Factors Affecting Utilization of Electronic Security Technologies in University Libraries in Tanzania

Richard C. Mfinanga[1*], Lilian D. Isowe[2] and Henry Mambo[3]
The Open University of Tanzania
[1]ORCiD: https://orcid.org/0009-0003-3233-2018
[2]ORCiD: https://orcid.org/0000-0001-7256-6749
[3]ORCiD: https://orcid.org/0000-0002-8722-9072
**Corresponding author e-mail: richardcmfinanga@gmail.com*

Abstract
This study investigated the factors affecting the utilization of Electronic Security Technologies (ESTs) for protecting library information resources in four Tanzanian university libraries: The University of Dar es Salaam (UDSM), the Institute of Accountancy Arusha (IAA), Mzumbe University (MU), and Muhimbili University of Health and Allied Sciences (MUHAS). The study used a convergent parallel research design. Quantitative data came from a questionnaire administered to a census of 184 library staff; qualitative data came from interviews with 12 key informants (library directors, ICT directors and IT personnel) and from non-participant observation. Quantitative data were analyzed descriptively in SPSS version 27, and qualitative data were analyzed thematically. Respondents perceived ESTs as contributing to the protection of physical and digital resources, notably through theft prevention and control of unauthorized access. However, staff skill gaps, inadequate training, insufficient funds, high maintenance and repair costs, and frequent technical malfunctions or downtime constrained utilization of electronic security technologies. Interviews and observations corroborated these constraints. The findings indicate that having ESTs does not by itself ensure their effective use. The study recommends prioritizing staff training, allocating a dedicated budget, implementing preventive maintenance with reliable vendor support, modernizing ICT infrastructure, and establishing an institutional security policy.

Keywords: *Electronic Security Technologies, Utilization, Library Information Resources, Academic Libraries, Library Security*

INTRODUCTION

University libraries are central to teaching, learning, research and innovation, providing access to information resources in both print and

electronic formats. As academic institutions increasingly rely on information and communication technologies (ICTs), library collection security has become a major concern. Library information resources face recurring threats, including theft, mutilation, unauthorized access, vandalism, cyberattacks, and improper handling, which can affect their availability, integrity, and accessibility. Electronic security technologies (ESTs) are therefore becoming more common in university libraries worldwide, strengthening their capacity to secure both physical and digital collections (Permana et al., 2025; Xu et al., 2024).

In this paper, ESTs refer to two related groups of technologies. The first comprises physical-security technologies: Radio Frequency Identification (RFID) systems for item tagging, tracking and theft detection; Closed-Circuit Television (CCTV) and related surveillance systems; biometric access control; alarm systems; and integrated library security systems. The second comprises digital-security measures, such as antivirus software and access controls, that protect computers, networks and electronic resources from malware and unauthorized access. The paper uses the same name and abbreviation for each technology throughout.

Recent advances in library automation and smart-library environments show that ESTs can support collection security, circulation control, inventory management, access control and the prevention of unauthorized use of library materials. RFID and integrated surveillance systems have been reported to improve operational efficiency, enable real-time monitoring, reduce resource losses and strengthen user accountability in academic libraries (Sureshkumar et al., 2025; Adewojo & Monjolaoluwa, 2025). However, effective EST utilization depends on institutional capacity, funding, staff skills, technical infrastructure, maintenance support, and institutional commitment (Ibrahim & Kotoroi, 2025).

In developing countries, especially in Sub-Saharan Africa, operational and institutionalization challenges constrain EST utilization. Existing research documents poor funding, inadequate staff training, outdated technological infrastructure, technical failures, weak maintenance support and shortages of qualified staff as continuing obstacles to the effectiveness of electronic security equipment in academic libraries (Ibrahim & Kotoroi, 2025; Iwara, 2019). These obstacles often lead to underutilization of available security technologies, frequent system failures and continued reliance on manual security methods that are no longer adequate in today's academic environment.

Many Tanzanian university libraries have invested in ESTs to protect their expanding print collections and electronic resources. The University of Dar es Salaam, Mzumbe University, Muhimbili University of Health and Allied Sciences and the Institute of Accountancy Arusha, for example, have adopted various electronic security systems to protect resources and facilitate library operations. Ibrahim and Kotoroi (2025) report that financial constraints, limited technical expertise, insufficient training, outdated infrastructure, and difficulties with system maintenance and upgrades often reduce these technologies' effectiveness.

Although Tanzanian academic libraries are increasingly introducing ESTs, empirical evidence on the factors affecting their actual use remains limited. Existing Tanzanian and regional studies have focused on a single institution (Ibrahim & Kotoroi, 2025), on the impact of security systems on resource preservation (Komba, 2020), or on constraints facing African academic libraries in general (Kotoroi, 2023). Little is known about how library staff perceptions compare with accounts from library and ICT directors, and with direct observation of system utilization, across several Tanzanian university libraries. This study addresses that gap by combining questionnaire, interview, and observation evidence from four libraries and by focusing on the utilization of ESTs, rather than their mere availability, in the analysis.

Accordingly, the study investigates the factors affecting the use of ESTs to safeguard library information resources in four university libraries: The Institute of Accountancy Arusha (IAA), Muhimbili University of Health and Allied Sciences (MUHAS), Mzumbe University (MU), and the University of Dar es Salaam (UDSM). Its findings contribute to the literature on library security management and extend beyond the mere availability of ESTs to the institutional conditions required for their sustained, effective utilization. The study further offers practical guidance to policymakers, university administrators, and library directors in Tanzania and similar developing-country contexts.

