Scientific Research Publishing

Open Journal of Social Sciences, 2026, 14(2), 65-84
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Cybersecurity Challenges and Barriers to Implementing Moodle for Blended Learning in Resource-Constrained Universities: A Case Study of Sierra Leone

Munda Jonathan Sahr Lebbie[1], Rahman Mukaila Alade[2], Enikuomehin A. Oluwatoyin[2]

[1]Lagos State University, Lagos, Nigeria
[2]Department of Computer Science, Lagos State University, Lagos, Nigeria
Email: mundajslebbie@yahoo.com

How to cite this paper: Lebbie, M. J. S., Alade, R. M., & Oluwatoyin, E. A. (2026). Cybersecurity Challenges and Barriers to Implementing Moodle for Blended Learning in Resource-Constrained Universities: A Case Study of Sierra Leone. *Open Journal of Social Sciences, 14,* 65-84.
https://doi.org/10.4236/jss.2026.142006

Received: December 24, 2025
Accepted: January 29, 2026
Published: February 2, 2026

Abstract

The expansion of blended learning has positioned Learning Management Systems (LMS) such as Moodle as central infrastructures in higher education. In resource-constrained contexts, however, the secure and effective implementation of such platforms remains a persistent challenge. This study examines the technological, institutional, and cybersecurity barriers affecting the implementation of Moodle for blended learning in Sierra Leonean universities. Adopting a mixed-methods design, the study combines qualitative data from semi-structured interviews, focus group discussions, and document analysis with quantitative survey data collected from educators and students. Qualitative data were analysed thematically, while quantitative data were analysed using descriptive statistics, with integration occurring at the design, analysis, and interpretation stages. The findings reveal that Moodle operates within a fragile digital ecosystem characterised by unstable internet connectivity, unreliable electricity supply, limited access to appropriate digital devices, weak institutional governance frameworks, and low levels of user cybersecurity awareness. These infrastructural and institutional constraints not only disrupt teaching and learning but also heighten exposure to cyber risks, including phishing attacks, weak authentication practices, and delayed system maintenance. The study further demonstrates that cybersecurity vulnerabilities are socially and institutionally patterned, disproportionately affecting users with limited digital resources and training. Conceptually, the findings position cybersecurity as a cross-cutting dimension of digital inequality and institutional capacity rather than a purely technical problem. The study concludes that Moodle's potential to support eq-

uitable and resilient blended learning in Sierra Leone will remain limited unless technological infrastructure, institutional governance, and human cybersecurity capacity are addressed in an integrated manner. It recommends recognising LMS platforms as components of critical information infrastructure and embedding cybersecurity within higher education policy, institutional practice, and capacity-building strategies.

Keywords

Blended Learning, Moodle, Cybersecurity, Digital Inequality, Higher Education, Sierra Leone

1. Introduction

The rapid expansion of blended learning has positioned Learning Management Systems (LMS) such as Moodle as critical infrastructures for teaching, learning, and academic administration in higher education globally (Garrison & Kanuka, 2004; Machado & Tao, 2007). In low- and middle-income countries, LMS platforms are increasingly promoted as solutions for improving access, flexibility, and continuity of learning. However, the assumption that digital platforms can seamlessly enhance educational outcomes often overlooks the structural conditions under which they are implemented, particularly in resource-constrained higher education systems (Selwyn, 2016; van Dijk, 2020).

In Sierra Leone, universities have adopted Moodle within a context characterised by unstable internet connectivity, unreliable electricity supply, limited access to appropriate digital devices, and uneven digital literacy among educators and students (Al-Emran, Malik, & Al-Kabi, 2020; Hodges et al., 2020). These infrastructural and capacity constraints undermine consistent engagement with Moodle and restrict its pedagogical potential. More critically, they create conditions under which digital learning platforms operate within fragile and insecure environments, increasing exposure to system failure and cyber risk.

Beyond infrastructural challenges, the secure governance of Moodle remains underdeveloped. Higher education institutions globally are increasingly targeted by cyber threats such as phishing attacks, data breaches, and ransomware, exploiting both technical vulnerabilities and low levels of user awareness (Zhou & Leung, 2022). In resource-constrained contexts, these risks are intensified by weak institutional cybersecurity policies, limited technical staffing, and inadequate system maintenance (Alotaibi, 2021). Despite Moodle's central role in managing sensitive academic data—including assessment records, personal information, and learning analytics—many universities in Sierra Leone lack comprehensive frameworks for digital safety, cybersecurity governance, and incident response.

Furthermore, existing research on blended learning in Sub-Saharan Africa has tended to focus on access, infrastructure, and pedagogical adoption, with limited

attention to cybersecurity as an embedded dimension of LMS implementation (Mtebe & Raisamo, 2014; Tawiah et al., 2019). Where cybersecurity is discussed, it is often treated as a technical or ICT management issue rather than as a socio-institutional challenge shaped by digital inequality, governance capacity, and user practices (Bijker, Hughes, & Pinch, 2012; Selwyn, 2016). This has resulted in a fragmented understanding of how infrastructural fragility, institutional weaknesses, and human behaviour interact to shape both the effectiveness and security of blended learning systems.

The absence of empirically grounded, context-specific research that integrates technological, institutional, and human-factor dimensions of cybersecurity in Moodle-based blended learning constitutes a significant gap in the literature. Without such evidence, policy responses and institutional interventions risk being partial, reactive, or misaligned with local realities. Consequently, Moodle's potential to support equitable, resilient, and secure blended learning in Sierra Leonean universities remains largely unrealised, while existing digital inequalities may be reinforced rather than reduced (van Dijk, 2020; Warschauer, 2004).

