

Availability and Use of Electronic Security Technologies in University Libraries in Tanzania

Richard C. Mfinanga

*Department of Media and Library Studies
The Open University of Tanzania (OUT), Dar Es Salaam
richardcmfinanga@gmail.com*

Henry Mambo

*Department of Media and Library Studies
The Open University of Tanzania (OUT), Dar Es Salaam
henry.mambo@out.ac.tz*

&

Lilian D. Isowe

*Department of Media and Library Studies
The Open University of Tanzania (OUT), Dar Es Salaam
lilian.isowe@out.ac.tz*

Abstract

This study assesses the availability and use of Electronic Security Technologies (EST) among university libraries in Tanzania to protect library information resources, using the libraries of the University of Dar es Salaam, Mzumbe University, Muhimbili University of Health and Allied Sciences, and the Institute of Accountancy Arusha as case studies. The study employed a convergent parallel research design and a mixed-methods research approach. It involves a sample of 196 respondents, particularly library staff, library directors, ICT directors, and IT personnel. These respondents were selected using a purposive sampling technique and a census method, respectively. The quantitative data were analyzed using SPSS, and the qualitative data were analyzed using thematic analysis. The findings revealed that CCTV cameras, electronic security gates, Radio Frequency Identification System (RFID), fire detection and suppression systems, and digital rights for e-resources are the most common types of electronic security technologies available. Library staff were aware of the availability of these electronic security technologies in their libraries. Despite high awareness among library staff of the availability and use of these ESTs, issues such as poor physical and operational conditions and insufficient training were identified. The study recommends frequent maintenance of ESTs, the procurement and enhancement of modern EST tools to improve the protection of library information resources, and training for library staff on the use of ESTs.

Keywords: *Academic library, availability, electronic security, technology, university.*

Introduction

Academic libraries are the heart of university education, because they provide information services and resources in various formats to support teaching, learning, and research objectives

of the learning institution (Nyemezu, Oladipupo & Ejuh, 2022). Hampwaye (2022) noted that the supply of up-to-date and effective library collections in higher education institutions' libraries is considered a major function in supporting teaching, learning, and research. Academic libraries are essential in discovery, cataloging, archiving, and accessing information resources to enable effective information retrieval and to serve the varied needs of users (International Federation of Library Associations and Institutions, 2023; Association of College and Research Libraries, 2022). In any higher learning institution, the library is important because it helps users access information resources for reading and report writing, and it enhances students' academic performance (Ibrahim & Kotoroi, 2025). To address this significant task in academic environments, the security of information resources must be ensured to protect library materials from theft, mutilation, and vandalism.

Academic libraries face several challenges, including theft, mutilation, and vandalism; as a result, library collections are not always safe and secure (Khan & Sonkar, 2024). This gives rise to the application of various methods of security technologies to safeguard library information materials. The overall security of libraries' collections, services, and investments has increased significantly through the installation of electronic security technologies (Nath, 2021). Sanga (2023) noted that safeguarding library information resources from theft and mutilation cannot be achieved solely through physical security measures, such as security guards and other traditional methods, given the growing number of library users and the expanding range of services offered in academic libraries. As library services expanded and the number of users grew, inadequacies of manual security measures became increasingly apparent. Relying solely on library security guards and staff proved insufficient to curb rising library security threats. Consequently, academic libraries began exploring alternative security measures to improve the security of library information resources and facilities, thereby adopting electronic security technologies (Lucas & Ibrahim, 2023).

Observations have revealed that most academic libraries in Tanzania have reported one form of security threat or another, which, if electronic security technologies were used, could be prevented. Considering the potential availability and use of electronic security technologies and the scarcity of similar studies conducted in academic libraries in Tanzania, this study was undertaken to fill the knowledge gap by assessing the availability and use of electronic security technologies in selected academic libraries in Tanzania, where there is a scarcity of similar studies conducted before among academic libraries to the best knowledge of the researcher.