Objectives of the Study

The general objective was to investigate the factors affecting the utilization of ESTs to protect library information resources in the four selected university libraries. The specific objectives were:

i) To assess the perceived protection outcomes of utilizing ESTs in the selected university libraries.

ii) To examine the factors that affect the utilization of ESTs for protecting library information resources in the selected university libraries.
iii) To propose strategies for improving the utilization of ESTs in the selected university libraries.

LITERATURE REVIEW

Perceived Protection Outcomes of ESTs Utilization

The use of Electronic Security Technologies (ESTs) in university libraries has been growing and has become an important issue in protecting information resources. University libraries use Closed-Circuit Television (CCTV), electronic security gates, Radio Frequency Identification (RFID), biometric systems, fire detection and suppression systems, access-control technologies, and digital security mechanisms to prevent, detect, and respond to threats to library information resources. For instance, Olaniyi and Abioye (2024) conducted a study on the use of CCTV, electronic security gates and IP surveillance systems as perceived protection technologies in a university library in Nigeria and found that these were some of the most widely used technologies for safeguarding information resources in the library. Similarly, Osayande et al. (2024) reported that in selected Nigerian University Libraries, the electronic security systems, especially CCTV, electronic security gates and RFID, were seen to have provided a positive contribution towards the protection of library resources.

Zhang et al. (2024) noted that Intelligent RFID mechanisms can support resource identification, detection of unauthorized access, monitoring of resource location, and improved circulation operations. Nsirim et al. (2025) identified RFID asset tracking, access control, CCTV surveillance, digital rights management, cybersecurity measures, and artificial intelligence-based anomaly detection as complementary technology-based tools libraries use to protect information resources. Kotoroi and Ibrahim (2025) found that personal, technical, managerial, and financial factors influenced the effectiveness of electronic security system utilization. Their findings are significant because they show that having CCTV, theft-detection systems, or other technologies is not enough to protect library materials. Electronic security technologies help prevent theft/mutilation, detect unauthorized activities, improve accountability, protect physical and digital resources, monitor library environments, and enhance resource availability (Nath, 2021).

Factors Affecting the Utilization of Electronic Security Technologies

Ibrahim and Kotoroi (2025) found that physical and technical conditions affect the effectiveness of electronic security systems in African University Libraries. Kotoroi (2023) further noted that technology availability should be distinguished from technology utilization because the existence of electronic security technologies does not necessarily mean they are consistently functional or effectively incorporated into daily library operations. Olaniyi and Abioye (2024) noted that inadequate funding, poor maintenance, and high installation costs are major challenges to effectively utilizing electronic security technologies in libraries. Similarly, Sunday et al. (2025) identified limited funding and poor supervision from parent institutions as limiting factors in implementing and utilizing electronic security systems in selected academic libraries in Southwestern Nigeria.

Mambo and Confort (2019) explained that poor library management, inadequate library budgets, unreliable electricity supply, lack of staff commitment, and inadequate training were significant challenges to utilizing electronic security systems. Ibrahim and Kotoroi (2025) argued that many of the limitations identified in this study of electronic security systems in Tanzanian university libraries are not inherent in the technologies, but in management and library staff practices.

Strategies for Improving the Utilization of Electronic Security Technologies

Risk assessment and planning, continuous monitoring, regular system updates, and implementing suitable security controls are crucial strategies for enhancing the protection of information resources through technology (Nsirim et al. 2025). Ibrahim and Kotoroi (2025) suggest sufficient funds for maintenance and repairs, along with robust institutional policies, to protect library information materials. Similarly, Sunday et al. (2025) highlight the importance of proper funding and institutional control in supporting the utilization of electronic security technologies in academic libraries. Sunday et al. (2025) further argued that for ESTs to be sustainable, university libraries should offer support beyond procurement, specifically maintenance, updates, technical support, and replacement of outdated technologies. Ibrahim and Kotoroi (2025) suggest that staff training can mitigate challenges encountered in using electronic security technologies in libraries.

University libraries need to offer induction training, refresher training, role-specific technical training, and training in real-life scenarios involving security incidents. Training must cover ethical and privacy issues, especially for CCTV, biometric systems, access control technologies, and digital surveillance systems (Kavak, 2024). This capacity building can boost staff confidence and competence, as well as institutional accountability for the appropriate utilization of electronic security technologies. Continuous monitoring, user awareness, system updating, patch management, privacy protection and risk-based security planning are all elements of a comprehensive technology-based security framework (Nsirim et al., 2025). Advancements in smart-library technology also suggest incorporating Internet of Things (IoT) infrastructure, intelligent sensing, and automated data processing to enhance real-time monitoring and resource management (Zhang et al., 2024).

RESEARCH METHODOLOGY

This section describes how the study examined the factors affecting the utilization of electronic security technologies to safeguard library information resources in four university libraries.

Research Philosophy

The study was grounded in pragmatism, which focuses on practical solutions to research problems, supports mixed methods, accepts multiple perspectives, and provides a comprehensive understanding through multiple methods (Allemang et al., 2022; Collis & Hussey, 2014; University of Nottingham, 2025).

