Based Access Control (RBAC) assigns privileges according to organizational roles [6], while NIST and OWASP guidance emphasizes least privilege, deny-by-default decisions, session integrity, complete mediation of protected requests, and resistance to broken access control [8], [11]-[15], [19]-[25]. These principles imply that successful login alone is insufficient: every eBook request should also be checked against current session state, role, entitlement, and the permitted delivery channel.

Recent work demonstrates the value of individual security components but also shows their separation across application contexts. Authorization research has examined database access-control requirements and broken-access-control attacks [16], [17], while a trusted-content framework has addressed content authorization in social-media environments [18]. Within Jurnal INOTERA, Hardiansyah et al. developed a low-cost key-management API that protects cryptographic keys through SoftHSM and PKCS#11 [28], whereas Angelika and Nurhasanah evaluated biometric authentication and active access control for an IoT smart-door system [29]. These studies strengthen specific controls—key custody or identity authentication—but do not establish an end-to-end entitlement chain for institutional eBook distribution.

The unresolved problem is therefore not the absence of authentication technology, but the lack of a traceable and lightweight policy chain that binds authenticated identity to a valid session, a permitted role, a verified eBook transaction, and server-mediated viewing. A user who passes one control should not bypass the remaining controls through account sharing, direct URL manipulation, session reuse, or a pending entitlement state.

This study addresses that gap by developing and operationally evaluating a layered Authentication-Based Access-Control Framework for an institutional web-based eBook platform. The study asks two questions: (1) can the proposed layers consistently produce the intended permit-or-deny decision across functional and security-control scenarios, and (2) what practical contribution and limitations emerge when the framework is deployed in a lightweight PHP-MySQL environment? The contribution is not a new cryptographic primitive. It is a context-specific reference architecture, a traceable decision rule, and an operational evaluation that explicitly separates demonstrated control correctness from performance and penetration-security claims.

II. Security Rationale and Proposed Framework

A. Security Engineering Basis

The framework is grounded in five complementary principles. First, deny-by-default requires a request to be rejected unless every required condition is satisfied. Second, least privilege limits users and administrators to actions associated with their roles. Third, separation of duties distinguishes user access, transaction verification, content administration, and platform administration. Fourth, complete mediation requires authorization to be checked at each protected request rather than only at login. Fifth, defense in depth places several independent checks between a user and the eBook resource [8], [14], [15], [19]-[25].

For user u, eBook e, requested action a, session s, and transaction state t, the framework applies the following decision rule:

$$Permit(u,e,a,s,t) = Auth(u) \wedge ValidSession(u,s) \wedge RoleAllows(u,a) \wedge Entitled(u,e,t) \wedge ProtectedDelivery(e) \quad (1)$$

A request is permitted only when all predicates are true. Failure at any predicate terminates the decision path and returns an access-denied response. This conjunctive rule makes the enforcement logic auditable and prevents a successful credential check from being treated as permanent authorization.

B. Authentication Layer

The Authentication Layer validates submitted credentials against registered user records. Invalid credentials are rejected before a session is created. This layer establishes identity but does not

independently authorize eBook access; it only allows the request to proceed to session and entitlement checks [11], [13].

C. Session Control Layer

The Session Control Layer validates the active session on each protected request and enforces a single-session policy for the same account. A concurrent login invalidates the previous session, while expired or reused sessions are denied. The mechanism reduces casual credential sharing and maintains a current link between the authenticated identity and the request [12], [20], [21].

D. Role and Transaction Authorization Layer

The Access-Control Layer evaluates both role permission and transaction-derived entitlement. Administrative roles may manage users, eBooks, access assignments, and transaction records, whereas standard users may access only eBooks linked to an authorized transaction. A pending transaction does not satisfy the entitlement predicate. Combining role and transaction state narrows access from general platform membership to resource-specific authorization [6], [16], [23]-[25].

E. Protected EBook Delivery Layer

The EBook Protection Layer serves content through an embedded viewer after all upstream checks succeed. Direct file URLs and download-oriented requests are rejected, so the application—not a publicly exposed path—mediates content delivery. This control reduces straightforward redistribution, although it cannot prevent screen capture, photography, or compromise of an authorized endpoint; stronger protection would require watermarking, encryption, or digital fingerprinting.