This study therefore addresses this gap by systematically examining the technological, institutional, and cybersecurity barriers affecting the implementation of Moodle for blended learning in Sierra Leonean universities. By positioning Moodle as part of higher education's critical information infrastructure and analysing cybersecurity as a cross-cutting dimension of digital inequality and institutional capacity, the study seeks to generate evidence that can inform more integrated, context-sensitive approaches to blended learning governance and digital resilience.

In response to the identified infrastructural, institutional, and cybersecurity gaps in Moodle-based blended learning, this study addresses the following research questions:

- *What technological and infrastructural barriers affect the implementation of Moodle for blended learning in Sierra Leonean universities*?
- *How do institutional policies and governance frameworks shape cybersecurity practices in Moodle-supported learning environments*?
- *How do user practices and levels of cybersecurity awareness influence vulnerability to cyber risks within blended learning systems*?

2. Aim

The aim of this study is to examine the technological, institutional, and cybersecurity challenges affecting the implementation of Moodle for blended learning in Sierra Leonean universities.

3. Literature Review

This literature review examines scholarly debates and empirical evidence on blended learning, Learning Management Systems (LMS), and cybersecurity within higher education, with particular attention to resource-constrained contexts. Its purpose is threefold: to situate Moodle-based blended learning within global and regional

higher education trends; to examine structural, institutional, and human factors influencing LMS adoption; and to position cybersecurity as an embedded and cross-cutting concern rather than a standalone technical issue (Garrison & Kanuka, 2004; Selwyn, 2016). Guided by socio-technical systems thinking, digital inequality perspectives, and human-factor cybersecurity scholarship, the literature reviewed here is organised to reflect the interaction between pedagogical systems, institutional capacity, user practices, and cybersecurity governance in resource-constrained higher education contexts.

While much of the existing literature treats cybersecurity as a technical or ICT management problem, emerging scholarship recognises that digital security in educational systems is deeply shaped by infrastructure, governance, digital inequality, and user behaviour (Bijker, Hughes, & Pinch, 2012; van Dijk, 2020). Accordingly, this review adopts an integrated approach that progressively links pedagogical foundations, institutional capacity, and cybersecurity risk.

3.1. Blended Learning and Learning Management Systems in Higher Education

Blended learning has emerged as a dominant pedagogical model in higher education, combining face-to-face instruction with online and technology-mediated learning activities (Garrison & Kanuka, 2004). Its evolution reflects broader transformations in educational delivery driven by digitalisation, expanding enrolments, and the demand for flexible and inclusive learning models (Hodges et al., 2020).

Learning Management Systems such as Moodle play a central role in enabling blended learning by supporting content distribution, assessment, learner interaction, and monitoring of academic progress (Machado & Tao, 2007). Moodle's pedagogical affordances include discussion forums, quizzes, assignment management, and collaborative learning tools aligned with constructivist and learner-centred pedagogies (Al-Ajlan & Zedan, 2008; Costello, 2013). Empirical studies suggest that effective LMS use can enhance student engagement and learning outcomes when supported by appropriate institutional and pedagogical structures (Benson, Anderson, & Ooms, 2011).

However, global evidence also demonstrates that LMS effectiveness is highly context-dependent. While studies from high-income contexts often assume stable infrastructure and institutional support, Sub-Saharan African literature highlights uneven adoption shaped by infrastructural deficits, limited technical capacity, and constrained pedagogical integration (Mtebe & Raisamo, 2014; Tawiah et al., 2019). These studies caution against uncritical transplantation of LMS models developed in technologically advanced environments into low-resource contexts.

3.2. Moodle Adoption in Resource-Constrained Higher Education Contexts

In resource-constrained higher education systems, Moodle adoption is shaped primarily by infrastructural and institutional limitations rather than pedagogical

choice. Persistent challenges include unstable internet connectivity, unreliable electricity supply, outdated servers, and limited campus-wide network coverage (Dakowska, 2017; Al-Emran, Malik, & Al-Kabi, 2020). These constraints undermine platform reliability and restrict consistent engagement with LMS tools.

Device access and platform usability further influence Moodle adoption. Studies show that students in low-resource contexts frequently rely on shared devices or smartphones, limiting interaction with advanced LMS functionalities (Mtebe & Raisamo, 2016). Platform usability issues are exacerbated when LMS interfaces are not optimised for low-bandwidth or mobile access, reinforcing minimal or surface-level usage patterns (Haworth, 2021).

Institutional readiness is a critical determinant of LMS sustainability. Readiness encompasses technical staffing, system maintenance routines, staff development, and pedagogical integration strategies (Fresen, 2010). Where Moodle is introduced without corresponding organisational restructuring, implementation tends to be fragmented and dependent on individual initiative rather than institutional systems (Unwin, 2009).

3.3. Digital Inequality and Capacity Gaps in LMS Use

Digital inequality in LMS use extends beyond access to encompass disparities in digital skills, quality of access, institutional support, and user confidence (van Dijk, 2005; Warschauer, 2004). These inequalities significantly shape how students and educators engage with Moodle in resource-constrained contexts.

Staff digital literacy plays a decisive role in pedagogical integration. Lecturers with limited LMS competence often reduce Moodle to a content repository rather than a space for interaction and assessment, limiting its pedagogical potential (Fresen, 2010; Selwyn, 2016). Similarly, students with low digital confidence may avoid participation in online discussions or assessments, reinforcing passive engagement patterns (Quayyum & Freberg, 2023).

