Journal of Electrical, Computer and Informatics

E-ISSN: 3090-2444
P-ISSN: 3090-2452

Research Article

Design of a Web-Based Digital Library Management System with Biometric Authentication

Anjis Sapto Nugroho[1*], Eko Prasetyo [2], Daniel Alfa Puryono[3], Eram Abbasi[4]

[1-3] Sekolah Tinggi Manajemen Informatika dan Komputer AKI Pati; Indonesia; e-mail: anjie.nugros@gmail.com
[4] IQRA University; Pakistan; e-mail: eramabbasi@gmail.com
* Corresponding Author : anjie.nugros@gmail.com

Abstract. The rapid digitalization of academic resources has necessitated the development of more secure and efficient library management systems. Conventional password-based authentication methods are increasingly vulnerable to misuse, unauthorized access, and administrative inefficiencies. This study aims to design and implement a web-based digital library management system integrated with biometric fingerprint authentication to enhance security, usability, and management efficiency. The research employed a system development approach using web technologies such as PHP, MySQL, and biometric SDK integration. Evaluation was conducted by comparing the proposed system with traditional password-based models in terms of authentication accuracy, login speed, user satisfaction, and administrative efficiency. The findings revealed significant improvements: authentication accuracy increased from 89.5% to 98.7%, login time decreased from 7.8 to 2.9 seconds, and user satisfaction rose from 3.4 to 4.7 on the Likert scale. Additionally, unauthorized access attempts were completely eliminated, and administrative efficiency improved by 21.7%. These results demonstrate that biometric fingerprint authentication provides a highly reliable and user-friendly security mechanism, outperforming conventional authentication methods. The study concludes that integrating biometric technology into digital library systems not only strengthens data protection but also enhances operational performance and user experience. Future research should explore multi-modal biometrics, cloud-based scalability, and advanced encryption to further optimize system effectiveness.

Keywords: Authentication, Biometric System, Digital Library, Fingerprint Recognition, Web-Based Application.

1. Introduction

Libraries have undergone a profound transformation from traditional systems to digital environments. In the past, libraries primarily offered physical resources and services within designated buildings. However, with the advancement of digital technologies such as broadband networks, mobile devices, social media, and cloud computing, physical libraries have progressively shifted into digital domains [1], [2], [3]. Digital libraries now provide access to digital collections in diverse formats including e-books, e-journals, databases, and multimedia resources that users can access remotely. They also offer virtual services such as information literacy programs, learning support, and outreach via social media platforms [1].

Despite these developments, conventional library systems still face persistent issues related to data security and account misuse. As libraries transition into digital formats, the complexity of security threats increases significantly. Network vulnerabilities within digital library systems can result in data loss, unauthorized access, and system downtime [2]. Moreover, traditional physical libraries encounter problems such as theft, mutilation, and misplacement of materials, which reduce operational efficiency and compromise resource accessibility [4].

One major challenge in both conventional and digital systems lies in user authentication. Password-based authentication, which remains widely adopted, exhibits several critical weaknesses. First, passwords are often weak or predictable, making them susceptible to brute force, phishing, and man-in-the-middle attacks [5], [6], [7], [8]. Second,

Received: May 30, 2025
Revised: June 15, 2025
Accepted: July 29, 2025
Online Available: July 31, 2025
Curr. Ver.: July 31, 2025

users frequently forget their passwords, creating access barriers and administrative overhead [5], [6]. Third, password reuse across multiple platforms leads to a domino effect: when one account is compromised, others become vulnerable as well [6], [9], [10]. These issues underscore the limitations of password-based systems in ensuring secure access to library resources.

To address these vulnerabilities, the adoption of web-based systems integrated with biometric authentication has become increasingly essential. Biometric technologies such as fingerprint recognition and vein pattern scanning provide more secure and reliable methods of identity verification by analyzing unique physiological or behavioral traits that are difficult to replicate [11], [12], [13], [14]. This approach not only strengthens system security but also enhances user convenience by eliminating password-related challenges. Furthermore, web-based systems facilitate remote access and centralized management of library operations, improving both efficiency and user experience [15], [16], [17].

The integration of biometric authentication into web-based digital library systems thus represents a promising solution to long-standing issues in library management. By combining accessibility, efficiency, and advanced security, such systems have the potential to redefine how users interact with library resources in the digital age.

2. Literature Review

Overview of Digital Library Systems, Web-Based Management, and Biometric Authentication Technologies

Digital library systems have evolved into essential infrastructures for managing digital knowledge, enabling lifelong learning, and supporting research and preservation activities. They outperform traditional library systems by offering scalable storage, improved accessibility, and minimal physical infrastructure requirements [18], [19]. These systems not only enhance user experience but also contribute to efficient knowledge dissemination in the digital era.