F. Framework Workflow

The workflow begins with credential submission and proceeds sequentially through session validation, role-and-transaction authorization, and protected viewing. The database stores user, role, session, transaction, eBook, and access-log records. Because every layer returns a binary permit-or-deny outcome, a failed check stops the workflow and prevents delivery. Figure 1 summarizes the enforcement chain and its fail-closed behavior.

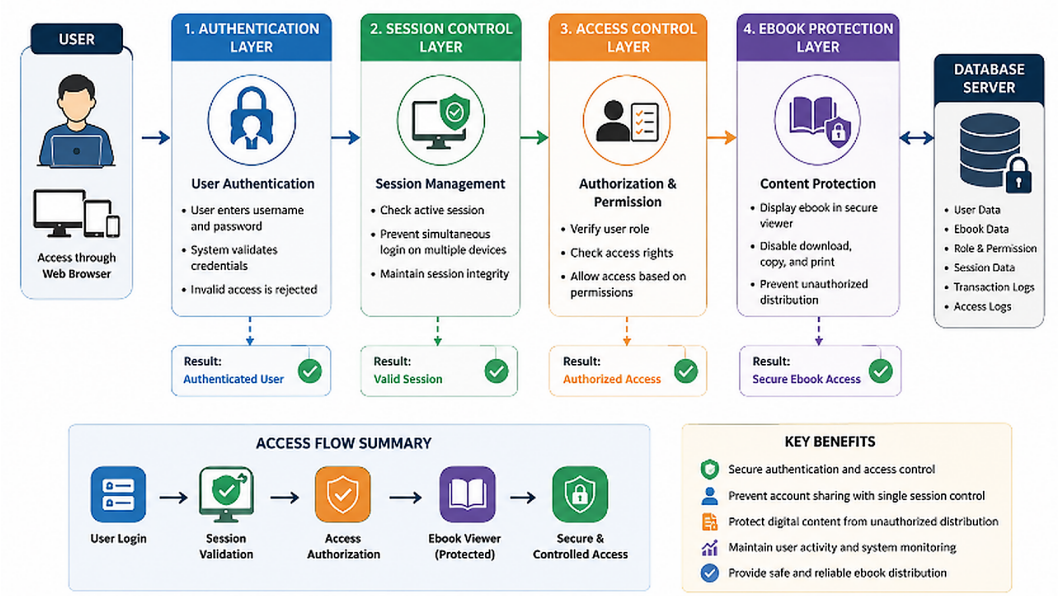


Fig. 1. Layered policy-enforcement chain. An eBook request is delivered only when identity, session, role and transaction entitlement, and protected-viewer checks all succeed; failure at any layer produces a deny-by-default decision

G. Research Positioning and Contribution

Table 1 positions the framework against representative recent work. The comparison focuses on the research object, enforcement scope, evaluation evidence, and unresolved gap rather than presenting feature checkmarks as proof of novelty. The scientific contribution is the explicit coupling

and traceability of controls within the eBook-access lifecycle, supported by an operational decision matrix and bounded claims.

Table 1. Research positioning of the proposed framework against representative security studies

Study	Primary security focus	Evaluation evidence	Gap relative to this study
Mohamed et al. [16]	Authorization requirements across database models	Systematic literature review	Does not implement an institutional eBook entitlement chain
Han et al. [18]	Trusted content authorization for social media	Framework design and application analysis	Different content context; no single-session or transaction-gated eBook access
Hardiansyah et al. [28]	Cryptographic key lifecycle using SoftHSM and PKCS#11	API implementation and functional validation	Protects key custody; does not govern user-to-eBook access lifecycle
Angelika and Nurhasanah [29]	Biometric authentication and active IoT access control	Prototype and black-box testing	Identity modality is emphasized; no digital-content entitlement workflow
Proposed framework	Identity, session, role, transaction entitlement, and protected eBook delivery	Operational deployment, 18 functional scenarios, and 11 security decisions	Context-specific layered framework; performance and penetration evaluation remain future work

III. Method

A. Research Design and Scope

This study used a design-and-evaluation software-engineering approach. The development process followed the Waterfall sequence of requirement analysis, system design, implementation, testing, and deployment because the core requirements and access rules were specified before implementation [26]. The unit of evaluation was the system response to predefined functional and security-control scenarios; the study did not evaluate human learning outcomes or user behavior.