Users frequently develop informal coping strategies such as peer support, offline content sharing, or selective feature avoidance (Roberts, 2005). While these workarounds enable functional participation, they also obscure systemic weaknesses and contribute to uneven learning experiences. Resistance to LMS use should therefore be understood as a rational response to cognitive overload and structural constraint rather than simple attitudinal opposition (Oh & Park, 2009).

3.4. Cybersecurity as a Cross-Cutting Challenge in Moodle-Based Learning

Cybersecurity risks in Moodle-based learning environments emerge from the intersection of infrastructural weaknesses, capacity gaps, and institutional governance failures rather than from isolated technical flaws (Zhou & Leung, 2022). Higher education institutions are increasingly targeted by phishing attacks, ransomware, data breaches, and system misuse, with developing countries facing heightened vulnerability due to limited investment in secure digital infrastructure (Alotaibi, 2021).

Infrastructural instability—such as outdated platforms, irregular system updates, and insecure network access—creates technical vulnerabilities that expose LMS platforms to exploitation (Constantin, 2017; Haworth, 2021). At the same time, limited cybersecurity awareness among users translates into behavioural risks, including weak password practices and unsafe access through public networks (Parsons et al., 2017).

As Moodle stores sensitive academic records and personal data, its role increasingly aligns with that of critical information infrastructure within higher education systems (Sierra Leone Cybersecurity Strategy, 2024). Security breaches therefore have implications beyond technical disruption, affecting institutional trust, academic continuity, and data protection.

3.5. Institutional Policy, Governance, and Human-Factor Cybersecurity

Institutional governance frameworks play a central role in shaping cybersecurity outcomes in blended learning systems. Many universities in resource-constrained contexts lack comprehensive cybersecurity policies defining access control, data protection, user responsibility, and incident response (Alotaibi, 2021; Sierra Leone Cybersecurity Strategy, 2024). In such environments, security practices tend to be inconsistent and reactive.

Human-factor cybersecurity models emphasise that users are central to both vulnerability and resilience within digital systems (Sasse, Brostoff, & Weirich, 2001). Risky behaviours are often predictable outcomes of limited training, unclear institutional guidance, and poorly designed systems rather than individual negligence (Parsons et al., 2017). This perspective shifts analytical focus from blaming users to examining institutional responsibility for creating secure digital cultures through training, governance, and system design

3.6. Theoretical Framework for Analysing Moodle Adoption and User Behaviour

To strengthen the explanatory grounding of user behaviour, adoption barriers, and cybersecurity practices in blended learning environments, this article integrates the Technology Acceptance Model (TAM) and Protection Motivation Theory (PMT) as complementary analytical frameworks. Together, these theories provide a robust socio-cognitive lens for understanding both why users adopt or resist MOODLE and how they respond to cybersecurity risks within resource-constrained university contexts.

3.6.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model analytically explains patterns of Moodle adoption by foregrounding how perceived usefulness and perceived ease of use interact with structural constraints to shape behavioural intention and actual system use. Although students and lecturers largely recognise Moodle's functional value for accessing materials and maintaining instructional continuity, their en-

gagement remains limited because ease of use is systematically undermined by infrastructural instability, low digital literacy, and inconsistent institutional support. From a TAM perspective, these constraints elevate the cognitive and practical costs of platform use, thereby weakening the positive effect of perceived usefulness on behavioural intention (Davis, 1989). As a result, users adopt compensatory behaviours—such as restricting use to basic functions—that reflect rational adaptation rather than resistance. This finding reinforces critiques that technology acceptance in low-resource contexts cannot be understood as an individual attitudinal issue but must be analysed as a socio-technical process shaped by organisational capacity and environmental conditions (Fresen, 2010; Selwyn, 2016).

3.6.2. Protection Motivation Theory (PMT)

Protection Motivation Theory provides an analytical framework for understanding cybersecurity behaviour by linking risk perception to users' capacity and motivation to engage in protective action. The study's findings reveal that low levels of perceived vulnerability and severity reduce users' motivation to secure their MOODLE accounts, particularly in contexts where cyber threats are abstract and consequences are not immediately visible. Simultaneously, weak coping appraisal—driven by limited training, ambiguous institutional responsibility, and low self-efficacy—undermines confidence in the effectiveness of protective measures. PMT predicts that when response efficacy and self-efficacy are low and response costs are high, users are unlikely to adopt secure practices, even when awareness exists (Rogers, 1983). This analysis demonstrates that cybersecurity risk in blended learning systems is institutionally produced, as weak governance and infrastructural fragility systematically erode both threat and coping appraisals (Parsons et al., 2017; Alotaibi, 2021).

3.6.3. Integrated Technology Acceptance and Protection Motivation Perspective

An integrated acceptance-protection perspective reveals how usability constraints and cybersecurity risks are mutually reinforcing in Moodle-based blended learning environments. Limited perceived ease of use not only reduces adoption intensity but also indirectly increases exposure to cyber risk by encouraging insecure coping strategies such as account sharing and public-network access. While TAM explains how structural barriers suppress behavioural intention and sustained use, PMT explains how the same barriers weaken protection motivation by diminishing self-efficacy and increasing response costs. Together, these theories show that insecure practices are not aberrant user behaviours but predictable outcomes of interacting technological, institutional, and cognitive constraints. This integrated analysis advances blended learning scholarship by demonstrating that adoption and security must be theorised together, particularly in resource-constrained contexts where digital inequality and weak institutional capacity shape both engagement and vulnerability (Selwyn, 2016; van Dijk, 2020).

The reviewed literature demonstrates that while blended learning and LMS adoption are widely studied, limited research integrates cybersecurity, digital ine-

quality, institutional governance, and human behaviour into a unified analytical framework—particularly in resource-constrained higher education contexts (Selwyn, 2016; van Dijk, 2020).