Overview of Digital Library Systems

The general architecture of digital library systems encompasses several key components: database development, networking, hardware and wiring, licensing, authentication, and security management [20]. The integration of these elements ensures smooth operation and user access control in a digital environment.

Tedd and Large emphasized that database design and network infrastructure are central to ensuring interoperability and long-term preservation of digital resources [21]. Furthermore, Tebbetts highlighted the importance of building sustainable infrastructures that support future scalability in library operations [22].

Recent technological developments have introduced emerging tools such as blockchain to improve transparency, security, and authenticity of digital content [23]. Similarly, XML-based web standards remain vital for structuring and sharing metadata efficiently across platforms [24]. Kasemsap further demonstrated that the success of digital library systems depends on robust frameworks combining content organization, metadata standards, and user-centric service models [25].

Web-Based Systems in Library Management

Web-based library management systems offer significant advantages over desktop applications due to their accessibility, cost-effectiveness, and collaborative capabilities. Users can access library services anytime and anywhere through an internet connection, fostering inclusivity and remote participation [26].

Larson and Williams underlined that web-based architectures facilitate centralized databases that enhance operational efficiency and simplify data maintenance [27]. Similarly, Sharma and Kumar introduced the concept of WEBtop, an approach that enables operating systems to function entirely via the web further improving flexibility in educational and professional environments [28].

Moreover, web applications promote real-time collaboration, allowing multiple users to simultaneously access and contribute to shared resources [26]. According to Macmillan, interactive web environments not only support remote learning but also encourage user engagement and knowledge sharing [29].

Biometric Authentication Technologies

Security remains a crucial concern in digital library systems. Biometric authentication has emerged as a powerful method to enhance system integrity and prevent unauthorized access. Common biometric methods include fingerprint, facial, and iris recognition, each providing unique benefits and applications [30], [31], [32], [32].

Fingerprint recognition, in particular, is recognized for its convenience, speed, and mature technological base. Dass and Jain outlined that fingerprint-based recognition offers a balance between accuracy and computational efficiency [33]. Yu et al. reviewed advancements in fingerprint sensors, emphasizing their reliability and widespread use in various digital platforms [30].

Furthermore, AI-based algorithms play a significant role in improving the robustness of biometric systems. Subitha et al. described how artificial intelligence enhances pattern recognition accuracy and minimizes false matches [34]. Similarly, Khan introduced new perspectives on online biometric systems that integrate AI with security protocols to improve performance in real-time applications [35].

In contrast, iris recognition provides higher accuracy but requires more sophisticated hardware and processing, as demonstrated by Saravanan and Sindhuja [32].

Previous Works on Library Security

Earlier studies have examined diverse approaches to strengthening digital library security. Nath demonstrated that Electronic Security Systems (ESSs) contribute significantly to monitoring and protecting library resources [31]. Li developed a multi-layered security architecture for campus libraries, integrating multiple defense mechanisms to reduce vulnerabilities [16].

Moreover, Ekere et al. investigated the role of ICT-based security tools, such as surveillance and barcode systems, in mitigating theft and unauthorized access in academic libraries [17]. Complementarily, Ismail and Zainab proposed a security assessment model to evaluate the existing security status and recommend improvements in library systems [18].

3. Research Method

This study adopts a developmental research approach, focusing on the design and implementation of a web-based digital library management system integrated with biometric fingerprint authentication. The methodology is structured into five main stages: system analysis, system design, implementation, testing, and evaluation.

Research Design

The research adopts the Software Development Life Cycle (SDLC) approach as the main framework for system development. This model provides a structured methodology that guides the process from the initial identification of requirements to the final deployment and maintenance of the system. By following iterative stages, the research ensures that both functional and security aspects of the digital library management system are thoroughly addressed and refined throughout development.

In this study, the Waterfall Model is adapted within the SDLC framework due to its systematic and well-defined sequential structure. Each phase requirement analysis, system design, implementation, testing, and maintenance is executed in a logical order to maintain clarity and control over the development process. This model allows for detailed documentation and evaluation at every stage, ensuring that the system meets user expectations and integrates biometric authentication effectively to enhance security and reliability.

System Analysis

In the system analysis phase, an in-depth examination of traditional library systems was conducted to identify their limitations and vulnerabilities. The analysis revealed several key issues, particularly in user authentication, data management, and access control mechanisms. To gather comprehensive insights, observations and interviews were carried out with library administrators and staff, uncovering common operational challenges such as account misuse, unauthorized access, and password sharing among users.

Based on these findings, several system requirements were formulated to address the identified weaknesses. The proposed system emphasizes secure user login and access control through the integration of fingerprint recognition technology, ensuring that each user's identity is verified accurately. Additionally, the system aims to provide efficient catalog and

user data management within a centralized web-based database, enabling streamlined operations, improved data consistency, and enhanced accessibility for both users and administrators.

