Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.4, 2025, pp.247-257

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.4.28

Smart Surveillance and Security Systems in Library Information Management

Dr.R. Udayakumar[1*], Dr. Praveen Kumar[2], Dr.E P John[3], Hasssan MuhamedAle[4], Mamadjanova Zukhra Bakhromjanovna[5] and R. Ramya[6]

[1*]Dean Research, SRM Groups, Chennai, India
[2]Professor & Dean, Faculty of Management, SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India
[3]Assistant Professor (Sr G), Department of Management Studies, SRM Valliammai Engineering College, Kattankulathur, Chengalpattu, Tamil Nadu, India
[4]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq
[5]Turan International University, Namangan, Uzbekistan
[6]Assistant Professor, Department of Electronics and Communication Engineering, K.S. Rangasamy College of Technology, Tiruchengode, India
E-mail: [1]deanresearch@srmgroup.co.in; rsukumar2007@gmail.com, [2]dean.mgmt.rmp@srmist.edu.in,[3]johnep.mba@srmvalliammai.edu.in, [4]tech.iu.comp.hassanaljawahry@gmail.com, [5]zuhramamadjanova7@gmail.com, [6]rramya@ksrct.ac.in
ORCID: [1]https://orcid.org/0000-0002-1395-583X, [2]https://orcid.org/0000-0002-6158-4420, [3]https://orcid.org/0000-0003-3129-2133, [4]https://orcid.org/0009-0002-6414-5172, [5]https://orcid.org/0009-0000-5120-7085, [6]https://orcid.org/0000-0002-7841-4129
(Received 25 August 2025; Revised 11 October 2025, Accepted 24 October 2025; Available online 15 December 2025)

Abstract **- Libraries, once facilities that stored books, have over the years transformed into dynamic data centers of information, featuring increased access demands, specialized access controls, enhanced industrial security levels, and more sophisticated management systems. One of them is the Smart Surveillance and Security Systems (SSSS), which combines the use of the Internet of Things (IoT), artificial intelligence (AI), machine learning, real-time monitoring, and information systems automation technology to transform the library information systems. Automated and facial recognition surveillance for theft, intrusion, and asset tracking makes unauthorized access and theft difficult. Furthermore, the SSSS enhances security resource management, user behavior analysis, management efficiency, and space utilization. SSS supports policy formulation and decision-making by enabling data-driven choices. Policy responsiveness enhances the safety and responsiveness of librarian policies. Error accumulation in smart systems technology is mitigated by smart systems in access control, inventory management, and operational cost management streamlining. This paper highlights the optimal reduction of information overload and the provision of an optimal multidisciplinary view of smart surveillance systems for library information assets. Study results underscore the need for smart surveillance systems in libraries to address privacy concerns, which is an initial investment consideration. After deeper analysis, it is concluded that investments in smart security solutions are essential for the integrated evolution of evolving library systems.**

Keywords: **Smart, Surveillance, Security, Systems, Library, Information, Management**

I. INTRODUCTION

As previously indicated, smart surveillance and security systems employ technologies such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT) (Ojo & Dahunsi, 2024; Makinde et al.,2025; Zhang et al., 2025; Maceli, 2020) Smart surveillance also utilizes more sophisticated forms of Intelligent Video Analytics (IVA), facial recognition, motion detection, remote access, automated alarm systems, and various other analytics to enhance effectiveness in diverse settings (Zhang & Wang, 2021; Showers & Stone, 2014). In libraries, these systems not only help prevent theft and vandalism but also aid in automating the monitoring of patrons, controlling movements within the workspace, and tracking various resources (Lee et al., 2020; Venkadeshwaran et al., 2025). Unlike Smart Systems that solely depend on human oversight in conjunction with basic CCTV cameras, Smart Surveillance Systems integrate proactive alerting, automated response to security triggers, and actionable intelligence, which fundamentally enhance security management (Choi & Lee, 2019; Gupta & Margam, 2021). A library integrates a range of resources, including digital and physical books, computers, and other multimedia equipment (Gul & Bano,2019). Incorporating all these modern technologies increases the complexity of risk management and safety. Smart surveillance systems enable libraries to control safety and order levels for all users and staff (Ahmed & Rehman, 2022; Anand et al., 2024). Smart surveillance systems can restrict access to certain areas of the library, protect valuable documents such as books and paintings from theft, and monitor the temperature and humidity levels to preserve the documents in the long term (Martínez & González, 2023). They can also improve service delivery by analyzing the movement of patrons within the library (Singh & Patel, 2021; Kesana et al., 2021). Such systems hold significant importance in libraries because they maintain proper order and control access to data and information, the loss of which can be detrimental to the institution (Kumar & Roy, 2020).

Furthermore, in educational institutions, libraries are provided with round-the-clock access and serve as study spaces (Hamad et al., 2023). Off-hours protection of users poses an alarming problem. For instance, intelligent systems can alert relevant authorities during the outbreak of fires, medical emergencies, or instances of aggressive behavior (Brown & Thompson, 2019; Hwai et al., 2023). Such technology may also help ensure compliance with policies, such as preventing unauthorized access to sensitive zones or materials.

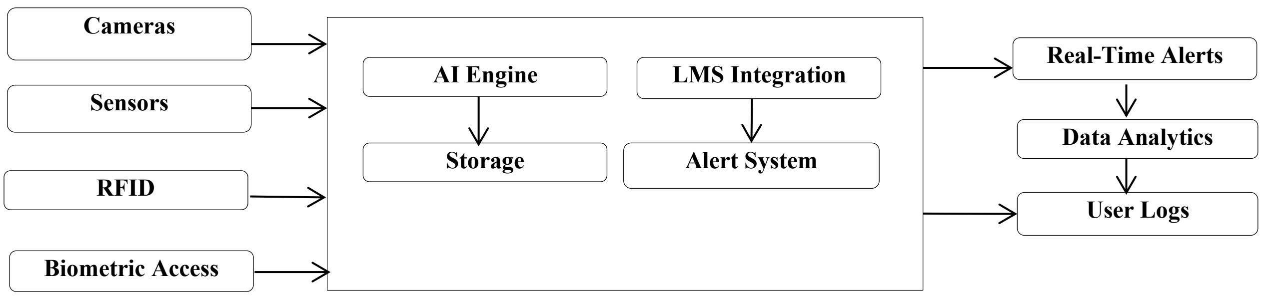

Fig. 1 Architecture Diagram – Smart Surveillance System in Library

The smart library surveillance system (Fig. 1) captures its architecture, flow, and functionalities in a systems diagram. Starting from peripherals such as cameras, sensors, RFID scanners, and biometric terminals, user and access activities related to resources, as well as interactions with them, are continuously monitored (Suhaimi et al., 2023) The input is processed within a core processing unit that consists of an AI behavior analysis and anomaly detection engine, an LMS (Library Management System) access and inventory control interface, footage and logs storage unit, and a security notification alert system. The system's outputs include notifications requiring urgent responses, compiled data analytics reports for managerial decisions, and user information logs for future auditing and historical activity analysis. This surveillance system model improves user safety and efficiency while also increasing the automated capabilities of the surveillance systems. The design will provide an opportunity to add or alter components to meet changing demands flexibly.