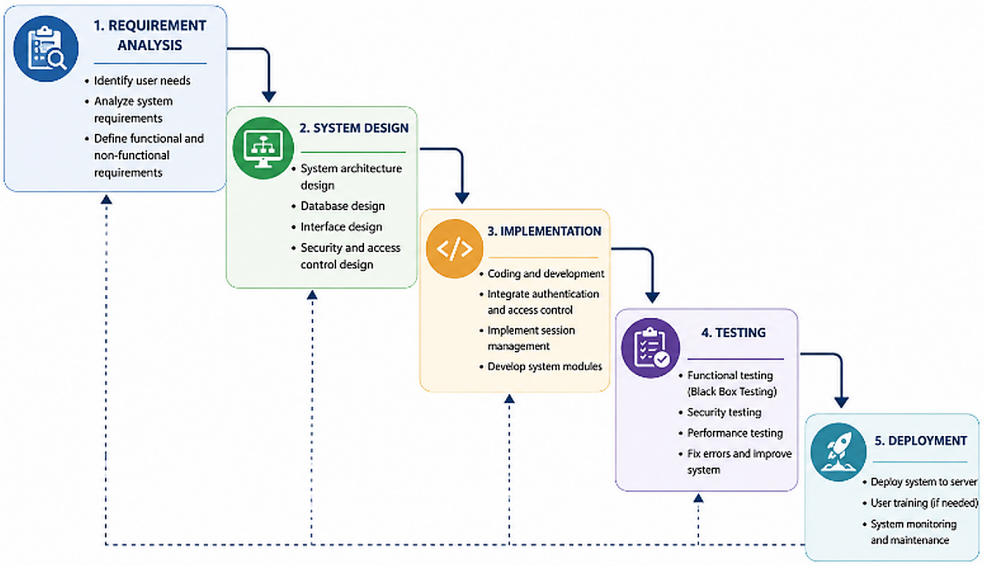


Fig. 2. Sequential design-and-evaluation workflow. Security requirements are traced through architecture design, implementation, control-validation testing, deployment, and corrective feedback.

B. Requirements and Operational Data

Requirements were derived from observation of existing eBook-distribution practices and analysis of recurrent risks: unauthorized credential use, simultaneous account access, privilege misuse, access

before transaction verification, direct URL manipulation, expired-session reuse, and direct download. The resulting functional requirements were user authentication, role management, transaction verification, session control, eBook administration, access logging, and protected viewing. Security requirements were expressed as expected permit-or-deny decisions for each threat scenario.

The operational dataset comprised aggregate records from the deployed platform: 153 registered users, six published eBooks, 151 eBook transactions, and 29 transactions awaiting verification. Only aggregate counts are reported; no identifiable user records are presented or analyzed.

C. System Design and Implementation

The system adopted a client-server architecture. Users interacted through a web browser, while authentication, authorization, session validation, transaction checks, and content delivery were executed by the application server. User, eBook, session, role, transaction, and access-log data were stored in MySQL. The server-side application was implemented in PHP and organized into authentication, session-management, access-control, transaction-management, eBook-management, protected-viewer, and administrative-monitoring modules.

The architecture used server-mediated decisions rather than exposing eBook files through unrestricted public links. The implementation therefore operationalized the decision rule in Section II: each viewer request had to satisfy identity, session, role, entitlement, and delivery-channel conditions before the eBook was rendered.

D. Test Protocol and Evaluation Criteria

Functional testing used a black-box approach in which predefined inputs were submitted through the user interface and the observed outputs were compared with expected outcomes [27]. Eighteen functional scenarios covered authentication, authorization, session management, transaction processing, eBook access, and administrative operations. The manuscript reports both the aggregate result and representative cases so that the 100% pass rate is not interpreted as evidence beyond the tested functions.

Security-control testing evaluated 11 explicit permit-or-deny decisions: valid single login, invalid credentials, concurrent login, role-prohibited administrative access, session timeout, unauthorized session reuse, authorized eBook access with a valid entitlement, pending transaction status, direct URL access, expired-session eBook access, and download restriction. Testing followed OWASP guidance for authentication, session management, authorization bypass, and insecure direct object references [11], [12], [19]-[25].