Most existing studies examine infrastructure, digital skills, or cybersecurity in isolation, resulting in fragmented explanations that fail to capture their interdependence. Context-specific empirical evidence from low-resource and post-conflict higher education systems remains underrepresented. These gaps justify the present study's focus on cybersecurity as a cross-cutting dimension of Moodle-based blended learning and its adoption of an integrated socio-technical and human-centred approach.

4. Methodology

4.1. Research Design

This study employed a mixed-methods design, which combined qualitative and quantitative approaches to examine the challenges and barriers of implementing Moodle for blended learning in Sierra Leonean universities. The mixed-methods design was considered appropriate because it allowed the researcher to explore both the lived experiences of educators, students, and administrators (qualitative dimension) and to measure the prevalence and patterns of key issues such as digital literacy, device ownership, and exposure to cybersecurity risks (quantitative dimension). The qualitative and quantitative data were collected concurrently and integrated during the interpretation stage to provide a comprehensive understanding of the phenomenon under study.

4.2. Research Approach

The qualitative strand followed an interpretivist approach, emphasizing the meanings and perceptions of stakeholders regarding Moodle adoption and cybersecurity vulnerabilities. The quantitative strand was grounded in a descriptive survey approach, which enabled the collection of measurable data on infrastructural constraints, usage frequency, and user awareness of digital safety practices. By integrating these two strands, the study ensured that subjective insights were supported with empirical evidence, thereby enhancing both the depth and generalizability of the findings.

4.3. Population and Sampling

The study targeted three groups:

- Educators engaged in blended learning through Moodle.
- Students who accessed courses via Moodle across different faculties.
- ICT administrators and policymakers responsible for overseeing Moodle systems and institutional cybersecurity.

4.3.1. Qualitative Sampling Strategy

The qualitative sample (8 educators, 12 students, and 3 ICT administrators/poli-

cymakers) was deliberately small, consistent with qualitative research principles that prioritise depth, contextual insight, and analytical relevance over statistical representativeness. Purposive sampling was employed to select participants with direct and sustained experience of Moodle-supported blended learning. Educators were drawn from different faculties and levels of seniority to capture variation in pedagogical practice and institutional roles. Students were selected across academic levels and disciplines to reflect diverse patterns of platform use, digital literacy, and access conditions. ICT administrators and policymakers were included based on their responsibility for system implementation, governance, and technical oversight.

The sampling strategy aimed for maximum variation rather than representativeness, enabling the exploration of contrasting experiences and institutional perspectives. Sampling continued until thematic saturation was reached, with no substantively new insights emerging. To reduce potential sampling bias, qualitative findings were triangulated with quantitative survey data from a larger, stratified sample, strengthening the credibility and explanatory power of the study. This mixed-methods integration strengthened the credibility of the findings by situating individual narratives within broader usage patterns and institutional trends. Consequently, while the qualitative sample is intentionally small, it is analytically robust, information-rich, and well-aligned with the study's exploratory and explanatory aims.

4.3.2. Quantitative Sampling Strategy

For the quantitative component, a stratified random sampling technique was employed to ensure representation across faculties. A total of 120 students and 40 educators completed structured questionnaires. Stratification ensured that different faculties (arts, social sciences, sciences, and professional schools) were proportionally represented. The quantitative component was designed to provide descriptive breadth, capturing patterns of Moodle use, digital access, and cybersecurity exposure across user groups. The sample size was sufficient to identify dominant trends and support cross-group comparison, consistent with the descriptive aims of the survey strand.

4.4. Integration of Qualitative and Quantitative Strands

In line with Creswell's mixed-methods framework, integration occurred at the levels of design, analysis, and interpretation, consistent with a convergent mixed-methods design with explanatory emphasis.

At the design level, both strands were aligned around shared constructs, including Moodle usage, infrastructural capacity, digital literacy, institutional governance, and cybersecurity practices. This ensured conceptual equivalence between survey instruments and qualitative interview guides.

At the analysis level, integration was operationalised through explanatory building rather than simple convergence or divergence. Quantitative results were used to establish the prevalence and distribution of key patterns, while qualitative find-

ings were employed to explain underlying mechanisms, institutional processes, and user decision-making that shaped those patterns.

At the interpretation level, findings were integrated through theoretical triangulation, drawing on socio-technical systems theory, digital inequality perspectives, and human-factor cybersecurity models. This allowed quantitative trends to be contextualised through qualitative insight, strengthening the study's explanatory power and ensuring that the two strands were analytically interdependent rather than parallel.

4.5. Data Collection Methods

Data for the study were collected using multiple methods to ensure a comprehensive understanding of the challenges associated with Moodle implementation and cybersecurity. Semi-structured interviews were conducted with educators, administrators, and policymakers to elicit in-depth narratives on infrastructural barriers, institutional responses, and cybersecurity risks encountered in the use of Moodle for blended learning. These interviews provided rich contextual insights into participants' experiences, perceptions, and coping strategies within resource-constrained university settings.

In addition, two focus group discussions were held with students, each comprising six participants. The FGDs facilitated collective reflection on students' experiences with Moodle, including challenges related to access, usability, and affordability, as well as the strategies they adopted to cope with infrastructural and cybersecurity constraints. This group-based approach enabled the exploration of shared experiences and divergent perspectives among students.

Document analysis was also undertaken to examine existing institutional policies and national frameworks relevant to digital learning and cybersecurity. Key documents reviewed included university-level policies, the Sierra Leone Cybersecurity Strategy (2024), and the Critical Information Infrastructure Report (2025). This analysis provided insight into the policy environment shaping Moodle implementation and highlighted gaps between policy intentions and institutional practice.