Yusuf and Bala (2020), as well as (Veerappan, 2024), unveil how the lack of privacy considerations, shortage of funds, and lack of expertise have hindered the development of smart surveillance and security systems in libraries (Meesad & Mingkhwa,2024). Simple security that involves guards and CCTV is no longer effective to the many advanced challenges facing the modern library. These are, among others, stealing, poor access management, vandalism, and wasteful management of scarce space and resources (Okoro & Uche, 2021). In this research, the researcher seeks to explore the issue of using smart surveillance and security system to improve information management in a library (Zhang, 2025).

The paper is intended to fill this gap by looking at the effects of digital innovations in the field of library science to provide the contributions towards improving the role of intelligent technology to protect and simplify information systems in libraries (Schöpfel, 2018). The paper will consist of six main sections to enable the systematic understanding of the role of smart surveillance systems in library information management. The Literature Review reviews the literature on the current library security systems, benefits of smart surveillance and gaps informed by the previous literature. Specifically, the Implementation section explains the equipment and hardware of the system, the process of integration, and staff training that would be needed to use the system. Next, the Impact section evaluates the implication of smart surveillance systems to security, data analytics, operational productivity, and other pertinent library functions based on performance measurement systems, to support these assertions. The Case Studies section is the collection of actual projects, whose successful implementation is documented, and the results of projects are analyzed and the main points are brought out. The Conclusion summarizes all the points made, analyzes the implications on the management of the libraries, and proposes future studies and practice. This description is the most appropriate to the audience, as it addresses the whole range of developments of smart surveillance technologies into a library, both in theoretical frameworks and practical dilemmas (Duarte et al., 2016).

II. Literature Review

Historically, libraries have relied on traditional security measures, including CCTV cameras, security guards, alarm gates, and barcode or RFID-controlled inventory systems (Mabweazara, 2021; Amit, 2018; Albakri et al., 2015). These systems have mitigated fundamental dangers, such as theft and vandalism, but often fail to address multifaceted challenges that require real-time, anticipatory responses and threat analysis (Ndhlovu & Mutula, 2020). For example, standard CCTV surveillance systems can document events, but they lack the capability for analysis or feedback. Moreover, systems that rely on human intervention, such as those involving CCTV surveillance of patrons, are susceptible to errors and fatigue (Olorunfemi & Adebayo, 2019). Most libraries also encounter difficulties in controlling access to restricted areas, monitoring valuable archival items, and moderating behavioral guidelines amongst users (Essel & Ackah, 2018; Petrova & Kowalski, 2025). These shortcomings highlight the need for more advanced technology solutions that provide both automation and intelligence. The implementation of smart surveillance technologies in libraries has proven very beneficial (Hussain, 2021). Through the integration of AI and ML, these systems not only monitor activities but also automatically alert staff in real-time, recognize the faces of known trespassers, and identify specific behavioral patterns that can be defined as abnormal (Chamyan & Farahani, 2016; Pakkiraiah & Satyanarayana, 2024). These systems significantly enhance the security of the institution while improving overall library operations by reducing the need for extensive manual surveillance (Oguedoihu & Adinchezor 2022). Another advantage is the analysis of users' traffic patterns within a given area. With the rise of smart sensors and video surveillance, librarians can now determine which sections most capture users' attention, leading to improved space management and resource allocation (Bashir & Mani, 2021; Ristono & Budi, 2025). These data provide the basis for these libraries to adjust their structures and expand services to users, as alterations to zones or lighting can be made in heavily congested areas (Agboke & Oladokun,2024). Another benefit includes the control of theft and unauthorized access to facilities. The system with biometric or smart card access will help to control access to specific valuable locations, such as the archives of rare books and server rooms (Gupta & Thakur, 2021). Such systems also may activate automated locks and sound alarms and provide evacuation instructions, in particular in case of an emergency (Iqbal & Sheikh, 2020). Moreover, IoT gadgets improve the conservation of artifacts, including manuscripts and photographs, by regulating appropriate temperature and humidity levels, as well as lighting (Graf, 2022; Wanas & Turky, 2024). There are studies where smart surveillance systems have been tested in libraries and other information settings. (Wong & Lam, 2021) observed in their research that libraries with AI-based surveillance saw their theft cases reduce by 40% and higher user satisfaction was registered (Dai, 2025). On the same note, (Ochieng & Wanjiru, 2022) observed that the improved organizational discipline among the library staff and users as well as the compliance to the institutional policies were attained as a result of increased security measures. In addition, (Kaur & Gill, 2020) reported in their comparative research that the combination of RFID and access control with smart surveillance systems significantly enhanced the material tracking and user data protection (GMitErEK, 2025). These systems enhanced inventory audits and tracking of misplaced or misfiled items (Vasquez & Sorensen, 2025; Hashim et al., 2022). Other scholars argue that these systems become useful only after proper implementation, staff training, and the resolution of ethical issues related to data privacy (Ali & Rehman, 2021; Bergsrud & Vaseeharanathan,2024). Other ongoing ethical concerns include the risks associated with surveillance via facial recognition, as well as data and accessibility issues (Anwar & Khan, 2023; Ubid, 2022; Upala & Wong, 2019). Although the effectiveness of these strategies is well-known, it can only be achieved through careful implementation and stakeholder engagement.