Objectives of the Study

The general objective of this study was to assess the availability and use of electronic security technologies for protection of library information resources in in university libraries, a case of the Institute of Accountance Arusha, Institute of Finance Management, Mzumbe University.and the University of Dar Es Salaam. Specifically, the study sought to achieve the following specific objectives.

- 1) To determine level of awareness among library staff on the availability of electronic security technologies in the selected academic libraries.
- 2) To identify the types and determine the level of utilization of the available electronic security technologies in the selected academic libraries.
- 3) To examine the physical and operational conditions of the available electronic security technologies in the selected academic libraries.
- 4) To assess the training needs of library staff on the utilization of electronic security technologies in the selected academic libraries.

Review of Literature

Awareness Among Library Staff on ESTs

Olubiyo and Olubiyo (2025) noted that library staff need awareness of the security situation of library resources and the use of electronic security systems. Hampwaye (2022) noted that awareness is an element that cannot be seen, but is demonstrated through perceptions such as staff's attitudes toward the importance of security policies and processes, their awareness of security threats, and the limitations of implementation. Nath (2021) explained that electronic security technologies improve the safety of library resources and facilitate efficient library operations; however, the extent to which library staff understand and are familiar with these technologies determines their successful deployment and sustainability.

In addition, electronic security technologies have been embraced in many academic libraries, there are several studies that show that a significant portion of library staff have only moderate awareness of the functionality and operational procedures of these electronic security technologies. In recent years, the literature also indicates that awareness and technical ability of staff members are important factors that impact the effectiveness of electronic security technologies and that are important in reducing theft, mutilation and unauthorized removal of library materials (Aina & Mooko, 2022). Proper use of electronic security technology, coupled with adequate knowledge, can help to secure the library resources and improve the overall security management of the academic libraries (Aina & Mooko, 2022; Kumar & Singh, 2023). Kotorio (2023) opined that even when security technologies are available, ineffective use resulting from poor awareness among library staff limits their effectiveness in protecting library resources.

Types of Electronic Security Technologies Available in Academic Libraries

Vandana (2024) noted that electronic security technologies in libraries are crucial for protecting resources against theft, damage, and other crimes, thereby reducing the risk of resource loss and inconvenience to library patrons. Libraries use numerous security systems to protect their resources and ensure a safe environment for both users and staff (Ibrahim & Kotoroi, 2025). These electronic security technologies include radio frequency identification (RFID), closed circuit television (CCTV) systems, biometric access control systems, burglar alarms, perimeter intrusion alarms, smoke and flame detection devices, and a variety of other security sensors to improve the security of library information resources and facilities. Recent research has shown that the application of these technologies has helped to enhance security management in modern academic libraries and has led to a decrease in theft, vandalism and unauthorised access (Okoro & Adeyemi, 2022; Sharma & Patel, 2023). Oguedoihu & Adinchezo (2022) stated that video surveillance and closed-circuit television (CCTV) systems serve as a way to monitor and record security, deter crime, and ensure safety.

Furthermore, Oguedoihu & Adinchezo (2022) suggest that libraries use CCTV cameras to identify visitors and employees, monitor work areas, deter theft, and ensure the security of the premises and other facilities. CCTV cameras are a common security measure in academic libraries, providing real-time monitoring and deterrence against theft, vandalism, and disruptive behaviour. A study by Moustapha (2022) in Nigeria found that CCTV systems were widely used in academic libraries to prevent vandalism of information resources, particularly textbooks and journals. In Tanzania, the Use of CCTV is less prevalent due to funding constraints and a lack of technical expertise to manage these systems (Kotorio, 2023).

Electronic Security Technologies' Physical and Operational Conditions

Ibrahim and Kotoroi (2025) noted that RFID systems at Mzumbe University are largely ineffective in the library. Ibrahim and Kotoroi (2025) further noted that the underperformance of RFID and access control systems suggests either technical issues or improper implementation and use of the systems. Lucas and Ibrahim (2025) noted that poor implementation of electronic security technologies in libraries is caused by numerous physical problems such as camera calibration problems, degradation problems, inadequate coverage or blind spots, and environmental concerns like dust or electrical surges.