Research Design and Approach

The study adopted a convergent parallel research design, consistent with a pragmatic philosophy. In this design, quantitative and qualitative data are collected in the same phase, analyzed separately, and then merged to compare or corroborate the findings (Creswell & Plano-Clark, 2018). The design allows a fuller understanding of a research problem by drawing on the strengths of both approaches (Creswell, 2014; Creswell & Creswell, 2018; Leavy, 2022; Tashakkori & Teddlie, 2010), and it was chosen to obtain a comprehensive understanding of the factors affecting the utilization of ESTs in university libraries.

Study Areas

The study was conducted in four university libraries in Tanzania: The Institute of Accountancy Arusha (IAA), Mzumbe University (MU),

Muhimbili University of Health and Allied Sciences (MUHAS) and the University of Dar es Salaam (UDSM). These libraries were selected because they had comparatively demonstrated evidence of adoption and utilization of electronic security technologies; availability of library personnel with direct experience of operating or interacting with electronic security technologies; substantial library information resources requiring protection; institutional diversity that could provide variation in organizational and technological contexts; and accessibility of information relevant to understanding factors affecting the utilization of electronic security technologies.

Population, Sampling Procedures and Sample Size

The study used purposive sampling and a census (total enumeration). The census covered all library staff in the four libraries: 20 at IAA, 46 at MU, 23 at MUHAS and 103 at UDSM, a total of 192 (Table 1). Key informants were selected purposively for their knowledge of, and responsibility for, the procurement, operation, or support of ESTs, making them information-rich cases for the qualitative inquiry (Bryman, 2016; Marshall & Rossman, 2022; Patton, 2015). The study included 12 key informants: four library directors, four ICT directors, and four IT personnel, with each role represented at every library. The library directors were included for their knowledge of policy and budgeting, ICT directors for infrastructure and network support, and IT personnel for the day-to-day operations and maintenance of electronic security systems.

Table 1:
Study Population, Sample and Response

Institution	Library staff (census)	Questionnaires analyzed	Response rate	Key informants
Institute of Accountancy Arusha (IAA)	20	19	95%	3
Mzumbe University (MU)	46	45	97.8%	3
Muhimbili University of Health and Allied Sciences (MUHAS)	23	21	91.3%	3
University of Dar es Salaam (UDSM)	103	99	96.1%	3
Cumulative Total	**192**	**184**	**95.8%**	**12**

Note: Key informants at each library were the library director, the ICT director and IT personnel. Response rate = questionnaires analyzed ÷ library staff in the census.

Data Collection Instruments

Questionnaire. Data were collected from the 184 library staff using a questionnaire with closed items rated on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree) and open-ended items inviting suggestions for improving the utilization of ESTs. The questionnaire was designed in Google Forms and self-administered (Taherdoost, 2022).

Interviews. The interview schedule, developed from the study objectives and containing structured and semi-structured questions, was used with the 12 key informants to capture their views and experiences.

Observation. The researcher conducted non-participatory observations to identify the practical limitations encountered in effectively using electronic security technologies in the selected academic libraries. The researcher recorded operational practices (maintenance routines and system troubleshooting), the staff competencies needed for effective EST utilization, and situational realities such as system sign-in and navigation, as well as infrastructure conditions such as internet stability and EST performance (Creswell, 2014; Patton, 2015). In addition, the researcher sat quietly in the library without interfering with library operations and did not inform library staff of the exact observation date in advance. Each observation lasted for 30 to 45 minutes per day. The observation checklist enabled the researcher to collect reliable, naturalistic information on the factors affecting the utilization of electronic security technologies in academic libraries (Osayande, 2019). Lastly, the researcher wrote field notes immediately after each session to reduce recall bias (Marshall & Rossman, 2022).

Data Analysis and Integration

Quantitative analysis. The researcher coded questionnaire responses using a coding manual and entered them into the Statistical Package for the Social Sciences (SPSS) version 27, which supported data management, display, and retrieval (Rahman & Muktadr, 2021). Descriptive statistics (frequencies and percentages; N = 184) were used to characterize responses. No inferential tests were applied; the findings therefore describe the prevalence of perceived barriers and do not establish statistical determinants.

Qualitative analysis. Interview data, open-ended questionnaire responses, and observation field notes were analyzed thematically following the phases described by Braun and Clarke (2021): familiarization with the

data, generation of initial codes, development and review of themes, and definition of themes. Codes and themes were developed iteratively, reflecting participants' perspectives and the study objectives. Open-ended responses were also counted to show how many respondents proposed each strategy.

Integration. Integration occurred at the interpretation stage. For each factor, the questionnaire percentages, interview themes and observation notes were placed side by side in a joint display (Table 4) and judged as convergent (sources agree), complementary (sources add different detail) or not corroborated. Where a source did not address a factor, this is stated. This kind of triangulation strengthens interpretation and deepens analysis (Creswell & Creswell, 2023).

Data Quality Assurance

The researcher submitted the data collection instruments to research experts for advice and suggestions on improvements and modifications. Suggestions from research experts helped the researcher refine the data collection instruments before data collection, strengthening content validity and ensuring the instruments covered key aspects of the factors affecting electronic security technologies utilization in university libraries. This study also triangulated questionnaire, interview, and observation data to increase confidence in the findings when different sources pointed in the same direction (Bryman, 2016). Furthermore, the pilot study was conducted at the Nelson Mandela African Institute of Science and Technology by purposively selecting eight library staff members conversant with electronic security technologies, given them questionnaires to complete, and interviewing one library director, one ICT director, and one IT personnel member to assess the validity and completeness of the instruments.