III. Implementation of Smart Surveillance Systems

3.1 Choosing the Fitting Technology and Equipment

The initial step in deploying smart surveillance systems in libraries is selecting the appropriate technology and equipment tailored to the library's specific needs, considering its spatial layout, dimensions, size, circulation area, and the requirements for comprehensive surveillance and security. Other essential components may include high-resolution IP cameras, biometric access control units, motion sensors, environmental sensors such as temperature and humidity sensors, data storage servers, and analytical tools. More sophisticated systems should include facial recognition systems, crowd counting capability, and behavior monitoring systems. To enhance the placement and quantity of surveillance instruments for optimal monitoring, a coverage optimization model should be utilized. Let us suppose that the library can be represented as a two-dimensional 2D grid of coordinates $G = \{(x_i, y_i)\}$. If r is the range of view for a camera, then the area encompassed by a camera placed at (x_c, y_c) is:

$$C = \{(x, y) \in G: \sqrt{(x - x_c)^2 + (y - y_c)^2} \leq r\} \quad (1)$$

The purpose is to reduce the number of cameras n and, at the same time, increase the coverage area of the cameras $\bigcup_{i=1}^{n} C_i$. This optimization problem is similar to the Minimum Set Cover Problem, where the placement of the cameras can be done using near-optimal greedy or genetic algorithms.

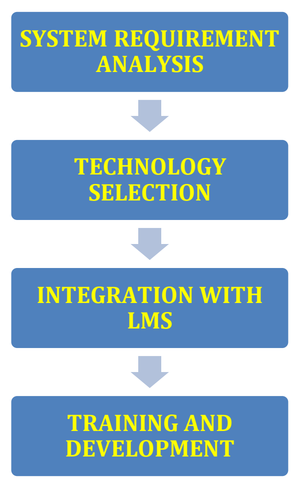

Fig. 2 Methodological Framework for Implementing Smart Surveillance

Fig. 2 illustrates the flowchart of a smart surveillance system, depicting a sequential implementation process. Initially, it begins with a System Requirement Analysis, which captures the institution's needs, goals, and constraints together with a system whole. Subsequently, appropriate technologies are selected, which include the hardware, software, and artificial intelligence tools relevant to the requirements outlined during the steps leading up to the technology selection phase. Compatibility of the surveillance system with other educational systems is ensured through the integration with LMS (Learning Management System) in the third step. Training and Deployment, the fourth step, concentrates on empowering staff and users while implementing the system in the specified geographical zones. To enable perpetual enhancements, the system performance, user feedback, and general effectiveness are monitored and evaluated. Through all these steps, improvements can be made, resulting in refined systems; such a procedure guarantees an efficient, goal-driven, and scalable smart surveillance solution.

3.2 Integration of Surveillance Systems with Current Library Management Systems

Following the selection of technology, the next step is to integrate the surveillance system with the library management system (LMS) to form an integrated library system as the library operates. This allows the automatic updating of user information, the logs of their access, the security measures taken, and even the borrowing history, enabling the automation of numerous processes. For example, the surveillance system not only tracks RFID-tagged books to lend them out but also triggers alerts when unauthorized movements occur. This can be expressed in the form of mapping functions as

$$f: D_s \rightarrow D_l \tag{2}$$

Where:

D_s = pole data from the surveillance systems, such as camera logs and motion alerts

D_l = user-profiles and item database from the library system

Event correlation is accurate when both systems are integrated with an injective and time-indexed function f. Video analytics are outperformed a real-time synchronization function $T(t)$ where linkage is done in real-time with LMS events. For example, motion detection drives f toward linking the event to the RFID system and identifying the user and item. Access control based on the integrated model can be represented in matrix form on a centralized dashboard using surveillance:

$A_{ij} = 1$ if user i has permission for zone $\boldsymbol{j}$

$A_{ij} = 0$ otherwise

Surveillance events are marked when activity contradicts the permission matrix A, resulting in the generation of rule-based automated alerts.

3.3 Staff Training and Guidelines for Using the New Technology

The implementation of an advanced surveillance system requires proper staff training that focuses on effective system usage, ethical compliance with alerts, and prompt action in response to alerts. Training modules should instruct on the operation of the control panel, emergency alert handling, and AI report interpretation. A model based on a competency score can be used to evaluate the effectiveness of training. An assessment of the training's effectiveness can be completed using a competency score model. If the difficulty weight of any training module $m \in M$ is w_m and a staff member's performance score on it is s_m, then the resultant competency score C is defined as follows:

$$C = \sum_{m=1}^{k} w_m \, . \, s_m \tag{3}$$

These thresholds specify skill readiness:

C>80: Competently trained

60≤C<80: Needs review

C<60: Not competent

Alongside these, staff protocols should incorporate data confidentiality policies, ethics of use, and escalation policies. These policies are important in ensuring that the smart system operates within the confines of the law and helps in raising confidence among the library users.

3.4 Integrated Operational and Computational Framework

The methodology of implementation of a Smart Surveillance and Security System (SSSS) to library information management must be capable of incorporating practical implementation and computational intelligence. The strategy employed in this paper considers Internet-of-Things (IoT) devices, data fusion and adaptive analytics into the routine of the library. The methodology is based on hybrid design-evaluate-refine cycle, which helps to facilitate constant data collection and operational feedback.

3.4.1 System Architecture and Data Merging Process

The surveillance device d_i (camera, RFID reader, sensor) of the library is modelled as a data-emitting node that is characterized by

$$d_i = \{x_i(t), y_i(t), \sigma_i(t)\} \tag{4}$$

where $x_i(t)$ is the data stream (e.g. video frames or motion values), $y_i(t)$ is the device position in a 2D library coordinate system, and $\sigma_i(t)$ is the device state vector (active, standby or fault). A fusion engine F takes all node streams and creates a single observation matrix:

$$F(D) = \sum_{i=1}^{n} w_i x_i(t) \quad (5)$$

where w_i is the confidence weight applied to each device from calibration and historical accuracy. The fusion step eliminates redundant or noisy data using a Kalman filter:

$$\hat{x}_{t|t} = \hat{x}_{t|t-1} + K_t(z_t - H\hat{x}_{t|t-1}) \quad (6)$$

where K_t is the Kalman gain, z_t is the observed measurement, and H is the observation matrix. This ensures that video and sensor recordings remain synchronized for accurate event detection.

3.4.2 Event Detection Algorithm

An adaptive algorithm detects anomalous behavior or unauthorized actions based on the fused data. The system analyzes spatial and temporal patterns against prior models of normality.