Finally, quantitative data were collected through a structured questionnaire administered to both students and educators. The questionnaire contained closed- and open-ended items designed to capture information on access to digital devices, frequency of Moodle use, internet stability, levels of digital literacy, and experiences with cyber threats. Prior to full deployment, the questionnaire was pilot-tested to ensure clarity, relevance, and reliability of the items.

4.6. Data Analysis

For the qualitative data, thematic analysis was conducted following Braun and Clarke's (2019) six-step process. Transcripts from interviews and FGDs were coded and categorized into themes. NVivo software was used to manage and organize the coding process. Three overarching themes emerged: technological and

infrastructural barriers, institutional and policy gaps, and cybersecurity vulnerabilities.

For the quantitative data, descriptive statistics (frequencies, percentages, and means) were generated to summarize responses on access to technology, internet connectivity, digital literacy, and exposure to cyber threats. Cross-tabulation was used to compare results between educators and students, as well as across faculties. Statistical analyses were conducted using SPSS software.

The findings from both strands were integrated during interpretation. Convergences (e.g., both qualitative narratives and survey results highlighting unstable internet access) and divergences (e.g., differences in perceived digital literacy between students and educators) were identified and discussed to provide a richer understanding of Moodle's implementation challenges.

Trustworthiness, Validity, and Reliability

To enhance trustworthiness in the qualitative strand, triangulation of interviews, FGDs, and documents was employed, along with member checking for accuracy of interpretations. For the quantitative strand, content validity was established by aligning questionnaire items with research objectives and insights from the literature. Reliability was tested using Cronbach's alpha, which confirmed acceptable internal consistency for the scales measuring digital literacy and cybersecurity awareness.

4.7. Ethical Considerations

Ethical approval was obtained from the University of Sierra Leone's Research and Ethics Committee. Participants were fully informed about the purpose of the study, their voluntary participation, and their right to withdraw at any point. Written consent was obtained before data collection. Anonymity and confidentiality were strictly maintained by assigning pseudonyms and removing identifiable information from transcripts and survey datasets. All data were stored securely in password-protected and encrypted digital files.

5. Presentation of Findings

The analysis of findings integrated both qualitative and quantitative strands of the study to provide a comprehensive understanding of the barriers and cybersecurity challenges in implementing Moodle for blended learning in Sierra Leonean universities. The qualitative data (interviews, FGDs, and document analysis) were thematically analyzed, while quantitative survey results were summarized using descriptive statistics. The findings are presented under three main themes: technological and infrastructural barriers, institutional and policy gaps, and cybersecurity vulnerabilities.

5.1. Figure 1: Key Quantitative Findings on Moodle Implementation and Cybersecurity

Figure 1 presents key quantitative findings on infrastructural barriers and cyber-

security vulnerabilities affecting Moodle-based blended learning among students and educators.

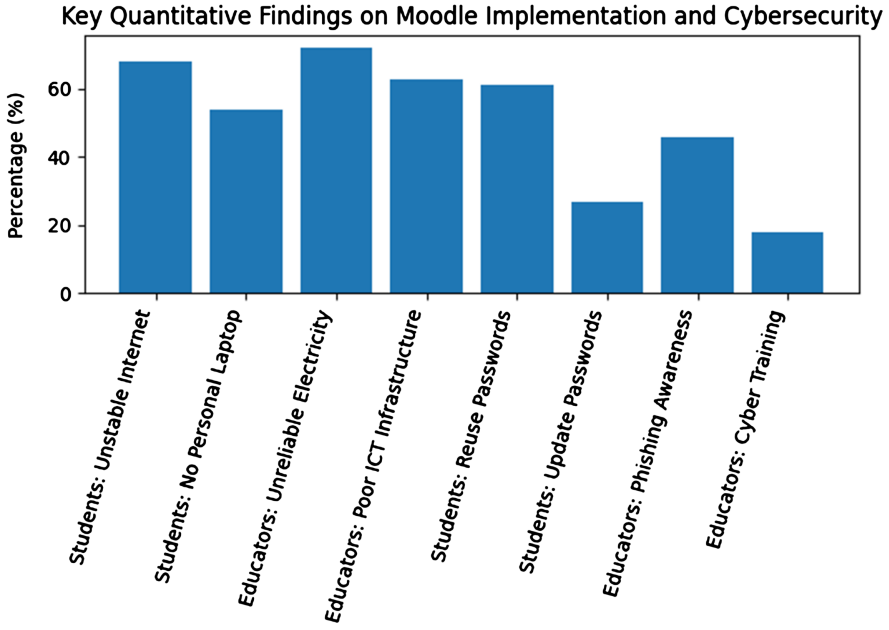

Figure 1. Key quantitative findings on Moodle implementation and cybersecurity.

5.1.1. Technological and Infrastructural Barriers

Interviews with educators and ICT administrators revealed that poor internet connectivity and unreliable electricity supply were the most significant challenges. Many educators reported frequent class disruptions due to system downtime and difficulties uploading course materials. Students highlighted the burden of traveling to internet cafés to access Moodle, which increased learning costs. Focus group participants also emphasized the unequal distribution of devices, with many relying on shared or borrowed smartphones.

Survey data supported these narratives. Out of 120 students surveyed, 68% reported unstable internet connectivity as a major barrier, while 54% lacked personal laptops, relying instead on smartphones with limited functionality. Among educators, 72% indicated that unreliable electricity hindered their ability to use Moodle consistently, and 63% cited insufficient institutional ICT infrastructure (such as outdated servers and weak campus Wi-Fi).