Lucas and Ibrahim (2025) also indicated that at Mzumbe University library, some electronic security technologies are installed and physically present; their operational conditions are inadequate due to poor maintenance, limited technical support, and budgetary constraints. In addition, electronic security equipment breakdowns reduce their effectiveness in academic libraries (Nyemezu, Oladipupo & Ejeh, 2022).

Library Staff ESTs Training Needs

Popoola (2020) noted that library staff need formal training on the security technologies installed in their libraries. Consequently, those who are trained demonstrate significantly higher awareness of the use of electronic security technologies. Insufficient use of electronic security technologies in academic libraries may reflect a lack of investment in staff training to fully leverage their benefits (Lucas & Ibrahim, 2025; Ibrahim & Kotoroi, 2025). Hampwaye (2022) opined that training on security technologies in academic and other types of libraries has been helpful to both library staff and users, as it makes everyone aware of library security issues and the consequences of being found on the wrong side of the law.

Hampwaye (2022) found that insufficient training and a lack of continuous professional development contributed significantly to the poor utilization of electronic security technologies

in libraries. Some strategies to enhance the availability and use of electronic security technologies among university libraries for effective service delivery are training library staff on acquiring ICT skills, improving funding for electronic security systems, updating systems to avoid failure, providing an alternative source of power, and employing competent personnel to handle electronic security systems in library organizing seminars and training on the use of electronic security systems.

Methodology

A convergent parallel research design was adopted for this study, which was carried out across four academic libraries: the University of Dar es Salaam, Mzumbe University, Muhimbili University of Health and Allied Sciences, and the Institute of Accountancy Arusha. The study population comprised the entire library staff from all four academic libraries, totaling 196. This is made up of one library director, one ICT director, one IT personnel, and 101 library staff from the university of Dar es Salaam, one library director, one ICT director, one IT personnel, and 46 library staff from Mzumbe University, one library director, one ICT director, one IT personnel and 19 library staff from Institute of Accountancy Arusha and one library director, one ICT director, one IT personnel and 18 library staff from Muhimbili University of Health and Allied Sciences. The purposive sampling technique was employed to select 12 key respondents and the study's areas. The study also employed a census method to select 184 library staff, as they all use electronic security technologies to protect library information resources.

Structured questionnaires, interviews, and observation checklists were the instruments used for data collection. The data were presented according to the research objectives that guided this study, and the quantitative data were analyzed using SPSS (Version 27). In contrast, the qualitative data were analyzed using thematic analysis.

Findings and Discussion

Awareness of the Availability of Electronic Security Technologies in the Library

Responses indicated that 184 (100%) were aware of the availability of electronic security technologies in their libraries for protecting library information resources (Table 1).

Table 1: *Awareness of Electronic Security Technologies Availability (N=184)*

University	Yes		No		Total	
	Frequency	%	Frequency	%	Frequency	%
IAA	19	10.3	0	0.0	19	10.3
MU	46	25	0	0.0	46	25
MUHAS	18	9.8	0	0.0	18	9.8
UDSM	101	54.9	0	0.0	101	54.9
Total	184	100	0	0.0	184	100

Source: *Field Data, 2026*

From Table 1, it was evident that library staff were familiar with electronic security technologies, as 184 (100%) of the respondents had, in one way or another, interacted with them. Even though the majority of respondents (184, 100%) are aware of the availability of electronic security technologies in their libraries, 92 (50%) hold lower-level positions (library officers), suggesting that the workforce may lack the authority to make decisions or implement modern electronic security systems. The results, on the other hand, paint a very positive picture of the part of the library staff that understands electronic security technologies and their corresponding targets.