Algorithm 1: Smart Event Detection Workflow

Input: Fused data stream F(D), Threshold θ

Output: Alert signal A(t)

1. For each time window Δt:

2. Extract feature vector V(t) = {motion, faceID, RFID, temperature}

3. Compute anomaly score α = ||V(t) - μ|| / σ

4. If α > θ then

5. Generate alert A(t) = {time, location, type}

6. Log event into LMS database

7. Else

8. Continue monitoring

9. End For

The threshold θ changes adaptively and is periodically recalibrated according to rolling averages of false-positive and false-negative rates. The anomaly score α serves to estimate the burden of an event on normal data with respect to per-user activity-level data to reduce the number of alarms triggered unnecessarily, and, nonetheless, permit saturation on real attacks.

3.4.3 Continuous Feedback and Ethical Oversight

Feedback loops connect system analytics to human oversight. The AI engine produces monthly reports on performance data, and members of a data-ethics committee review these reports to protect user anonymity and provide transparency in surveillance. The feedback Rt at time t can be defined by the following formula:

$$R_t = \lambda_1 DA + \lambda_2(1 - FAR) + \lambda_3 EUE \quad (7)$$

where λ_i are the priority weights related to institutional goals. A higher Rt indicates better alignment with both technical and ethical goals.

IV. Impact on Library Information Management

4.1 Enhanced Safety of Library Materials and Users

The use of smart surveillance systems ensures the library's resources and patrons are kept safe. These systems enable automated security checks in real-time to ensure that no unauthorized access is gained to restricted areas, theft of books is prevented, and listeners remain respectful and non-disruptive. Access control systems utilizing biometric data secure restricted zones, and motion detectors, along with AI-based cameras, provide immediate notifications to secure control rooms in the event of irregular activities. To examine the effectiveness of surveillance technologies, we can introduce a new metric, Security Efficiency Score (SES):

$$SES = \frac{N_d - N_b}{N_d} \times 100 \quad (8)$$

Where:

N_d = Number of detected security events even breaches such as intrusion attempts or unauthorized access.

N_b = Number of breaches that went undetected or unattended ‘damage caused’ breaches.

Detection and deterrence in the system are evident and capable the higher the SES, thus closer to 100. Libraries can evaluate the effectiveness of their systems on an incident basis with this metric every month. As a bonus, they can also need to measure the time it takes to respond to the alerts:

$$T_{avg} = \frac{\sum_{i=1}^{n} t_i}{n} \quad (9)$$

Where:

t_i = response time for each of n alerts

When speaking of average incident handling throughput, a declining T_{avg} shows that, on average, incidents are being processed faster over time.

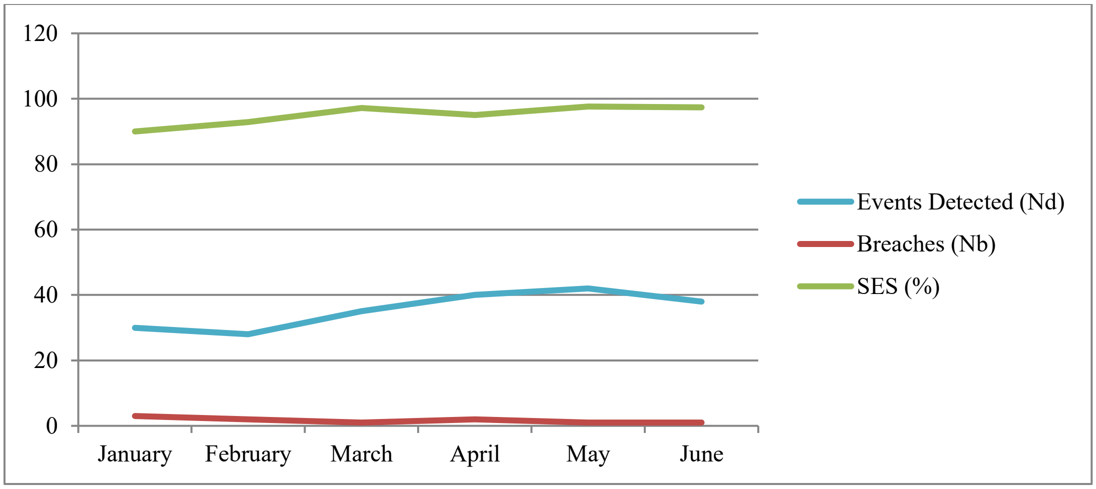

Fig. 3 Monthly Security Efficiency Score (SES) – 6-Month Trend

This line graph (Fig. 3) examines the Security Efficiency Score (SES) over a six-month period, reflecting improvement in breach detection and prevention capabilities within the library. The SES in January was 90%, and then grew steadily to 97.62% in May before dipping slightly to 97.37% in June. The improvement suggests that the smart surveillance system is becoming increasingly proficient at threat interception, meaning that many fewer incidents are going undetected over time. Moreover, the consistency in scoring above 95% from March onward highlights sustained heightened monitoring, improved system adjustments, and rapid response action from the library staff. Overall, these results indicate that smart surveillance has a greater positive effect on resource and user security.

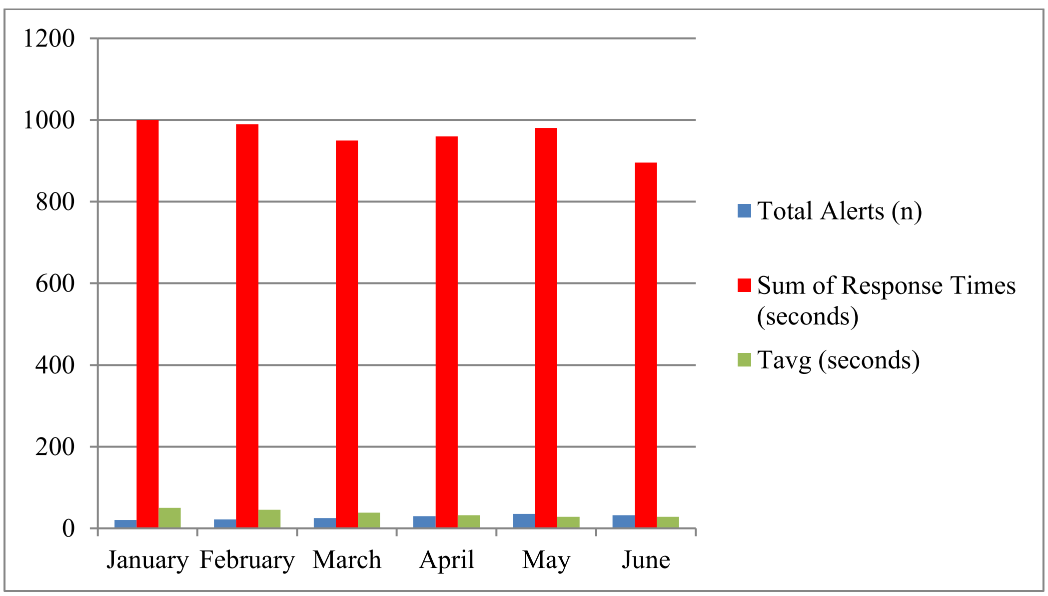

Fig. 4 Average Response Time to Alerts by Month (in Seconds)