Three descriptive indicators were calculated:

$$FSR = \frac{\text{passed functional scenarios}}{\text{total functional scenarios}} \times 100\% \quad (2)$$

$$ADC = \frac{\text{correct permit-or-deny decisions}}{\text{total security decisions}} \times 100\% \quad (3)$$

$$PBR = \frac{\text{blocked or invalidated prohibited requests}}{\text{total prohibited requests}} \times 100\% \quad (4)$$

The evaluation is a deterministic control-validation study, not a performance benchmark or penetration test. Authentication latency, throughput, resource consumption, vulnerability-scanner findings, and load behavior were not instrumented in the available deployment records. These boundaries are stated explicitly to prevent the functional pass rate from being interpreted as comprehensive security assurance.

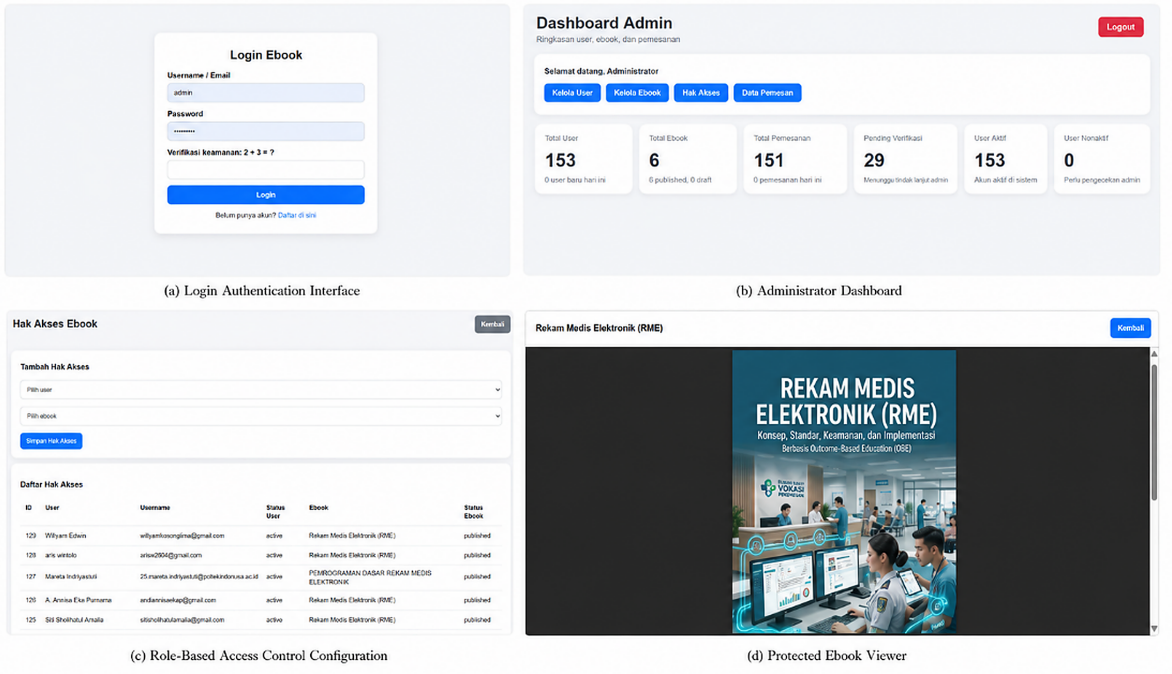
IV. Results and Discussion

A. Operational Deployment Evidence

The framework was deployed as an operational web-based eBook platform. Table 2 summarizes the available deployment evidence. Of 151 recorded transactions, 29 (19.2%) remained pending verification, showing that the platform maintained a distinguishable pre-authorization state rather than automatically converting every transaction into eBook entitlement.

Table 2. Aggregate characteristics of the deployed eBook platform

Indicator	Value	Interpretation
Registered users	153	Accounts available for authentication and role assignment
Published eBooks	6	Protected digital collections managed by the platform
Recorded eBook transactions	151	Transactions processed by the entitlement workflow
Pending verification	29 (19.2%)	Transactions not yet satisfying verified-entitlement status
Active users	153	Accounts enabled in the deployment snapshot
Inactive users	0	No account marked inactive in the deployment snapshot



(a) Login Authentication Interface (b) Administrator Dashboard

(c) Role-Based Access Control Configuration (d) Protected Ebook Viewer

Fig. 3. Operational interfaces representing the principal enforcement points: credential authentication, administrative monitoring, role and eBook-entitlement assignment, and server-mediated protected viewing.