The picture of electronic security utilization awareness resonate with that on Africa as depicted in literature Olaniyi and Abioye (2024), reported that when library staff are aware of the existence of electronic security technologies, they are more cautious in whatever they are doing

and are less likely to engage in malicious actions such as stealing information and library resources, when at a library and other acts which contribute to the deterioration of library and information resources in the library, such as theft, mutilation and vandalism, eating in the library, smoking in the library environment and more. Ogedoihu and Adinchezor (2022) observed that library staff were aware of various electronic security technologies/measures available in academic libraries in Southeast Nigeria, and that both management should provide adequate safety measures for library resources.

The findings also align with the findings of Olubiyo and Olubiyo (2025), who conducted a study on awareness of security issues on library resources by library staff in Adeyemi Federal University of Education Library, Ondo, Nigeria pointed out that out of 24 participants of their study, all 24 (100%) said that they are aware of the library security issues which implies that library staff are aware of library security issues. Komba (2020), in his study on an assessment of the effectiveness of electronic security systems in higher learning institutions in Tanzania, noted that all respondents in his study were aware of the use of electronic security systems in the libraries, as they had seen the detection machine installed at the main entrances of the library buildings.

Furthermore, the fact that all respondents (100%) were aware of electronic security technologies indicates that awareness is no longer a major barrier to their adoption in academic libraries. This suggests that electronic security systems have become visible and recognizable components of library operations. High staff awareness may help protect library resources, as informed staff are more likely to comply with security procedures, identify suspicious activities, and support institutional security goals. The findings, therefore, imply that library-based awareness-raising initiatives have been relatively successful.

Types of Available Electronic Security Technologies

Table 2 presents findings on the types of electronic security technologies implemented in academic libraries to protect library and information resources.

Table 2: *Types of Available Electronic Security Technologies (N=184)*

Type of Electronic Security Technology	Frequency	Per cent (%)
Closed-circuit television (CCTV)	122	66.30%
Electronic security gate	85	46.2%
Radiofrequency identification system (RFID)	56	30.43%
Fire detection and suppression systems	118	64.1%
Digital rights (DRM) for e-resources	101	54.9%

Source: *Field Data, 2026*

Table 2 shows that closed-circuit television cameras (CCTV) 122 (66.30%) are the most used electronic security technology for the protection of library resources, followed by fire detection and suppression systems 118 (64.1%), and digital rights for e-resources 101 (54.9%); the second least was electronic security gates 85 (46.2%). The least was radio frequency identification systems (RFID) 56 (30.43%).

The findings of this study indicated that one form or another of electronic security technologies (ESTs) was in use in the participating academic libraries. These security technologies included the closed-circuit television (CCTV) cameras, electronic security gates, and the radio frequency identification (RFID) system. These findings concur with Aina & Mooko, 2022; Ogedoi, 2022; Kotori, 2023 and Ibrahim & Kotori, 2025) who explained that Closed Circuit Television (CCTV) cameras, library electronic security gates, and a radio frequency

identification (RFID) system are some of the electronic security systems (ESS) that are implemented or installed in academic libraries to curb the menace of book theft and mutilation. They are among the most popular and commonly implemented electronic security technologies in libraries.

With respect to types of electronic security technologies available, one key respondent had the following to say:

"Our library has CCTV cameras, security gates, and RFID, which are used to enhance the security of our library resources in the sense that library materials that are not legally checked are not allowed to be taken out of the library premises by any library user". (Library Director 1, 2026)

Library Director 2 pointed out that:

"Our library uses an electronic security gate, which is fully functional, and our library resources (books) have strips inserted into them, and they are integrated with the security gate that has a sensor which detects when unchecked library materials are taken out of our library. (Library Director 2, 2026)

Library Director 3 noted that:

"Our library has CCTV cameras in place that help to monitor the movements of our users, whereby if any unethical incident happens, our technical team revisits the security systems to identify the suspect for legal action". (Library Director 3, 2026)

From the findings, it is evident that CCTV cameras can help monitor library resources and are the most widely used electronic security technology across the four visited academic libraries.