Ethical Considerations

This research complied with key ethical standards that protected participants' rights, safety, and dignity. Before data collection began, the researcher obtained official permission from relevant authorities, including the Open University of Tanzania, Institute of Accountancy Arusha (IAA), Muhimbili University of Health and Allied Sciences (MUHAS), Mzumbe University (MU), and the University of Dar es Salaam (UDSM). Participants (library directors, ICT directors, IT personnel, and library staff) were fully informed about the purpose of the study and what was expected from them. In addition, the study

maintained confidentiality and anonymity. The actual names and places of the participants in this study were not used, and instead codes were used to protect the participants' anonymity. The researcher kept all research data secure and accessible only to them. The researcher also ensured honesty and accuracy in data collection and reporting by properly acknowledging all sources used.

RESULTS, ANALYSIS AND DISCUSSION

184 questionnaires were analyzed (Table 1). Percentages in Tables 2 and 3 are calculated from N = 184 and rounded to one decimal place. “Agree + SA” combines the *Agree* and *Strongly agree* categories; *Neutral* is reported separately and is not counted as agreement.

Perceived Protection Outcomes of Utilizing ESTs

This section presents respondents' perceptions of the protection outcomes of the ESTs used in their libraries. These outcomes provide context for the utilization factors reported in the next section. Table 2 presents the results.

Table 2:
Respondents' Perceptions of the Protection Outcomes of ESTs (N = 184)

Statement	SD	D	N	A	SA	Agree + SA
A. Perceived protection outcomes						
ESTs effectively prevent theft of physical resources.	0 (0.0%)	0 (0.0%)	2 (1.1%)	52 (28.3%)	130 (70.7%)	**182 (98.9%)**
ESTs protect digital resources from unauthorized access.	1 (0.5%)	3 (1.6%)	0 (0.0%)	106 (57.6%)	75 (40.8%)	**181 (98.4%)**
ESTs reduce financial losses.	6 (3.3%)	32 (17.4%)	13 (7.1%)	98 (53.3%)	35 (19.0%)	**133 (72.3%)**
ESTs help track and locate misplaced or borrowed items more efficiently.	20 (10.9%)	37 (20.1%)	84 (45.7%)	28 (15.2%)	15 (8.2%)	**43 (23.4%)**
ESTs provide real-time alerts and notifications when security breaches occur.	16 (8.7%)	21 (11.4%)	14 (7.6%)	102 (55.4%)	31 (16.8%)	**133 (72.3%)**
ESTs generate useful statistical reports on security incidents.	4 (2.2%)	7 (3.8%)	111 (60.3%)	43 (23.4%)	19 (10.3%)	**62 (33.7%)**
B. Operational cautions						
ESTs sometimes cause false alarms or technical anomalies that disrupt library operations.	4 (2.2%)	8 (4.3%)	25 (13.6%)	91 (49.5%)	56 (30.4%)	**147 (79.9%)**
ESTs require regular maintenance and staff training to remain effective.	2 (1.1%)	5 (2.7%)	10 (5.4%)	44 (23.9%)	123 (66.8%)	**167 (90.8%)**

Scale: SD = strongly disagree; D = disagree; N = neutral; A = agree; SA = strongly agree. Cells show the number of respondents and the percentage; N = 184 in brackets.
Source: Field data, 2026.

Perceptions were most favourable for theft prevention (182 respondents; 98.9% agreement) and protecting digital resources from unauthorized access (181; 98.4%), followed by real-time alerts (133; 72.3%) and reduced financial losses (133; 72.3%). Respondents were less certain about the analytical and inventory functions of the systems: 111 (60.3%) were neutral on statistical reporting on security incidents and 84 (45.7%) were neutral on tracking and locating misplaced items, and only 33.7% and 23.4% respectively agreed that these functions work well. Two operational cautions were also evident. A total of 147 respondents (79.9%) agreed that false alarms or technical anomalies sometimes disrupt library operations, and 167 (90.8%) agreed that the systems need regular maintenance and staff training to remain effective. These results are perceptions of effectiveness, not measured protection outcomes. No loss or incident records were analyzed, so the data cannot show whether ESTs reduced theft or unauthorized access. However, these perceptions align with Nath (2021), who described electronic security systems as effective against theft, mutilation, vandalism, and unauthorized access.

The high neutral shares for reporting and tracking functions point to limited use of advanced features rather than to their absence. Observation showed that only a small group of staff worked with IT staff to process security reports and incident data, and the study noted continued reliance on manual damage-checking of returned materials. These patterns suggest that some available functions are not used routinely. Weak infrastructure, limited system functionality, and skill gaps may explain this, and the current data cannot separate them; the skill-related constraints reported below align with the latter. The pattern also agrees with Ibrahim and Kotoroi (2025), who observed that traditional security measures are becoming less effective in modern libraries.

Factors Affecting the Utilization of ESTs

The second objective was to identify the factors that limit the effective utilization of ESTs. Respondents rated nine statements on possible constraints; Table 3 ranks them by combined agreement.