B. Functional and Security-Control Results

All 18 functional scenarios produced the specified outputs, yielding an FSR of 18/18 (100%). The security-control matrix also produced the expected decision in all 11 cases, yielding an ADC of 11/11 (100%). Nine invalid or prohibited requests were blocked or invalidated (PBR = 9/9, 100%), while two authorized requests were permitted. These values establish correctness for the defined test set; they do not estimate the probability of resisting unseen attacks.

Table 3. Quantitative summary of the operational evaluation

Evaluation indicator	Correct / total	Rate	Meaning
Functional success rate	18 / 18	100%	All predefined functional scenarios matched expected outputs
Access-decision correctness	11 / 11	100%	Every documented permit-or-deny decision matched the policy
Prohibited-request blocking rate	9 / 9	100%	All invalid or prohibited requests were blocked or invalidated
Authorized-request preservation	2 / 2	100%	Legitimate login and entitled eBook access remained available

Table 4. Authentication, authorization, and session-control decision matrix

Scenario	Expected policy decision	Observed result	Status
Valid single login	Create one active session	Session created	Pass
Invalid credentials	Deny authentication	Access denied	Pass
Concurrent login with identical account	Invalidate the previous session	Previous session terminated	Pass
Role-prohibited administrative request	Deny privileged operation	Access denied	Pass
Session timeout	Require reauthentication	Session invalidated	Pass
Unauthorized session reuse	Deny protected request	Request blocked	Pass

Table 5. Transaction and eBook-protection decision matrix

Scenario	Expected policy decision	Observed result	Status
Authorized user with verified entitlement	Open protected viewer	EBook accessible	Pass
Pending or unverified transaction	Withhold eBook entitlement	Access not granted	Pass
Direct eBook URL request	Deny server bypass attempt	Access denied	Pass
EBook request after session expiry	Deny and require login	Access denied	Pass
Direct download attempt	Keep content within controlled viewer	Download restricted	Pass

C. Interpretation of the Findings

The results show that the framework operated as a coherent policy chain rather than as a collection of independent interface features. Invalid credentials were stopped before session creation; session anomalies were invalidated before authorization; role and transaction state narrowed access to a specific eBook; and the viewer mediated delivery after the preceding checks succeeded. This traceability is the main empirical contribution of the implementation.

The findings extend conventional RBAC by binding role permission to session validity and resource-specific transaction entitlement. The systematic review by Mohamed et al. [16] identifies the diversity of authorization requirements across data models, while Anas et al. [17] emphasize that broken access control frequently arises when authorization checks are missing or inconsistently applied. The present framework addresses that problem through complete mediation of viewer requests, although its effectiveness has only been demonstrated for the reported scenarios.

The trusted-content framework reported by Han et al. [18] similarly recognizes that content protection requires authorization beyond identity verification. The present work differs in its institutional eBook context and in the use of transaction status as an entitlement attribute. The distinction matters because a registered user may be legitimate at the platform level but still lack permission for a particular eBook.

The two INOTERA studies are complementary rather than direct substitutes. The SoftHSM-based KMS by Hardiansyah et al. [28] secures the lifecycle and non-exportability of cryptographic keys, a capability that could strengthen future encryption of eBook files. The iris-based smart-door system by Angelika and Nurhasanah [29] demonstrates active authentication and access response in a physical IoT setting. In contrast, the present study focuses on continuous digital-content authorization after identity has been established.

D. Practical Implications and Trade-Offs

For educational institutions, the framework offers a deployable baseline when full DRM infrastructure is financially or operationally disproportionate. It centralizes access decisions, provides an auditable transaction gate, and reduces casual account sharing and direct-link distribution. The architecture can also be adapted to institutional modules, reports, proceedings, and other controlled digital publications.

The controls introduce several trade-offs. Single-session enforcement improves account control but may inconvenience legitimate users who change devices or browsers. Transaction verification

strengthens entitlement governance but may delay access when administrative verification is slow. Controlled viewing reduces direct downloading but cannot prevent screen capture or recording by an authorized user. A centralized session store may also become a bottleneck as concurrent usage grows.