The findings align with those reported by Komba (2020), who found that CCTV cameras are installed and utilized in academic libraries and has been found to be effective to deter theft, mutilation and vandalism in the library, the identification of library visitors and employees and monitoring of various library areas. In contrast, the findings reported by Ibrahim and Kotoroi (2025) at Mzumbe University indicate that CCTV cameras are underutilized due to limited coverage, inadequate staff to monitor footage, or budgetary constraints. Since CCTV cameras offer broad surveillance, underutilizing them could leave certain areas of the library vulnerable to security breaches. Electronic security technologies can be used as proof in a law court (CCTV cameras), together with improving the working efficiency in libraries (Nyemezu, Oladipupo, & Ujuh, 2022).

Physical and Operational Conditions for the Available Electronic Security Technologies

Table 3 presents findings on the physical and operational conditions of each security technology implemented in libraries.

Table 3: *Perceived Physical and Operational Conditions for the Electronic Security Technologies (N=184)*

Technology	Rating Scale					
	Very Poor (%)	Poor (%)	Don't Know (%)	Fair (%)	Good (%)	Very Good (%)
Closed-circuit television (CCTV)	-	25	-	56	83	20
	-	13.6%	-	45.1%	30.4 %	11%
Electronic security gate	-	-	30	62	18	14
	-	-	16.3%	33.1%	9.8%	7.6%
	5	46	-	82	36	-

Radiofrequency identification system (RFID)	2.72%	25%	-	44.6%	19.6%	-
Fire detection and suppression systems	-	-	126	28	9	-
	-	-	68.5%	15.2%	4.1%	-
Digital rights management (DRM) for e-resources	-	-	139	-	-	-
	-	-	75.5%	-	-	-

Source: *Field Data, 2026*

The findings from the study show that out of 184 respondents, the majority, 139 (75.5%), indicated that they are not aware whether the digital rights management for e-resources is operationally working, and 126 (68.5%) of respondents noted that they do not know the physical condition of fire detectors and suppression systems. In contrast, 62 (33.1%), said that the electronic security gate is in fair condition, 30 (16.3%) of respondents reported that they do not know the physical condition of electronic security gates in their libraries, 18 (9.8%) said the electronic security gate is in good condition, and 14 (7.6%) of respondents said that the electronic security gate is in a very good condition. In contrast, 83 (45.1%) of respondents said CCTV cameras are in fair condition, 57 (31%) said they are in good condition, and 20 (11%) said they are in very good condition. In contrast, 25 (13.6%) said that CCTV cameras are in poor physical and operational condition. With respect to RFID, 82 (44.6%) said that the RFIDs are fair, 46 (25%) said RFIDs are in poor condition, 36 (19.6%) said RFIDs are good, and 5 (2.72%) said RFIDs are in very poor physical and operational condition.

The findings indicate that, in general, the electronic security technologies available in the study areas are in relatively good condition but require maintenance, and some require total replacement. The findings align with those of Ibrahim and Kotoroi (2025), who noted that RFID systems at Mzumbe University are largely ineffective in the library. Ibrahim and Kotoroi (2025) further noted that the underperformance of RFID and access control systems suggests either technical issues or improper implementation and use of the systems.

Observation findings indicated that some electronic security systems were non-functional, specifically CCTV cameras, RFID systems, and access control systems. The poor and uneven performance of the systems leaves gaps in security infrastructure that expose library information resources to theft, mutilation, unauthorized access to materials, vandalism, and potential damage. The observation aligns with Ibrahim and Kotoroi (2025), who noted that the library's failure to utilize more advanced electronic security technologies, such as RFID, access control, and CCTV cameras, to their full potential leaves it vulnerable to both physical and digital threats. Academic libraries need to adopt a universal security approach that balances physical theft, digital asset protection, and access control. This can be achieved by upgrading and maintaining underperforming systems.

Interviews with IT personnel to identify the physical and operational conditions of the available electronic security technologies indicated that some technologies are not functioning and others require repair and maintenance, as illustrated by the following quotes.