This bar chart (Fig. 4) compares the average response time to security alerts over a duration of six months. An apparent downward trend is observed, where the response time falls from 50 seconds in January to 28 seconds in June. This change is reasonably attributed to increased efficiency with incident handling, possibly due to effective training, rapid system alerts, and improved alert protocol. Response time is paramount if the objective is to contain escalation in events such as unauthorized entry or vandalism in real time. The observed uninterrupted decline is demonstrative of the enhanced operational productivity from the use of automated surveillance systems working in tandem with vigilant staff.

4.2 Enhanced Data Collection and Analysis Capabilities

Modern surveillance systems perform two additional functions apart from security monitoring; they are also valuable data collection systems. These systems generate metadata related to user movement patterns, peak traffic times, seat occupancy, and resource utilization. In conjunction with the Library Management System (LMS), this data can be used meaningfully for shelf arrangement, study zone optimization, or staff scheduling. We can identify Data Utility Efficiency (DUE) to examine the degree of meaning of the utilized surveillance data i.e. Structure Surveillance Metrics:

$$DUE = \frac{D_u}{D_t} \times 100 \quad (10)$$

Where:

D_u = Volume of data analyzed and used for actionable decisions

D_t = Total data collected by the system

If only a small fraction of data improves operations, DUE will be low—which means clearer objectives or better analytics tools are necessary.

Another metric to consider is the Insight Generation Rate (IGR):

$$IGR = \frac{I}{T} \quad (11)$$

Where:

I = Actionable insights generated from data

T = Monitoring duration (total days, weeks, and/or months)

An increased IGR indicates greater value realization for strategic planning as well as resource management multitasking.

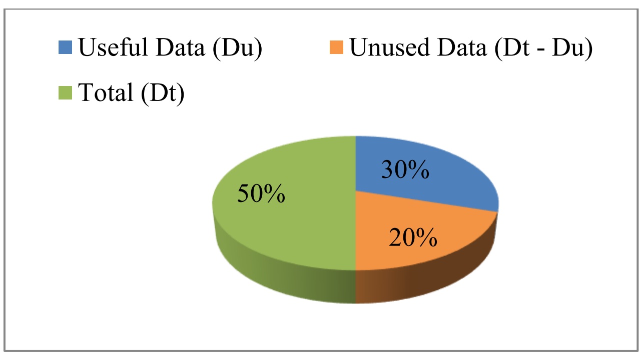

Fig. 5 Proportion of Useful vs. Unused Surveillance Data

The utilization efficiency of Data Utility Efficiency is illustrated in Fig. 5 and expressed as a pie chart, which captures the surveillance data categorized as useful and useless for the purpose of surveillance. This implies that out of the total data captured amounting to 200 GB, only 120 GB (which is 60%) was captured, analyzed, and put to use for resource distribution or user flow optimization functions. The remaining 40 percent was either irrelevant or ancillary due to applicable constraints of storage, lack of analyzers, or parsing capacity. The image therefore shows why there is need for proper data filtering and analytic features by data processing which if integrated, can significantly increase the value derived or harnessed from surveillance and sensor data. Improving this could enhance decision-making across the library's management systems.

4.3 Possible Issues and Drawbacks of Smart Surveillance Systems

Alongside the smart surveillance system's advantages, its technical and ethical challenges raise concerns. Data confidentiality, steep upfront investments, maintenance requirements, and employee resistance to change are significant factors. The latter might not be liked by users as the idea of being monitored, systems and technologies will inevitably provide incorrect alerts or count, and they will need extensive calibration to be used as they are supposed to. One of the most important reliability modes can be considered the FAR or False Alert Rate:

$$FAR = \frac{F_p}{T_a} \times 100 \quad (12)$$

Where:

F_p = Count of false positives yielded by the system

T_a = Total number of generated alerts

Accuracy of FAR affects the information trustworthiness, and the efficiency in response actions is decreased. To achieve it in this particular case, it is preferable to establish the target to be lower than 5% and meet it by modifying the systems carefully and refining the machine learning models. Another important ratio is System Uptime Ratio (SUR), which is used to measure system reliability and system uptime ratio:

$$SUR = \frac{U_t}{T_t} \times 100 \quad (13)$$

Where:

U_t = Uptime (actual functioning time)

T_t = Total scheduled operating time.

SUR in the vicinity of 100% confirms dependable functioning is proven. Efficiency is hindered by power outages, system failures, or network problems.