Table 3:
Perceived Factors Affecting the Utilization of ESTs (N = 184)

Statement	SD	D	N	A	SA	Agree + SA
I lack the skills to operate and manage ESTs effectively and efficiently.	3 (1.6%)	8 (4.3%)	1 (0.5%)	36 (19.6%)	136 (73.9%)	**172 (93.5%)**
Staff training is inadequate for using and managing the systems.	8 (4.3%)	5 (2.7%)	0 (0.0%)	37 (20.1%)	134 (72.8%)	**171 (92.9%)**
My library lacks sufficient funds or budget to purchase modern ESTs.	0 (0.0%)	0 (0.0%)	13 (7.1%)	48 (26.1%)	123 (66.8%)	**171 (92.9%)**
My library cannot afford the high maintenance and repair costs of existing ESTs.	22 (12.0%)	7 (3.8%)	2 (1.1%)	95 (51.6%)	58 (31.5%)	**153 (83.2%)**
I frequently face technical malfunctions or system downtime.	18 (9.8%)	8 (4.3%)	5 (2.7%)	130 (70.7%)	23 (12.5%)	**153 (83.2%)**
ESTs are complex and user-unfriendly.	30 (16.3%)	16 (8.7%)	24 (13.0%)	104 (56.5%)	10 (5.4%)	**114 (62.0%)**
The ESTs in use, including IT and network infrastructure, are outdated.	6 (3.3%)	13 (7.1%)	52 (28.3%)	86 (46.7%)	27 (14.7%)	**113 (61.4%)**
My library lacks reliable vendor technical support and after-sales service.	1 (0.5%)	2 (1.1%)	123 (66.8%)	31 (16.8%)	27 (14.7%)	**58 (31.5%)**
My library has unreliable electricity and no power backup.	70 (38.0%)	58 (31.5%)	0 (0.0%)	44 (23.9%)	12 (6.5%)	**56 (30.4%)**

Scale: SD = strongly disagree; D = disagree; N = neutral; A = agree; SA = strongly agree. Items are shown as worded in the questionnaire and ordered by combined agreement. Cells show the number of respondents and the percentage; N = 184 in brackets.
Source: Field data, 2026.

Human-resource, financial and technical constraints were the most prominent. Skill gaps (172; 93.5% agreement), inadequate training (171; 92.9%), and insufficient funds (171; 92.9%) drew the highest agreement, followed by high maintenance and repair costs (153; 83.2%) and technical malfunctions or downtime (153; 83.2%). A smaller majority agreed that the systems are complex and user-unfriendly (114; 62.0%) and that the technologies and supporting infrastructure are outdated (113; 61.4%). Two factors received little agreement. 56 respondents (30.4%) reported unreliable electricity without power backup, while 128 (69.6%) disagreed. For vendor support, 58 (31.5%) agreed that it is unreliable, but 123 (66.8%) were neutral. The neutral majority suggests uncertainty about, or limited exposure to, vendor arrangements rather than a demonstrated vendor problem.

Staff skills and training

Skill gaps and inadequate training were the most widely reported constraints. For ESTs to work effectively, staff must be able to operate, manage and troubleshoot them, and without regular training the smooth functioning of the systems is likely to suffer. The perception that staff lack the skills to protect library resources effectively is consistent with the view of key informants:

> *"Our library is faced with a challenge of the absence of system librarians who are trained to handle technical issues associated with the failure of electronic security systems."* (Library Director 1, 2026).

This suggests that the challenge is organizational as well as technological: the number and preparation of staff responsible for the systems matter as much as the systems themselves. It also indicates a need to review how security-related training is designed and delivered, including its content, frequency, and impact on security practice.

Funding and maintenance costs

Insufficient funds to acquire modern technologies 171 (92.9%) and to maintain and repair existing ones (153; 83.2%) were widely reported. This is consistent with earlier studies that found budget constraints limit libraries' ability to implement comprehensive security solutions (Hampwaye, 2022; Ibrahim & Kotoroi, 2025). Key informants reported that allocations fell short of what libraries requested in their annual procurement plans:

> *"Thank you for your question. Our library received less money than was allocated for this financial year, and the same needs to be channelled to*

> *different activities within the library. It is a problem and has a direct impact on our security operations."* (Library Director 1, 2026).

This may indicate that library security receives limited priority in institutional budgeting, making it difficult to upgrade outdated systems, acquire advanced technologies, and sustain technical support, training, and replacement.

Technical failures and malware

153 respondents (83.2%) reported technical malfunctions and downtime. Key informants from all four libraries reported computer viruses as a threat to their electronic security devices, particularly on internet-connected computers. One ICT director explained:

> *"Computer viruses are one of the greatest challenges in our library's automated environment. It is a threat when the antivirus software is not regularly updated."* (ICT Director 1, 2026).

Observations also showed that viruses caused malfunctions in computing equipment and that the risk of data loss was high when antivirus software was not updated promptly. This suggests that having technology does not necessarily lead to effective use when other important technical issues are neglected. It also illustrates that libraries must protect not only physical security devices but also the computers and networks on which digital security depends, so maintenance and cybersecurity practice belong together.

Electricity supply

Most respondents (128; 69.6%) did not perceive unreliable electricity as a constraint, although 56 (30.4%) did, which is not a negligible share. The pattern may reflect power-backup arrangements provided through parent institutions, but the data do not confirm this. Because ESTs cannot function without power, and because the pooled sample is dominated by one large library, institution-level checking is advisable.

Integrated view of the factors

Table 4 places the questionnaire, interview and observation evidence side by side. For skills and training, funding, and technical failures and malware, the sources converge. For electricity supply, only questionnaire evidence is available, and questionnaire and observation evidence support the underuse of advanced system functions, but interviews do not.