"We have been experiencing technical issues with our security systems, and we normally carry out preventive maintenance, and sometimes some of the electronic systems have been unstable". (IT personnel 1, 2026)

"Our library only uses theft and smoke detectors to prevent theft and fire damage after they occur. Additionally, regular maintenance checks have not been conducted to prevent systems from failing due to budgetary issues; for example, our CCTV cameras are not functioning in many areas in the library, which makes it difficult to monitor activities within the library, making both library resources and library users vulnerable to security threats." (IT personnel 2, 2026)

"Well, our electronic security technologies may require upgrading to more standardized technologies which are currently in the market to improve security effectiveness and enable more efficient tracking of library resources". (IT personnel 3, 2026)

"The library has procured new electronic security systems, which are now installed to replace the old systems. As it is known, some of the systems were installed many years ago and are not functioning properly, hence the library management has decided to procure the new ones to improve the security in the library". (IT personnel 4, 2026)

From the above responses, respondents believe that although electronic security technologies are available and used to protect library resources, they require frequent maintenance and upgrading to newer security technologies to improve security. Nath (2021); Nyemezu, Oladipupo & Ejeh (2022) noted that inadequate funding from parent institutions has ultimately affected the delivery of library and information services, including the installation and maintenance of electronic security systems. The findings also align with Ibrahim and Kotoroi's (2025) observation that CCTV cameras at the MU library are not functioning in many areas, a significant concern in academic libraries in Tanzania.

The study's findings imply that the effectiveness of electronic security technologies in the studied libraries is compromised by poor functionality, inadequate maintenance, and obsolete systems. Although some respondents reported technologies such as CCTV cameras and RFID systems to be in fair or good condition, the high proportion of respondents reporting poor condition or uncertainty about system functionality suggests that the technologies are not operating optimally. This creates vulnerabilities in library security systems, thereby increasing the risk of theft, vandalism, mutilation of information resources, unauthorized access, and fire-related damage. The observation that CCTV cameras and RFID systems were non-functional

in several areas further implies that the libraries are relying on partially effective security infrastructures. Consequently, the inability of these systems to provide continuous surveillance and monitoring weakens both preventive and detective security mechanisms in academic libraries.

Training on the Use and Implementation of Electronic Security Technologies

Figure 1 presents findings on library staff training needs for the use of electronic security technologies in libraries.

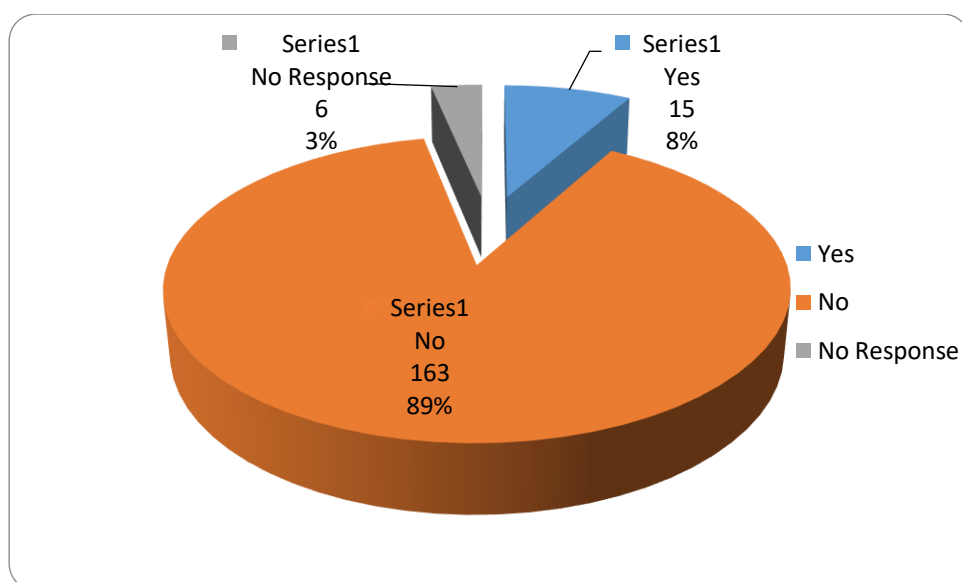


Figure 1: Library Staff Training on ESTs (N=184)