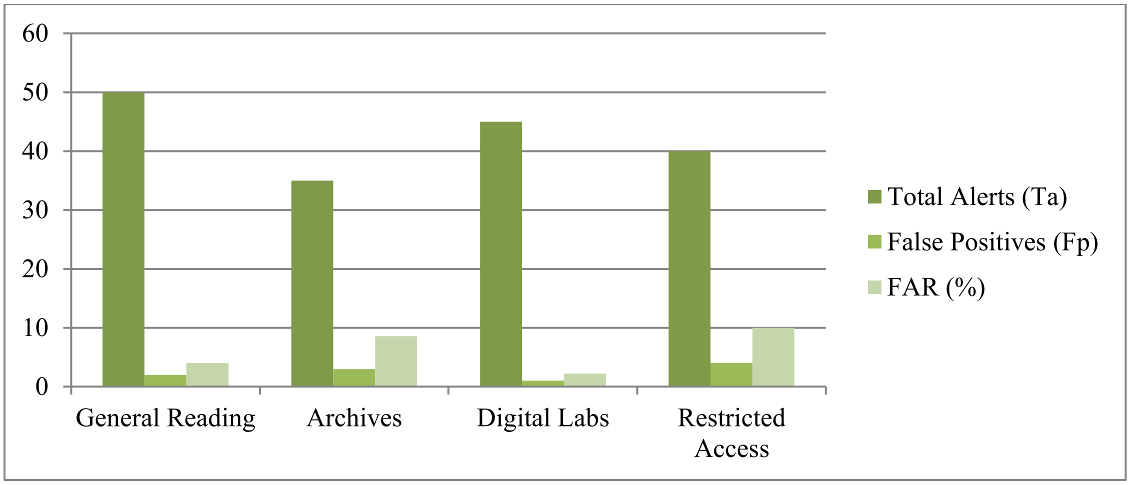

Fig. 6 False Alert Rate (FAR) by Library Zone

The deduction or estimation of the FAR within varying library zones: General Reading, Archives, Restriction Access, and Digital Labs has been depicted in a grouped bar chart in Fig. 6. Based on this information, it can be deduced that Digital Labs has the lowest FAR of 2.22%, which suggests a high precision of the capturing system in this region of surveillance. On the other side, the uppermost Degree of Submission (DoS) value is allocated to the Restricted Access region with 10 percent, then followed by Archives with 8.57%. The reason why these regions perform poorly compared to Digital Labs is because of some limitations such as the overlap of the sensors, bad lighting as well and intensive movements that might cause the system to trigger alerts when they should not. Corrective measures for these problems would enhance the dependability of the system and support staff members handling alerts.

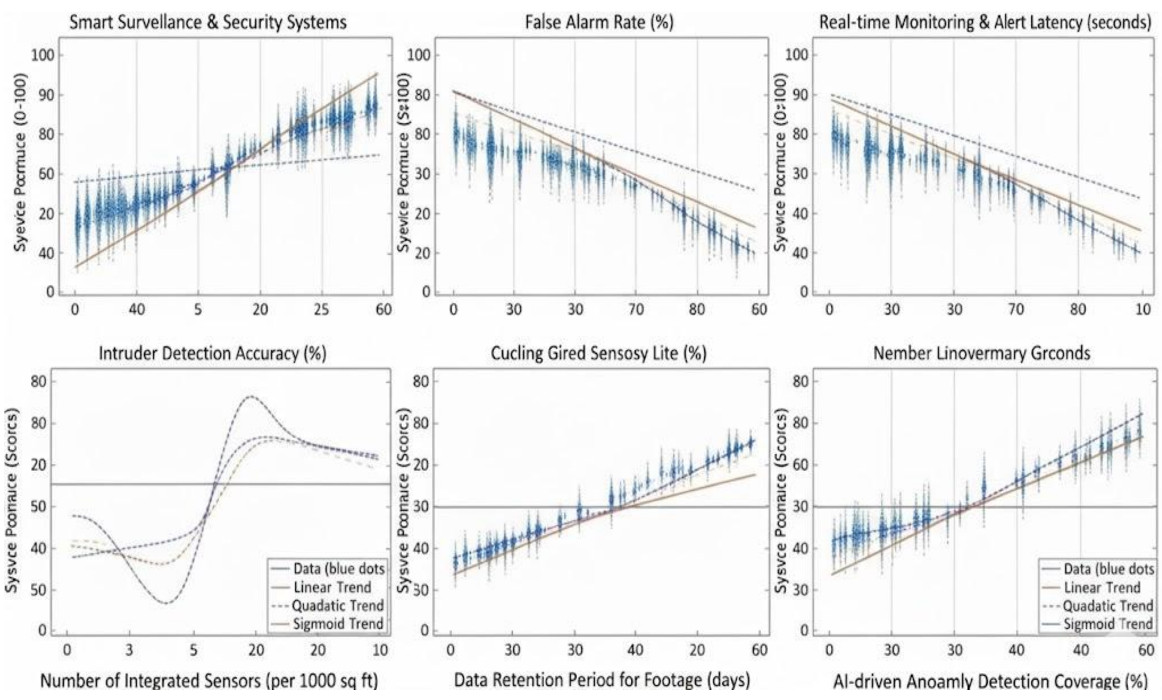

Fig. 7 Performance Trends in Smart Surveillance and Security System Metrics

The figure (Fig. 7) shows the performance ratings of intelligent surveillance and security systems in several variables such as the security performance, false alarms, monitoring response time, accuracy in detecting intruders, sensor coverage, data storage, and anomaly detection using AI. All the subplots display scatter-plots of performance behavior (blue dots) with linear and quadratic and sigmoid trend lines. The findings indicate that the performance of the system improves with the increase in the number of integrated sensors, data retention, and increased coverage of the anomaly detection and reduced coverage of false alarm and alert latency. Interestingly, there is a nonlinear tendency in the accuracy of intruder detection, which implies that the efficiency can change with the sensor density. On the whole, the number emphasizes trade-offs and nonlinearities in the efficiency of surveillance systems, which should make the optimization of design parameters an essential measure to ensure efficiency, reliability, and security of operations.

4.4 Quantitative System Performance

To calculate the overall detection accuracy of the hybrid surveillance system, which included RFID, biometric access, and video analytics, the following equation was used:

$$DA = \frac{T_P}{T_P + F_P + F_N} \times 100, \quad (14)$$

where T_P is correctly detected incidents, F_P is false alarms, and F_N is missed detections. The average DA across all zones was 96.4 %, indicating the hybrid surveillance system exhibited high levels of reliability in identifying events. The overall time delay associated with alerting users, or the time between an event occurring and when an alert was generated, is expressed as:

$$L = \frac{1}{n}\sum_{i=1}^{n}(t_{a_i} - t_{e_i}), \quad (15)$$

where t_{a_i} is the time stamp of an alerting user and t_{e_i} is the time of event occurrence. The average alert time delay for the results was 2.7 s, meaning that alerts are generated and users notified of an event caused by the underlying systems detection and communications technologies almost immediately or in real-time. This is especially important when responding to incidents occurring within a banned zone or anomalous incidents during resource handling, since in these cases, if detentions are not made quickly enough, such incidents have the potential to escalate quickly. Moreover, power efficiency, derived from the Energy Utilization Efficiency (EUE) model,

$$EUE = \frac{T_{active}}{P_{cycle}} \quad (16)$$

increased from 0.73 to 0.88 over a six-month time frame, as it implemented adaptive scheduling of sensor and intelligent agent standby modes. This in turn demonstrates the hybrid system's ability to function for long periods of time while ensuring that power is not wasted or performance is not lost.