The convergence of qualitative and quantitative data demonstrates that infrastructural weaknesses remain the primary barrier to Moodle adoption.

5.1.2. Institutional and Policy Gaps

Interviews with administrators revealed that most universities lacked clear institutional policies on digital safety and cybersecurity. While some departments had informal practices (e.g., using personal email accounts for Moodle access), there were no standardized guidelines for user authentication, data encryption, or cyber incident response. Educators expressed frustration at the absence of technical sup-

port staff dedicated to Moodle, leaving them to troubleshoot problems on their own.

The survey confirmed these gaps, 79% of educators and 66% of students reported that they had never received formal training on Moodle use or cybersecurity awareness. Furthermore, only 21% of respondents indicated that their institution had shared any written policy on digital safety.

The lack of institutional commitment to cybersecurity and digital pedagogy undermines trust in Moodle as a reliable platform. These findings echo global research, which emphasizes that the absence of clear frameworks often leaves e-learning systems exposed to risks and inconsistencies (Alotaibi, 2021).

5.1.3. Cybersecurity Vulnerabilities and User Awareness

Students in the FGDs described experiences of phishing attempts and suspicious pop-up links when accessing Moodle on shared public devices. Educators admitted limited awareness of cyber hygiene practices, with some reusing weak passwords across multiple platforms. ICT administrators revealed that Moodle servers were often left unpatched for extended periods due to lack of funds or expertise.

Survey results highlighted significant vulnerabilities. Only 27% of students reported regularly updating their passwords, while 61% admitted to using the same password across multiple accounts. Among educators, 46% acknowledged they would struggle to recognize a phishing email, and only 18% reported attending any training on cybersecurity practices.

5.2. Cross-Tabulation Tables: Moodle Implementation Study

As shown in Table 1, the cross-tabulation indicates a pronounced disparity between students and educators in terms of internet connectivity stability. While a substantial majority of students (72%) reported unstable internet access, the proportion was lower among educators (54%), suggesting that infrastructural constraints disproportionately affect students and may limit their sustained engagement with Moodle-supported blended learning.

Table 1. Internet connectivity stability by user group.

User Group	Stable Internet (%)	Unstable Internet (%)
Students (n = 120)	28	72
Educators (n = 40)	46	54

Table 2 demonstrates clear differences in device access between user groups, with educators far more likely to access Moodle via laptops (68%) compared to students (46%). Students' heavier reliance on smartphones and shared devices suggests constrained interaction with advanced Moodle functionalities, which may partially explain lower levels of participation in assessments and collaborative activities.

Table 2. Primary device used to access Moodle by user group.

User Group	Laptop (%)	Smartphone (%)	Shared Device (%)
Students (n = 120)	46	38	16
Educators (n = 40)	68	22	10

As illustrated in Table 3, educators reported significantly higher levels of cybersecurity awareness than students, with over half indicating high awareness compared to less than one-third of students. This imbalance highlights a critical vulnerability within Moodle-based learning environments, where students with lower awareness may be more exposed to cyber risks such as phishing and insecure access practices.

Table 3. Cybersecurity awareness by user group.

User Group	High Awareness (%)	Moderate Awareness (%)	Low Awareness (%)
Students (n = 120)	29	41	30
Educators (n = 40)	52	33	15

Taken together, the cross-tabulation results (Tables 1-3) reveal that infrastructural access, device ownership, and cybersecurity awareness are unevenly distributed across user groups. These disparities help explain variations in Moodle engagement and reinforce the need for context-sensitive institutional interventions that address both technological and human-capacity dimensions of blended learning.

5.3. Discussions of Findings

This study set out to examine the technological, institutional, and cybersecurity barriers affecting the implementation of Moodle for blended learning in resource-constrained universities in Sierra Leone. While the empirical findings clearly demonstrate infrastructural deficits, weak institutional policies, and low levels of cybersecurity awareness, a deeper analytical reading reveals that these challenges are not merely technical or managerial in nature. Rather, they are embedded within broader structural conditions of digital inequality, institutional capacity gaps, and asymmetrical exposure to cyber risk, which shape how blended learning platforms function in low-resource higher education contexts.

5.3.1. Cybersecurity as a Dimension of Digital Inequality

The findings strongly support theoretical perspectives that conceptualise digital inequality as a multi-level phenomenon, extending beyond access to include skills, institutional capacity, and risk exposure. While limited internet connectivity, unreliable electricity, and device scarcity reflect first-level digital divides, the study's evidence on weak password practices, phishing susceptibility, and delayed system

patching points to second- and third-level digital divides, where inequalities manifest in differential ability to use digital systems safely and benefit from them securely.

Students who relied on shared devices, public internet cafés, or unsecured networks were disproportionately exposed to cyber threats, illustrating how cybersecurity vulnerability is socially patterned rather than randomly distributed. In this sense, Moodle does not operate as a neutral educational technology; instead, it is embedded in unequal digital ecosystems that determine who is protected, who is exposed, and who bears the consequences of cyber failure. This finding aligns with international scholarship, which argues that digital learning platforms, when deployed without adequate institutional safeguards, can inadvertently reproduce and intensify existing educational inequalities rather than mitigate them.

5.3.2. Institutional Capacity, Governance, and Risk Transfer

A key analytical contribution of this study lies in demonstrating how institutional cybersecurity weaknesses shift risk downward to individual users. The absence of clear institutional policies on digital safety, combined with limited technical staffing and irregular system maintenance, effectively transfers responsibility for cybersecurity from institutions to students and educators. This aligns with critical governance perspectives that view cybersecurity in public institutions as a matter of political and organisational capacity rather than individual compliance.