Table 4:
Joint Display of Questionnaire, Interview and Observation Evidence

Factor	Questionnaire (Agree + SA)	Interview evidence	Observation / other evidence	Integration
Staff skills and training	Skill gaps 172 (93.5%); inadequate training 171 (92.9%)	Absence of trained system librarians (Library Director 2)	Only a small group of staff worked with IT staff to process security reports and incident data	Convergent
Funding and maintenance costs	Insufficient funds 171 (92.9%); maintenance and repair costs 153 (83.2%)	Allocations below requested amounts (Library Director 1)	Not reported	Convergent (questionnaire and interviews)
Technical failures and malware	Malfunctions or downtime 153 (83.2%)	Viruses are a threat when antivirus is not updated (ICT Director 1); viruses reported at all four libraries.	Viruses caused equipment malfunctions; internet stability and EST performance recorded as infrastructure issues.	Convergent
Underuse of advanced functions	Neutral on reporting 111 (60.3%) and on tracking 84 (45.7%)	Not reported	Small group of staff processes reports; manual damage-checking of returned materials continues.	Complementary
Electricity supply	Agree 56 (30.4%); disagree 128 (69.6%)	Not reported	Not reported	Not corroborated

Source: Field data, 2026.

Taken together, the evidence indicates that the utilization of ESTs in these libraries is limited mainly by gaps in human capacity, funding and technical support. The performance of security technologies therefore depends not only on their availability but also on the skills of the people who operate them and on the resources committed to maintaining them. When library staff are not well prepared, technologies are likely to be underused, which may leave resources exposed to theft, vandalism, and unauthorized access. Because these results describe the prevalence of perceived barriers and were not tested inferentially, read them as indications of priority rather than proof of causation.

Strategies Proposed to Improve the Utilization of ESTs

Respondents were also asked, through open-ended questions, to propose measures to improve EST utilization. Their suggestions complement the researcher's recommendations and are summarized below by theme.

Providing adequate funds

The most widely endorsed proposal was that parent institutions allocate sufficient budget to procure, maintain, and sustain ESTs. A total of 138 respondents (75.0%) proposed that top management prioritize and allocate adequate funding to overcome the financial constraints affecting the performance of library security technologies. In the Tanzanian university context, where resources are shared among competing priorities such as teaching infrastructure and research grants, libraries may be left operating outdated or malfunctioning security technologies. Budgets should therefore be based on each library's assessed security needs.

Providing frequent training

A total of 172 respondents (93.5%) proposed frequent training for library staff on using ESTs, in line with the skill gaps reported in Table 3. Earlier studies of Tanzanian university libraries have reported similar human-factor barriers, including limited ICT competencies, a lack of in-service training, and low awareness of the importance of ESTs. Studies at institutions such as Mzumbe University, the University of Dar es Salaam, and the Nelson Mandela African Institution of Science and Technology have documented skill deficiencies linked to poor maintenance, unreliable performance and failure to realize the protective potential of EST investments (Ibrahim & Kotoroi, 2025; Komba, 2020; Kotoroi, 2023). Respondents therefore recommended frequent training as a sustainable way to close competency gaps. The researcher suggests a structured

program of regular training, for example at least quarterly, in place of occasional orientation sessions, so that staff keep pace with software updates and emerging threats in settings with staff turnover and multiple job roles.

Improving security technology infrastructure

Library staff proposed improving existing IT and network infrastructure, which they described as outdated, fragmented and inadequate for modern security requirements. This is consistent with Table 3, where 113 respondents (61.4%) agreed that the technologies in use are outdated. Based on these views, the researcher recommends that libraries prioritize modernizing core infrastructure, including servers, routers, and surveillance systems, to support technologies such as RFID-based tracking, biometric access control, and integrated surveillance, and that libraries institutionalize regular system audits, preventive maintenance schedules, and lifecycle-management plans to avoid obsolescence.

Limitations and Directions for Future Research

Four limitations should be noted. First, the analysis was descriptive: it reports the prevalence of perceived barriers and does not statistically test which factors determine utilization. Second, the questionnaire data are self-reported perceptions, and no loss or incident records were analyzed, so perceived protection outcomes cannot be treated as evidence that ESTs reduced losses. Third, results are pooled across four libraries of very different sizes, with UDSM contributing 51.6% of respondents, so pooled percentages may mask differences between institutions; the authors did not report institution-level comparisons. Fourth, the study included only four libraries, limiting generalization to other Tanzanian university libraries. Future studies should compare institutions directly, use inferential techniques such as regression to test determinants, and combine perception data with incident and loss records.

CONCLUSION

This study investigated the factors affecting the utilization of ESTs to safeguard information resources in four Tanzanian university libraries. Respondents perceived ESTs as contributing to the protection of physical and digital resources through theft prevention, control of unauthorized access, and real-time alerts. However, these are perceptions rather than measured outcomes.

Several factors were perceived to limit effective utilization: staff skill gaps, limited training, insufficient funds, high maintenance and repair costs, and frequent technical failures. Smaller groups reported outdated infrastructure and system complexity, whereas electricity supply and vendor support were not widely seen as constraints. Interviews and observation corroborated the human-resource, funding and technical constraints. The findings suggest that these constraints are interdependent rather than isolated barriers. The study also indicates that having security technology does not ensure effective use; utilization appears to depend on trained personnel, secure funding, ongoing maintenance, and supportive institutional policies. Enhancing the utilization of electronic security technologies therefore requires a comprehensive strategy that addresses technological, financial, organizational, and human-capacity issues and improves the protection and sustainability of library information resources in Tanzanian university libraries and, potentially, in similar academic settings.