Source: Field Data, 2026

From Figure 1, it is seen that a vast majority, 163 (89%) of the respondents, did not receive or attend any training on the utilization of electronic security technologies in their libraries; 15 (8%) respondents said they had received training on ESTs. They even reported that the training was useful. On the contrary, 6 (3%) did not respond to the question at all. A further inquiry

revealed that those library staff who had not received or attended training on electronic security technologies operation suggested that they need to be trained on various issues, such as how to operate and use ESTs, security devices troubleshooting, and how to implement new security technologies in libraries, data management and reporting training, and library electronic data access security control.

From the findings above, it is established that the majority, 163 (89%) of the respondents have not received or attended any training on the use of ESTs. Interview with library directors and IT personnel to know if they have special library staff training on ESTs training program, and the results indicated that all four (04) academic libraries under study had no scheduled staff training on the Use of ESTs, as illustrated by the following quotes.

"Actually, we have no specific budget set aside for the training of library staff on the utilization of electronic security technologies. Some of our library staff and IT personnel were trained during the installation process and during induction sessions when they were newly employed, but that was not enough, as they did not have enough time to learn the system's operations in depth. Some of those who were trained have retired". (Library Director 1, 2026)

"Our IT personnel team is trained by the electronic security systems vendors/suppliers during the process of system installation, and we also receive the after-sales training from the suppliers". (ICT Director 1, 2026)

"When the university has a budget set aside for training, we outsource a technical team from outside to train our IT personnel, but for some years now, this has not been done due to the decline in our budget". (ICT Director 2, 2026)

"If a system's fault happens and needs to be addressed with our technical team, and if it is not within our capacity, we communicate with the vendor to solve the issue or invite the vendor's team to the field, and that is when our technical personnel get the chance to learn from them". (ICT Director 3, 2026)

"As an IT personnel assigned to manage and solve EST's technical issues, I was trained by vendors during the installation process, and thereafter, I use the acquired skills to manage the systems". (IT Personnel 1, 2026)

The findings reveal that EST training is not frequently provided to system users (library staff), and those who have received it still need ongoing training to keep up with new trends. On the other hand, it is expected that IT personnel who manage the ESTs could have gained skills through the systems' vendors during the installation and after-sales training. The findings underscore the significance of in-house EST training and workshops for library staff and IT personnel to enhance the security of library resources. Library staff need to learn more about electronic security technologies operations through either on-campus or by attending workshops and professional conferences. Hampwaye (2022) opined that there was a need for a continuous programme of in-service training to facilitate on-the-job skills development for library personnel, thereby enabling effective information and service delivery to the library clientele.

In the Tanzanian context, the existing literature shows that academic libraries have not been able to train their library staff to effectively utilize electronic security technologies, which has ultimately affected the delivery of library and information services, including the installation, management, and maintenance of these technologies. Insufficient Use of ESTs in academic

libraries may reflect a lack of investment in staff training to fully leverage the benefits that electronic security technologies can offer (Lucas & Ibrahim, 2025; Ibrahim & Kotoroi, 2025).

They further explained that it may also be necessary to invest in library staff training to ensure that all personnel can use these electronic security systems to their full potential.

The implication of failing to expose library staff to EST-related workshops and training is that this discrepancy is likely to result in low utilization of ESTs by key library staff. Additionally, a lack of training suggests that library staff were unlikely to perform key security-related activities for library information resources.