Production deployment should therefore complement the framework with Transport Layer Security, secure password hashing, rate limiting, CSRF protection, security logging, backup and recovery procedures, dependency patching, and periodic authorization testing in accordance with NIST and OWASP guidance [8], [11]-[15], [19]-[25]. For distributed deployment, session revocation and entitlement checks may require a shared cache or token-introspection service to preserve consistent decisions across application nodes.

E. Limitations and Future Evaluation

Four limitations define the scope of the evidence. First, the deployment involved 153 accounts, six eBooks, and 151 transactions, so large-scale behavior is unknown. Second, the evaluation measured deterministic decision correctness rather than authentication latency, viewer response time, throughput, or computational overhead. Third, no independent penetration test, dynamic application security test, or source-code review was reported. Fourth, viewer restriction does not provide cryptographic control after content is displayed on an authorized device.

Future research should conduct repeated performance experiments under controlled concurrency, report latency distributions and throughput, apply OWASP ASVS and Web Security Testing Guide test cases, and use independent penetration testing. The framework can also be extended with per-user watermarking, encryption and managed keys, device-risk signals, anomaly detection, and revocable offline access. Comparative studies should quantify the incremental overhead and protection benefit of each added layer.

V. Conclusion

This study contributes a layered and auditable access-control model for institutional eBook distribution. Its distinctive element is the explicit policy chain that links authenticated identity, single-session validity, role permission, transaction-derived entitlement, and protected content delivery. Operational evaluation showed correct outcomes for all 18 functional scenarios and all 11 reported security decisions in a deployment containing 153 users, 151 transactions, and six eBooks.

The findings support the framework as a lightweight control baseline, not as equivalent to cryptographic DRM or as proof of comprehensive application security. Its practical value lies in making each access decision traceable and in preventing straightforward credential sharing, unauthorized role use, pending-entitlement access, direct URL bypass, expired-session reuse, and direct download within the evaluated conditions. Further claims about scalability and attack resistance require instrumented performance testing, independent security assessment, and stronger post-delivery protection.

References

[1] OECD, OECD Digital Education Outlook 2023: Towards an Effective Digital Education Ecosystem. Paris, France: OECD Publishing, 2023, doi: 10.1787/c827b81a-en.

[2] R. Pitt, “Open Textbooks in Higher Education Teaching,” in Distributed Learning Ecosystems: Concepts, Resources, and Repositories, Wiesbaden, Germany: Springer VS, 2023, pp. 97–113, doi: 10.1007/978-3-658-38703-7_6.

[3] World Intellectual Property Organization, Completion Report of the Project on Copyright and the Distribution of Content in the Digital Environment, CDIP/31/6, Geneva, Switzerland, 2023. [Online]. Available: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=620344. [Accessed: Jun. 10, 2026].

[4] World Intellectual Property Organization, “Copyright in the Digital Environment,” WIPO, 2026. [Online]. Available: https://www.wipo.int/en/web/copyright/activities/digital. [Accessed: Jun. 10, 2026].

[5] W. M. Volckmann II, “A model of digital rights management with user disutility,” Journal of Industrial and Management Optimization, vol. 20, no. 1, pp. 282–310, 2024, doi: 10.3934/jimo.2023069.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38–47, 1996, doi: 10.1109/2.485845.

[7] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, 2014, doi: 10.6028/NIST.SP.800-162.

[8] Joint Task Force, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Rev. 5, 2020, doi: 10.6028/NIST.SP.800-53r5.

[9] I. Gamayanto, D. Kurniawan, and R. Prasetyo, "Security evaluation of Keycloak-based role-based access control in microservice architectures using the OWASP ASVS framework," Journal of Applied Informatics and Computing, vol. 9, no. 6, 2025. [Online]. Available: https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/11604.

[10] Y. Yuricha and I. K. Phan, "Penerapan role based access control dalam sistem supply chain management berbasis cloud," MALCOM: Indonesian Journal of Machine Learning and Computer Science, vol. 3, no. 2, pp. 339–348, 2023, doi: 10.57152/malcom.v3i2.1259.

[11] OWASP Foundation, "Authentication Cheat Sheet," OWASP Cheat Sheet Series, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html. [Accessed: Jun. 10, 2026].