The findings indicate that Moodle servers were often left unpatched due to financial and technical constraints, while users received little or no formal training on cyber hygiene. In such contexts, cybersecurity becomes reactive rather than preventive, and incidents such as phishing attempts or account compromise are treated as isolated events rather than symptoms of systemic vulnerability. This governance gap mirrors patterns observed in other low- and middle-income countries, where universities are increasingly digitised but insufficiently securitised, rendering them soft targets within global cyber threat landscapes.

This downward transfer of risk has important equity and accountability implications. Students and educators with limited digital literacy, unreliable access to secure devices, or dependence on public internet facilities are disproportionately exposed to cyber threats, despite having the least capacity to mitigate them. As a result, cybersecurity risk becomes unevenly distributed along existing lines of digital inequality, reinforcing structural disadvantage rather than merely reflecting individual user behaviour. The expectation that users should independently manage complex security decisions in the absence of institutional guidance represents a form of *institutional abdication* rather than user failure.

From a governance perspective, this pattern underscores the need to reconceptualise Moodle and similar learning management systems as components of critical educational infrastructure rather than optional pedagogical tools. Effective cybersecurity in blended learning environments requires institutional investment

in policy enforcement, technical staffing, preventive maintenance, and continuous capacity building. Without such systemic interventions, further expansion of digital learning risks amplifying institutional vulnerability and normalising the transfer of organisational risk onto individuals who lack both authority and resources to manage it effectively.

5.3.3. Positioning Sierra Leone within Global Cybersecurity Debates

Although the study is contextually grounded in Sierra Leone, the findings resonate strongly with broader international debates on cybersecurity in higher education. Globally, universities are recognised as attractive targets for cyberattacks due to their open systems, large user populations, and valuable data repositories. However, resource-constrained universities face a compounded form of vulnerability, where infrastructural fragility intersects with low digital literacy and weak policy enforcement.

The Sierra Leonean case should therefore not be interpreted as exceptional, but rather as an intensified illustration of global structural trends. What distinguishes this context is not the presence of cyber risk per se, but the limited institutional capacity to anticipate, absorb, and respond to such risks. This contributes to the growing body of Global South scholarship that challenges universalist assumptions embedded in digital education models developed in high-income contexts, where stable infrastructure and mature cybersecurity frameworks are often taken for granted.

5.3.4. Moodle, Pedagogy, and the Limits of Technological Solutionism

The discussion also challenges technologically deterministic narratives that present Learning Management Systems as inherently transformative. While Moodle offers pedagogical affordances that can enhance interaction, flexibility, and continuity of learning, the findings demonstrate that its effectiveness is contingent upon institutional readiness, governance structures, and user support systems. In the absence of these conditions, Moodle risks being reduced to a content repository rather than a genuinely interactive learning environment, while simultaneously introducing new layers of digital risk.

From a critical pedagogical perspective, this underscores the limits of technological solutionism in higher education reform. Digital platforms alone cannot compensate for structural deficits in infrastructure, training, and policy coherence. Instead, they must be embedded within broader institutional strategies that integrate pedagogy, cybersecurity, and equity considerations. Without such integration, blended learning initiatives may expand nominal access while deepening qualitative inequalities in learning experience and digital safety.

5.4. Implications for Theory and Practice

Theoretically, this study contributes to the intersection of digital inequality theory and cybersecurity studies by demonstrating how cyber risk functions as an underexamined dimension of educational inequality. It extends existing debates by

showing that cybersecurity is not only a technical concern but also a social and institutional one, deeply entangled with questions of access, power, and responsibility in digital education systems.

Practically, the findings highlight the need for universities in resource-constrained contexts to reconceptualise Moodle and similar platforms as components of critical information infrastructure, requiring coordinated investment in policy development, technical capacity, and continuous user training. Cybersecurity awareness programmes, institutional protocols for system maintenance, and context-appropriate digital pedagogy training are not optional add-ons but foundational requirements for sustainable blended learning.

5.5. Conclusion

This study demonstrates that the implementation of Moodle for blended learning in Sierra Leonean universities is constrained by interconnected infrastructural, institutional, and human factors. Unreliable internet connectivity, unstable electricity supply, and limited access to appropriate digital devices undermine consistent platform use and heighten exposure to cybersecurity risks. These structural weaknesses are compounded by the absence of clear institutional policies and limited technical support, which erode trust in Moodle as a secure learning environment. The findings further reveal significant human-factor vulnerabilities, including low cybersecurity awareness, weak password practices, and minimal training among users. Overall, the study concludes that Moodle's potential to support equitable and resilient blended learning will remain limited unless technological capacity, institutional governance, and user cybersecurity competence are addressed in an integrated manner.

5.6. Recommendations

Based on the findings of this study, the following recommendations are proposed:

Strengthen ICT Infrastructure

Universities should prioritize investments in reliable electricity supply, campus-wide high-speed internet connectivity, and modern ICT infrastructure. Strategic partnerships with government agencies, private sector providers, and international development partners can help mobilize resources to address infrastructural deficits.

Develop and Enforce Institutional Cybersecurity Policies

Higher education institutions should establish comprehensive policies on digital safety and cybersecurity, covering user authentication, data protection, system maintenance, and incident response. Clear guidelines will promote consistency, accountability, and trust in Moodle as a secure learning platform.

Enhance Capacity Building and Training

Continuous professional development programs should be implemented to improve educators' digital pedagogy and cybersecurity skills. Similarly, students should receive structured training on Moodle use, cyber hygiene, and safe online

practices to reduce human-related vulnerabilities.