Conclusions and Recommendations

The study found that library staff have a high level of awareness of the availability and use of electronic security technologies. This is primarily due to the understanding of the importance of library information resources security in academic libraries. The most common types of electronic security technologies available and used in academic libraries include CCTV cameras, electronic security gates, RFID, fire detection and suppression systems, and digital rights for e-resources. The findings indicate that, in general, the electronic security technologies available in the study areas are in relatively good condition but require maintenance, and some require total replacement. The findings also revealed that EST training is not frequently provided to library staff, and those who have received it still need ongoing training to keep up with new security technology trends.

The following recommendations are provided based on the findings of this study; First, academic libraries and their parent institutions should adequately fund their libraries to enable them to procure modern electronic security technologies and maintain them. Second, library staff should be trained to acquire the skills needed to effectively utilize the electronic security technologies to enhance the protection of library information resources and third, with constant

improvements in electronic security technology infrastructure, there is a need to enhance EST infrastructure, such as internet connectivity, power supply, and EST devices, to ensure smooth security provision in libraries.

References

- Aina, R. F., & Mooko, N. P. (2022). Electronic security systems and protection of information resources in academic libraries. *Library Management*, 43(6/7), 412–425.
- Association of College and Research Libraries. (2022). Standards for Libraries in Higher Education.
- Hampway, B. (2022). Assessment of the security systems in selected libraries of higher learning institutions in Zambia [Unpublished manuscript]. *The 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
- International Federation of Library Associations and Institutions. (2023). IFLA Guidelines for Academic Libraries.
- Komba, G. (2020). The impact of security systems on resource preservation in Tanzanian academic libraries. *Tanzania Library Journal*, 29(3), 14–28.
- 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>
- Kumar, S., & Singh, P. (2023). Staff awareness and utilization of electronic security technologies in university libraries. *The Journal of Academic Librarianship*, 49(2)
- Lucas, M. & Ibrahim, Z. (2025). Investigating the Ineffectiveness of Electronic Security Systems in Safeguarding Library Materials at Mzumbe University Library: Challenge Of Using Electronic Security Systems In Academic Libraries. *International Journal of Librarianship*, 10(1). <https://doi.org/10.23974/ijol.2025.vol10.1.438>

- Nath, R. (2021). Electronic security systems (ESSs) in academic libraries. *Library Philosophy and Practice* (e-journal), 6234. <https://digitalcommons.unl.edu/libphilprac/6234>
- Nyemezu, C. O., Oladipupo, R. O., & Ejuh, E. (2022). Availability and utilization of electronic security system among university libraries in Rivers State, Nigeria. *Rivers State University Journal of Education (RSUJOE)*, 25(2), 60–73. www.rsujoe.com.ng
- Oguedoihu, J. C. & Adinchezor, I. P. (2022). Library and information services and security challenges in two selected academic libraries in Southeast Nigeria. *Ghana Library Journal*, 27(2), 139–293.
- Okoro, C. C., & Adeyemi, O. A. (2022). Adoption of electronic security technologies in academic libraries: Trends and challenges. *Library Hi Tech News*, 39(8), 15–21.
- Olaniyi, O. E. & Abioye, A. (2024). Use of Electronic Security Systems for Preservation of Information Resources in a University Library in Oyo State, Nigeria. University of Ibadan
- Olubiyo, P. O. & Olubiyo, J. T. (2025). Awareness of security issues on library resources by library staff in Adeyemi Federal University of Education Library, Ondo, Nigeria. *Academic Research Journal on Health Information Management*, 6(2), 59-67. <https://www.academicresearchjournals.org/ARJHIM/Index.htm>
- Popoola, S. O. (2020). Training and awareness as correlates of library personnel's use of security technologies in university libraries in South-West Nigeria. *Nigerian Libraries*, 53(1), 1–14.
- Sanga, W. K. (2023). Acceptance and Use of Online Resources amongst University Students in Selected Higher-Learning Institutions in Iringa, Tanzania (Doctoral dissertation, The Open University of Tanzania).
- Sharma, R., & Patel, M. (2023). Electronic surveillance systems and library resource protection in higher education institutions. *The Electronic Library*, 41(3), 487–501.