[12] OWASP Foundation, "Session Management Cheat Sheet," OWASP Cheat Sheet Series, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html. [Accessed: Jun. 10, 2026].

[13] R. Galluzzo, A. Regenscheid, D. Temoshok, and C. LaSalle, Incorporating Syncable Authenticators Into NIST SP 800-63B, NIST Special Publication 800-63Bsup1, 2024, doi: 10.6028/NIST.SP.800-63Bsup1.

[14] OWASP Foundation, "A01:2025 Broken Access Control," OWASP Top 10, 2025. [Online]. Available: https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/. [Accessed: Jun. 10, 2026].

[15] OWASP Foundation, OWASP Application Security Verification Standard 5.0.0, 2025. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/. [Accessed: Jun. 10, 2026].

[16] A. Mohamed, D. Auer, D. Hofer, and J. Küng, "A systematic literature review of authorization and access control requirements and current state of the art for different database models," International Journal of Web Information Systems, vol. 20, no. 1, pp. 1–23, 2024, doi: 10.1108/IJWIS-04-2023-0072.

[17] A. Anas, S. Elgamal, and B. Youssef, "Survey on detecting and preventing web application broken access control attacks," International Journal of Electrical and Computer Engineering, vol. 14, no. 1, pp. 772–781, 2024, doi: 10.11591/ijece.v14i1.pp772-781.

[18] J. Han, Q. Li, Y. Xu, Y. Zhu, and B. Wu, "Design of a trusted content authorization security framework for social media," Applied Sciences, vol. 14, no. 4, Art. no. 1643, 2024, doi: 10.3390/app14041643.

[19] OWASP Foundation, Web Security Testing Guide, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/. [Accessed: Jun. 10, 2026].

[20] OWASP Foundation, "WSTG: Session Management Testing," OWASP Web Security Testing Guide, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/README. [Accessed: Jun. 10, 2026].

[21] OWASP Foundation, "Testing for Session Management Schema," OWASP Web Security Testing Guide, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/06-Session_Management_Testing/01-Testing_for_Session_Management_Schema. [Accessed: Jun. 10, 2026].

[22] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos, Digital Identity Guidelines: Authentication and Lifecycle Management, NIST Special Publication 800-63B, 2020, doi: 10.6028/NIST.SP.800-63B.

[23] OWASP Foundation, "Authorization Cheat Sheet," OWASP Cheat Sheet Series, 2025. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html. [Accessed: Jun. 10, 2026].

[24] OWASP Foundation, "Testing for Bypassing Authorization Schema," OWASP Web Security Testing Guide, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/02-Testing_for_Bypassing_Authorization_Schema. [Accessed: Jun. 10, 2026].

[25] OWASP Foundation, "Testing for Insecure Direct Object References," OWASP Web Security Testing Guide, 2025. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References. [Accessed: Jun. 10, 2026].

[26] R. S. Pressman and B. R. Maxim, Software Engineering: A Practitioner's Approach, 9th ed. New York, NY, USA: McGraw-Hill, 2020.

[27] S. H. Putri and H. Prasetiya, "Pengujian software testing sistem ERP PT XYZ dengan metode black box testing," Kurawal: Jurnal Teknologi, Informasi dan Industri, vol. 6, no. 1, pp. 15–29, 2023, doi: 10.33479/kurawal.v6i1.604.

[28] R. Hardiansyah, Nurhasanah, and F. Ariadi, "Design and implementation of a cryptography key management system API using SoftHSM and PKCS#11," Jurnal Inotera, vol. 11, no. 1, pp. 8–22, 2026, doi: 10.31572/inotera.Vol11.Iss1.2026.ID565.

[29] N. Angelika and Nurhasanah, "Design and construction of an automatic door system based on iris detection using ESP32-CAM and OpenCV using the Rapid Application Development (RAD) method," Jurnal Inotera, vol. 11, no. 1, pp. 190–202, 2026, doi: 10.31572/inotera.Vol11.Iss1.2026.ID581.

[30] S. H. Putri and H. Prasetiya, "Pengujian software testing sistem ERP PT XYZ dengan metode black box testing," Kurawal: Jurnal Teknologi, Informasi dan Industri, vol. 6, no. 1, pp. 15–29, 2023, doi: 10.33479/kurawal.v6i1.604.