Strengthen Technical Support and System/infrastructural Maintenance

Universities should allocate dedicated technical personnel to manage Moodle platforms, ensure timely system updates, and address cybersecurity threats. Regular patching and monitoring of Moodle servers are essential to maintaining system integrity.

Integrate Cybersecurity into National Digital Education Strategies

Policymakers should recognize Moodle and other LMS platforms as part of Sierra Leone's critical information infrastructure. Integrating cybersecurity considerations into national higher education and digital transformation strategies will enhance institutional resilience and sustainability.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Al-Ajlan, A., & Zedan, H. (2008). Why Moodle. In *2008 12th IEEE International Workshop on Future Trends of Distributed Computing Systems* (pp. 58-64). IEEE. https://doi.org/10.1109/ftdcs.2008.22

Al-Emran, M., Malik, S. I., & Al-Kabi, M. N. (2020). Investigating the Impact of Digital Learning on Students' Academic Performance in Higher Education. *Education and Information Technologies, 25,* 3159-3176.

Alotaibi, S. (2021). Cybersecurity Challenges in E-Learning Systems: Risks and Mitigation Strategies. *International Journal of Information Security Science, 10,* 45-57.

Benson, V., Anderson, D., & Ooms, A. (2011). Educators' Perceptions, Attitudes and Practices: Blended Learning in Business and Management Education. *Research in Learning Technology, 19,* 143-154. https://doi.org/10.3402/rlt.v19i2.10353

Bijker, W. E., Hughes, T. P., & Pinch, T. (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. MIT Press.

Braun, V., & Clarke, V. (2019). Reflecting on Reflexive Thematic Analysis. *Qualitative Research in Sport, Exercise and Health, 11,* 589-597. https://doi.org/10.1080/2159676x.2019.1628806

Constantin, L. (2017). Higher Education Institutions Increasingly Targeted by Cyberattacks. *Computerworld*. https://www.computerworld.com/

Costello, E. (2013). Opening up to Open Source: Looking at How Moodle Was Adopted in Higher Education. *Open Learning, 28,* 187-200. https://doi.org/10.1080/02680513.2013.856289

Critical Information Infrastructure Report (2025). *National Workshop Report on Critical Information Infrastructure Protection in Sierra Leone*. Government of Sierra Leone.

Dakowska, A. (2017). Infrastructure Challenges in E-Learning Adoption in Developing Contexts. *International Journal of Educational Technology in Higher Education, 14,* 1-14.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13,* 319-340. https://doi.org/10.2307/249008

Fresen, J. (2010). Factors Influencing Lecturer Uptake of E-Learning. *Teaching English*

with Technology, 10, 81-97.

Garrison, D. R., & Kanuka, H. (2004). Blended Learning: Uncovering Its Transformative Potential in Higher Education. *The Internet and Higher Education, 7,* 95-105. https://doi.org/10.1016/j.iheduc.2004.02.001

Haworth, B. T. (2021). Cybersecurity Risks in Online Learning Environments. *Computers & Security, 104,* Article 102211.

Hodges, C., Moore, S., Lockee, B., Trust, T., & Bond, A. (2020). The Difference between Emergency Remote Teaching and Online Learning. *Educause Review*. https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning

Machado, M., & Tao, E. (2007). Blackboard vs. Moodle: Comparing User Experience of Learning Management Systems. In *Proceedings of the 37th ASEE/IEEE Frontiers in Education Conference* (pp. 7-12). IEEE.

Mtebe, J. S., & Raisamo, R. (2014). Investigating Perceived Barriers to the Use of Open Educational Resources in Higher Education in Tanzania. *The International Review of Research in Open and Distributed Learning, 15,* 43-66. https://doi.org/10.19173/irrodl.v15i2.1803

Mtebe, J. S., & Raisamo, R. (2016). Challenges and Instructors' Intention to Adopt and Use Open Educational Resources in Higher Education. *The International Review of Research in Open and Distributed Learning, 17,* 1-18.

Oh, E., & Park, S. (2009). How Are Universities Involved in Blended Learning? *Educational Technology & Society, 12,* 327-342.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 69,* 249-260.

Quayyum, F., & Freberg, K. (2023). Human Factors and Cybersecurity Awareness in Higher Education Institutions. *Journal of Cybersecurity Education, Research and Practice, 1,* 1-15.

Roberts, J. (2005). Limits to Communities of Practice. *Journal of Management Studies, 43,* 623-639. https://doi.org/10.1111/j.1467-6486.2006.00618.x

Rogers, R. W. (1983). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176). Guilford Press.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "Weakest Link"—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19,* 122-131. https://doi.org/10.1023/a:1011902718709

Selwyn, N. (2016). *Education and Technology: Key Issues and Debates*. Bloomsbury Academic. https://doi.org/10.5040/9781474235952

Sierra Leone Cybersecurity Strategy (2024). *National Cybersecurity Strategy*. Government of Sierra Leone.

Tawiah, Y. S., Agyeman, F. O., & Obeng, E. (2019). Adoption of LMS in Sub-Saharan Africa. *Education and Information Technologies, 24,* 2789-2806.

Unwin, T. (2009). *ICT4D: Information and Communication Technology for Development*. Cambridge University Press.

van Dijk, J. (2005). *The Deepening Divide: Inequality in the Information Society*. Sage Publications.

van Dijk, J. (2020). *The Digital Divide*. Polity Press.

Warschauer, M. (2004). *Technology and Social Inclusion: Rethinking the Digital Divide*. MIT Press.

Zhou, L., & Leung, L. (2022). Cybersecurity Threats and Resilience in Higher Education Institutions. *Computers & Security, 113,* Article 102548.