RECOMMENDATIONS

This section provides recommendations from the findings of the study. Although academic libraries in Tanzania have made significant investments to improve the efficiency of their ESTs, challenges such as inadequate capacity-building, limited technical support, and maintenance issues persist. This report offers comprehensive suggestions for library staff, university library management, Tanzanian universities, and policymakers to address these challenges and maximize EST utilization. The recommendations provided are based on the findings.

Recommendations to Library Staff

i) **Improve Technical Competence:** Library staff should gain the skills to operate, troubleshoot and optimize use of electronic security technologies. Integrate basics of technologies like CCTV, RFID, and access control into operational training programmes. Knowledge of advanced troubleshooting skills to resolve system failures and data management and reporting skills to interpret systems effectively.

ii) **Encourage Ongoing Training:** Library staff should attend periodic security refresher training sessions to keep abreast of new electronic security developments and threats. This will help keep library personnel up to date on the latest systems.

iii) **Promote Feedback Mechanisms:** Library personnel should offer input to electronic security technologies in terms of their functionality, operational problems and new security concerns. This will help library management identify gaps and fine-tune the security system's performance.

Recommendations to the Library Management

i) **Establish a written maintenance schedule**: The library should establish a maintenance schedule for library electronic security technologies as part of library management. These schedules should include periodic system evaluation, inspection, and preventive procedures.

ii) **Invest in Integrated Electronic Security Technologies:** Library management should focus on the implementation of integrated electronic security technologies like the RFID system that integrates theft detection, inventory and circulation management. These systems can be integrated into the library management system to improve the efficiency of security operations.

iii) **Dedicated Security Personnel:** Library management should ensure that there are dedicated security staff to keep an eye on the CCTV systems and other security technologies in real time. This will enable proactive responses to security incidents, not just retrospective investigations.

iv) **Enhance** Communication and Collaboration: Library management should encourage collaboration among operational staff and the IT department so that all staff members know how to operate each of the security systems and how to follow the security protocols. This will reduce reliance on specific technical experts.

Recommendations to University Management

i) **Budget Allocation for Electronic Security Technologies:** University management should dedicate a budget for procurement, maintenance and upgrading of electronic security technologies. This will keep security systems sustainable and prevent them from becoming obsolete.

ii) **Enhance Support Staff Development:** The University management should build in an ongoing staff development program for library personnel and IT staff. These programmes should equip library staff with technical knowledge, operational skills, and strategic security management capabilities.

iii) **Implement Succession Planning:** Universities should have measures to maintain the knowledge of the institution, so technical skills remain even after trained personnel retire and leave the university library. This can involve documenting procedures and providing mentoring.

iv) **Support Digital Security:** Universities need to ensure electronic information resources are protected from unauthorized access and cyber threats by investing in cyber security measures like firewalls, antivirus, and digital rights management systems.

Recommendations to Policy Makers

Establish National Standards for Library Security: Develop national standards for library security, including guidelines for the deployment, operation and upkeep of technologies for electronic security. These standards should cover physical and digital security concerns. Additionally, effective implementation and maintenance of the library's security system should be an important factor in accreditation and quality assurance by policymakers such as the Tanzania Commission for Universities (TCU). This will raise the profile of library security as a requirement for library institutions.

REFERENCES

Adewojo, A. A., & Monjolaoluwa, O. P. (2025). Smart library environments: IoT and automation for next-generation services. *Information Development, 42*(4). https://doi.org/10.1177/02663821251384884

Allemang, B., Sitter, K., & Dimitropoulos, G. (2022). Pragmatism as a paradigm for patient-oriented research. *Health Expectations, 25*(1), 38–47. https://doi.org/10.1111/hex.13384

Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. Sage.

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Collis, J., & Hussey, R. (2014). *Business research: A practical guide for undergraduate and postgraduate students* (4th ed.). Palgrave Macmillan.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). Sage.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Sage.

Hampwaye, B. (2022). *Assessment of the security systems in selected libraries of higher learning institutions in Zambia* [Unpublished manuscript]. University of Zambia. https://dspace.unza.zm/server/api/core/bitstreams/9d9dc04f-bef9-418a-a323-0020f1c16396/content

Ibrahim, Z., & Kotoroi, G. (2025). Overcoming challenges in implementing electronic security systems at Mzumbe University Library: Strategic pathways for improvement. *American Journal of Information Science and Technology, 9*(1), 1–14. https://doi.org/10.11648/j.ajist.20250901.11

Iwara, F. U. (2019). Security, abuse of library materials and prevention in academic library: A case study of Kenneth Dike Library, University of Ibadan, Nigeria. *University of Ibadan Journal of Library and Information Science, 2*(1), 100-111. https://journals.ui.edu.ng/index.php/uijlis/article/view/793/694

Kavak, A. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. *The Journal of Academic Librarianship, 50*(5), 102937. https://www.sciencedirect.com/science/article/abs/pii/S0099133324000983

Komba, C. (2020). An Assessment Of The Effectiveness Of Library Electronic Security Systems In Higher Learning Institutions In Tanzania: A Case Study Of Udsm And Nm-Aist Libraries. [Unpublished manuscript]. The Open University of Tanzania. https://repository.out.ac.tz/2700/1/COMFORT%20SOLANOUS%20KOMBA%20-%20FINAL%202020.pdf

Kotoroi, G. (2023). Constraints facing African academic libraries in applying electronic security systems to protect library materials. *International Journal of Librarianship, 8*(1), 31–48. https://doi.org/10.23974/ijol.2023.vol8.1.272

Leavy, P. (2022). *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches* (2nd ed.). Guilford Press.