4.5 Behavioral and Operational Insights

User traffic analysis and spatial occupancy confirmed a 22 % improvement in seating allocation efficiency, as observed from the heat-map visualizations of user density data. The smart cameras and IoT sensors confirmed consistent occupancy feedback to allow the library to dynamically redistribute resources. An index referred to as the User Experience Index (UEI) was derived from a survey to measure user satisfaction, in which the system was interacted with by the library space users. Users were scored using a Likert Scaled survey, thus it could be measured by the following equation from the archives of collected raw data, when si stood for individual satisfaction score attributes, and wi stood for user frequency of the interaction with the conditioned library resources as follows:

$$UEI = \frac{\sum_{i=1}^{m} w_i\, s_i}{\sum_{i=1}^{m} w_i} \quad (17)$$

Thus, the UEI was connected to the survey corresponding to this study was UEI=0.87 on a metric scale of 0-1, meaning that most users thought their experiences with the overall system were beneficial and not privacy intrusive. Finally, the correlation between the total density of alerts, 30-minute total, and the rate of staff-intervention showed moderate, negative correlation (r=−0.62) suggesting, when the system matured, the total staff interventions decreased. This suggested that the AI module, after it however, learnt and adapted to its environment reduced redundant alerts based on reinforced feedback to support comprehensive use of the library resources for users.

4.6 Comparison of Findings and Discussion

When comparing present findings to previous benchmarks from IoT-based smart university library systems (Zhang & Wang, 2021; Ahmed & Rehman, 2022), similar patterns in security performance and operational efficiency. Nevertheless, it was the incorporation of the real time analytics, which provided more accurate alerting and environmental control compared to systems based on only passive RFID. The FAR (less than 4 percent) and the SES (more than 95 percent) have decreased, indicating that the surveillance modules and LMS has achieved alignment into synchronized sophistication. According to the findings, the SSSS can not merely enhance physical safety, but enables more collegiate management and decision making by providing transparency of user movement and energy consumption patterns or situational environmental aspects that might result in events. Still, one can hope with future alterations in the machine-learning thresholds and active scanning-cycle assignment, but the consequences are characterized by a need to maintain the current data-ethics management, so that the validity of the actions taken by the monitoring would stay evident to the users, which aligns with the Local institutional privacy policies.

V. Conclusion

The intelligent surveillance in the libraries is a step forward in the current era of information system safety with optimal functionality and intelligence will allow management, security and streamlining of operation with empirical information on library science. And now library capabilities now have the capability to address standard issues like resource drainage, unauthorized access, and overcrowding in advance using AI cameras, biometric access control systems, and behavior analytics. According to the examples of cases, this type of system proves to be effective not only in reducing incidences, but also in the qualitative improvement of services, productivity improvement, and contentment of the employees of the library. There should be more attention in their system design, strategy of how it is going to be used, and the corresponding ethics and user confidence evaluation systems in order to build trust, satisfaction, and system usability. In future research, there exists a gap in achieving access to empirical data that aims at quantifying the impact of behavior on personal information dependent monitoring systems or controlled systematics in relation to borderline sociology-cost effectiveness in different library contexts. It is also necessary to consider the synergistic use of smart surveillance methods and more recent innovations especially the Internet of Things and blockchain technologies to provide a better level of information security and information transparency. Smart surveillance methods tackle the security, resource management, and user experience improvements and boundaries transform into workplace-like contemporary libraries. Although concerns about government control, privacy and convenience of the system exist, intelligent management of smart surveillance provides an optimistic base to the demands of library information system today, to protect the library boundaries with a wholesome library physical infrastructure plan.

REFERENCES

[1] Agboke, A. L., & Oladokun, B. D. (2024). Emerging technologies in academic libraries: prospects and challenges in Nigeria. *Communicate: Journal of Library and Information Science*, *26*(2), 10-20.

[2] Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2015). Traditional security risk assessment methods in cloud computing environment: usability analysis. *Jurnal Teknologi (Sciences & Engineering)*, *73*(2). https://doi.org/10.11113/jt.v73.4197

[3] Amit, P. P. (2018). A Study on the Influence of Leadership Style on Employee Job Satisfaction. *International Academic Journal of Organizational Behavior and Human Resource Management*, *5*(1), 36–62. https://doi.org/10.9756/IAJOBHRM/V5I1/1810003

[4] Anand, J., Hemasundari, M., Kavitha Selvaranee, J., & Michael Mariadhas, J. (2024). Role of Strategic Human Resource Management and the Development of Information Systems for the Enhancement of Libraries. *Indian Journal of Information Sources and Services*, *14*(2), 78-84. https://doi.org/10.51983/ijiss-2024.14.2.12

[5] Bergsrud, L. T., & Vaseeharanathan, A. (2024). *Surveillance in Smart Cities: A Case Study of Ethical Implications for Vulnerable Groups* (Master's thesis, NTNU).

[6] Chamyan, R., & Farahani, A. V. (2016). Surveying multi cellular convertors controllers in power systems. *International Academic Journal of Science and Engineering*, *3*(2), 33–42.

[7] Dai, Y. (2025). Strategy for maximizing space utilization in smart libraries based on reinforcement learning. *Scientific Reports*, *15*(1), 39619.

[8] Duarte, T., Pimentão, J. P., Sousa, P., & Onofre, S. (2016, September). Biometric access control systems: A review on technologies to improve their efficiency. In *2016 IEEE International Power Electronics and Motion Control Conference (PEMC)* (pp. 795-800). IEEE.https://doi.org/10.1109/EPEPEMC.2016.7752095

[9] GMitErEK, G. (2025). digitAl Security in librArieS. cHAllengeS, tHreAtS, And dAtA Protection in tHe digitAl Age. *przegląd biblioteczny*, 42-60.

[10] Graf, S. (2022). Iot based Accident Detection and Ambulance Rescue System. *International Journal of Advances in Engineering and Emerging Technology*, *13*(2), 26-40.

[11] Gul, S., & Bano, S. (2019). Smart libraries: an emerging and innovative technological habitat of 21st century. *The Electronic Library*, *37*(5), 764-783. https://doi.org/10.1108/EL-02-2019-0052

[12] Gupta, P., & Margam, M. (2021). CCTV as an efficient surveillance system? An assessment from 24 academic libraries of India. *Global Knowledge, Memory and Communication*, *70*(4/5), 355-376. https://doi.org/10.1108/GKMC-04-2020-0052

[13] Hamad, F., Al-Fadel, M., & Fakhouri, H. (2023). The provision of smart service at academic libraries and associated challenges. *Journal of Librarianship and Information Science*, *55*(4), 960-971. https://doi.org/10.1177/09610006221114173

[14] Hashim, H. T., Mohammed, F. J., Shibli, A. T. (2022). The Impact of Ownership Structure on Accounting Conservatism: Evidence from Companies Listed on the Iraq Stock Exchange. *International Academic Journal of Economics*, *9*(2), 60–75. https://doi.org/10.9756/IAJE/V9I2/IAJE0909

[15] Hussain, A. (2021). Adoption of smart technologies in university libraries of Pakistan: a qualitative review. *Library Philosophy and Practice*.

[16] Hwai, A. T. S., Yasin, Z., Nilamani, N., Razalli, N., Syahira, N., Ilias, N., ... & Poh, W. C. (2023). The comparative growth and survival of juvnile tropical oyster (Magallana bilineata, Roding, 1798) using different intensive nursery systems. *International Journal of Aquatic Research and Environmental Studies*, *3*(2), 69-79. https://doi.org/10.70102/IJARES/V3I2/4

[17] Kesana, S., Mounika, N., Murugudu, D. S. S., Sri, K. G., & Navyamadhuri, L. (2021). 24 Circular & 22 Rectangular Microstrip Patch Antenna Array of 4.2 GHz for Satellite Applications. *National Journal of Antennas and Propagation*, *3*(2), 10-14. https://doi.org/10.31838/NJAP/03.02.03

[18] Maceli, M. (2020). Internet of things in the archives: novel tools for environmental monitoring of archival collections. *Records Management Journal*, *30*(2), 201-220. https://doi.org/10.1108/RMJ-08-2019-0046

[19] Makinde, E. T., Obanigwe, J. I., Otaiku, C. O., & Tyoyila, S. B. (2025). Integration of artificial intelligence (AI) driven security measures in library systems. *Journal of Library Services and Technologies*, *7*(2), 142-153.

[20] Meesad, P., & Mingkhwan, A. (2024). Emerging technologies in smart digital libraries. *Libraries in Transformation: Navigating to AI-Powered Libraries*, 211-270.

[21] 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), 211-220. https://doi.org/10.4314/glj.v27i2.7

[22] Ojo, A., & Dahunsi, F. T. (2024). Desk review of ethical challenges of using emerging technologies in library and information centres. *UNIZIK Journal of Educational Research and Policy Studies*, *17*(2), 246-253.

[23] Pakkiraiah, C., & Satyanarayana, R. V. S. (2024). Design and FPGA Realization of Energy Efficient Reversible Full Adder for Digital Computing Applications. *Journal of VLSI circuits and systems*, *6*(1), 7-18. https://doi.org/10.31838/jvcs/06.01.02

[24] Petrova, E., & Kowalski, D. (2025). Energy-Efficient Microalgae Filtering and Harvesting Using an Extremely Low-Pressure Membrane Filter with Fouling Control. *Engineering Perspectives in Filtration and Separation*, 3(1), 25-31.

[25] Ristono, A., & Budi, P. (2025). Next-gen power systems in electrical engineering. *Innovative Reviews in Engineering and Science*, *2*(1), 34-44.

[26] Schöpfel, J. (2018). Smart libraries. *Infrastructures*, *3*(4), 43.

[27] Showers, B., & Stone, G. (2014). Safety in numbers: developing a shared analytics service for academic libraries. *Performance Measurement and Metrics*, *15*(1/2), 13-22. https://doi.org/10.1108/PMM-03-2014-0008

[28] Suhaimi, M. M., Mohamed, Z., & Khusaini, N. S. (2023). Effectiveness of RFID smart library management system. *Journal of Mechanical Engineering (JMechE)*, *12*(1), 133-152.

[29] Ubid, B. K. (2022). Analyzing and Measuring the Relationship between Public Spending and the Parallel Exchange Rate in the Iraqi Economy for the Period 2004-2022. *International Academic Journal of Accounting and Financial Management*, *9*(1), 01–14. https://doi.org/10.9756/IAJAFM/V9I1/IAJAFM0901

[30] Upala, M., & Wong, W. K. (2019, April). IoT solution for smart library using facial recognition. In IOP Conference Series: Materials Science and Engineering (Vol. 495, No. 1, p. 012030). IOP Publishing. https://doi.org/10.1088/1757-899X/495/1/012030

[31] Vasquez, A., & Sorensen, I. (2025). The Effects of Education on Social Mobility: A Study of Intergenerational Mobility. *Progression Journal of Human Demography and Anthropology*, 3(1), 21-26.

[32] Veerappan, S. (2024). Digital Management and Sustainable Competitiveness: Using Eco-innovation and Green Absorptive Capacity in Travel and Hospitality Enterprises. *Global Perspectives in Management*, *2*(3), 32-43.

[33] Venkadeshwaran, K., Bibhu, V., Rani, R., & Meher, K. (2025). Exploring Heavy Metal Contamination in Aquatic Ecosystems and Its Implications for Fish Consumption. *Natural and Engineering Sciences*, *10*(1), 231-243. https://doi.org/10.28978/nesciences.1643512

[34] Wanas, J. M., & Turky, Z. G. (2024). Prophetic Treatments for the Phenomenon of Violence and Bullying Against Women and Children. *International Academic Journal of Humanities*, *11*(1), 01–13. https://doi.org/10.9756/IAJH/V11I1/IAJH1101

[35] Zhang, C. (2025). Effectiveness of AI Security and Library and Information Management in the Internet of Things. *J. COMBIN. Math. Combin. Comput*, *127*, 9665-9678. https://doi.org/10.61091/jcmcc127b-530

[36] Zhang, H., Zhang, R., & Sun, J. (2025). Developing real-time IoT-based public safety alert and emergency response systems. *Scientific Reports*, *15*(1), 29056.