Mambo, H. L., & Comfort, K. (2019). An assessment of the effectiveness of library electronic security systems in higher learning institutions in Tanzania: A case study of UDSM and NM-AIST libraries. *Journal of Issues and Practice in Education, 11*(1), 102-111. https://doi.org/10.61538/jipe.v11i1.831

Marshall, C., & Rossman, G. B. (2022). *Designing qualitative research* (7th ed.). Sage.

Nath, R. (2021). Electronic security systems (ESSs) in academic libraries. *Library Philosophy and Practice (e-journal)*, Article 6234. https://digitalcommons.unl.edu/libphilprac/6234

Nsirim, O., Okeke, O. C., Ukubeyinje, E. S., & Dumbiri, R. (2025). Technology-based security systems and security of information resources in the university library. *Southern African Journal of Security*, *3*, 1-20. https://doi.org/10.25159/3005-4222/15883

Olaniyi, E. O., & Abioye, A. (2024). Use of electronic security systems for preservation of information resources in a university library in Oyo State, Nigeria. *Library Philosophy and Practice (e-journal)c*, 1- 20. https://digitalcommons.unl.edu/libphilprac/8198

Osayande, O., Mutula, S., & Izugbe, R. (2024). A comparative study of electronic security systems of academic libraries in selected public and private universities in South-West, Nigeria. *Journal of Applied Information Science and Technology, 17*(1). https://www.researchgate.net/publication/396356748_Odaro_Osayande_A_COMPARATIVE_STUDY_OF_ELECTRONIC_SECURITY_SYSTEMS_OF_ACADEMIC_LIBRARIES_IN_SELECTED_PUBLIC_AND_PRIVATE_UNIVERSITIES_IN_SOUTH-WEST_NIGERIA

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Sage.

Permana, I. S., Harianto, H., Syamsuddin, S., & Arifin, Z. (2025). Implementation of RFID (radio frequency identification) technology in libraries: A literature review. *Ilmu Informasi Perpustakaan dan Kearsipan, 13*(2). https://doi.org/10.24036/jiipk.v13i2.131897

Rahman, A., & Muktadr, G. (2021). SPSS: An imperative quantitative data analysis tool for social science research. *International*

Journal of Research and Innovation in Social Science, 5(10), 300–302. https://dx.doi.org/10.47772/IJRISS.2021.51012

Sunday, O. O., Maryann, N. O., Ajibola, R. R., Ayomide, O. A., Giwa, A. O., Faith, O. Y., & Tola, O. A. (2025). Adoption of electronic security systems in three academic libraries in Southwestern Nigeria. *Jewel Journal of Librarianship, 20*(2). https://www.jeweljournals.com/admin/published/21721326808.pdf

Sureshkumar, T., Hussain, A. A., & Jeyalakshmi, A. R. (2025). Enhancing library efficiency and user experience through RFID and kiosk integration. *International Journal of Engineering Research & Technology, 14*(11). https://www.researchgate.net/publication/398283442_Enhancing_Library_Efficiency_and_user_Experience_through_RFID_and_Kiosk_Integration

Taherdoost, H. (2022). What are Different Research Approaches? Comprehensive Review of Qualitative, Quantitative, and Mixed Method Research, Their Applications, Types, and Limitations. *Journal of Management Science & Engineering Research, 5*(01), 53-63. https://doi.org/10.30564/jmser.v5i1.4538

Tashakkori, A., & Teddlie, C. (2010). *Mixed methods in social & behavioral research*. Sage.

University of Nottingham. (2025). *Understanding pragmatism*. https://www.nottingham.ac.uk/helmopen/rlos/research-evidence-based-practice/designing-research/types-of-study/understanding-pragmatic-research/section03.html

Xu, H., Liu, W., Lu, L., & Zhou, Q. (2024). An IoT-based low-cost architecture for smart libraries using SDN. *Scientific Reports, 14*, Article 7022. https://doi.org/10.1038/s41598-024-57484-2

Njiru, M. (2022). Determinants of smallholder farmers' participation in agricultural cooperatives in East Africa. *Journal of Rural Development Studies, 14*(2), 78–90.

Tefera, S. (2022). Factors influencing cooperative membership in Ethiopia. *Journal of African Agrarian Studies, 18*(2), 55–66.

Verhofstadt, E., & Maertens, M. (2015). Can agricultural cooperatives reduce poverty? Heterogeneous impact of cooperative membership on farmers' welfare in Rwanda. *Agricultural Economics, 46*(4), 1–13. https://doi.org/10.1111/agec.12161

Zhou, Y., Li, X., & Wang, Q. (2021). Effect of cooperatives on farmers' income: Evidence from propensity score matching in Shennongjia region. *Sustainability, 13*(23), 13172. https://doi.org/10.3390/su132313172