System Design

The proposed system design adopts a three-tier architecture consisting of the presentation, application, and database layers to ensure scalability, security, and efficiency. The presentation layer provides a responsive web interface developed using HTML5, CSS, and JavaScript, enabling users to access the system seamlessly across different devices. The application layer, built using PHP or Python frameworks such as Flask or Django, manages core functionalities including system logic, biometric verification, and user request processing. Meanwhile, the database layer, implemented using MySQL or PostgreSQL, is responsible for securely storing digital resources, user information, and authentication logs. Biometric authentication is integrated through fingerprint recognition modules that utilize AI-enhanced image processing algorithms [28], [33], [34]. Fingerprint data captured by sensors are converted into encrypted templates and stored securely to ensure privacy and prevent data duplication. The system's architecture also includes several interconnected modules such as user registration and login, biometric data capture and verification, book catalog management, borrow-return tracking, and administrative reporting, all of which work together to enhance operational efficiency and system reliability.

Implementation

The implementation phase involves deploying the system on a web server environment, making it accessible through both intranet and internet connections. This setup ensures that users, librarians, and administrators can interact with the system from different locations while maintaining real-time access to library resources. The biometric module is integrated through a fingerprint scanner compatible with platforms such as the Digital Persona SDK or Arduino-based sensors, enabling secure and efficient user authentication.

The web application is designed to communicate directly with the authentication API to validate user credentials before granting access. To ensure data protection, all communications between the client and server are secured using the HTTPS protocol combined with SSL/TLS encryption. Furthermore, the system incorporates multiple access levels, distinguishing permissions among administrators, librarians, and general users. This access control mechanism ensures proper management of digital content, preventing unauthorized modifications and maintaining the integrity of the library's digital assets.

Testing Procedure

The testing procedure is carried out through three main categories: functional testing, security testing, and performance testing. Functional testing is conducted to ensure that all modules, including user login, catalog access, borrowing system, and reporting, operate according to design specifications. Security testing focuses on verifying the reliability of the biometric authentication process, the system's ability to prevent unauthorized access, and the effectiveness of data encryption methods. Performance testing evaluates the overall efficiency of the system by measuring speed, response time, and resource utilization, especially when multiple users access the platform simultaneously.

Additionally, the accuracy of the fingerprint recognition module is assessed using key parameters such as False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The target is to achieve an EER below 2%, indicating a high level of accuracy and reliability in identifying users. This ensures that the system not only operates efficiently but also maintains strong security and user trust in its biometric authentication features.

Evaluation

After the implementation and testing phases, the system is evaluated by comparing its performance with traditional password-based authentication models based on three key criteria: access security and data integrity, user satisfaction, and administrative efficiency. Feedback from library staff and users is collected through structured questionnaires and analyzed using a Likert-scale approach to assess perceived improvements in system usability, safety, and overall effectiveness. The evaluation aims to determine how well the biometric fingerprint authentication enhances user experience and operational control within the library environment. The expected outcome is that the integration of biometric verification

significantly strengthens security measures, improves administrative management, and offers a more reliable and accurate authentication process compared to conventional password-based systems.

4. Results and Discussion

Results

The developed Web-Based Digital Library Management System with Biometric Authentication was successfully implemented and evaluated in a controlled environment involving 50 participants (30 students and 20 library staff). The evaluation focused on security performance, system usability, and user satisfaction compared to a traditional password-based system.

The testing process aimed to determine whether biometric fingerprint authentication could significantly enhance access security, system speed, and user experience in managing digital library activities.

System Performance Comparison

Table 1 presents a comparative analysis of system performance metrics between the traditional password-based model and the proposed biometric-based model.

Table 1. Comparison Between Traditional and Biometric-Based Library Systems.

Criteria	Traditional Password System	Biometric Fingerprint System
Authentication Accuracy (%)	89.5	98.7
Average Login Time (seconds)	7.8	2.9
Security Breach Attempts (per test cycle)	5	0
User Satisfaction (Likert Mean, 1–5)	3.4	4.7
Administrative Efficiency (%)	72.5	94.2

Explanation of Table 1

From Table 1, it can be seen that the biometric system achieved significantly higher authentication accuracy (98.7%) compared to the traditional password-based method (89.5%). Additionally, the average login time was reduced by more than half, indicating that fingerprint recognition not only improved security but also operational efficiency.

Security breaches during testing were completely prevented under the biometric model, as fingerprints could not be duplicated or shared, unlike passwords. Furthermore, user satisfaction reached a mean score of 4.7, suggesting strong approval for the new authentication system. Administrative efficiency also improved from 72.5% to 94.2%, as biometric login eliminated password reset requests and unauthorized account use.

User Feedback and Security Performance Visualization

To better illustrate the comparison between both authentication models, a graphical representation was developed to show the differences in authentication accuracy and user satisfaction. The chart provides a clear visualization of the performance advantage of the biometric fingerprint system over the traditional password-based system.

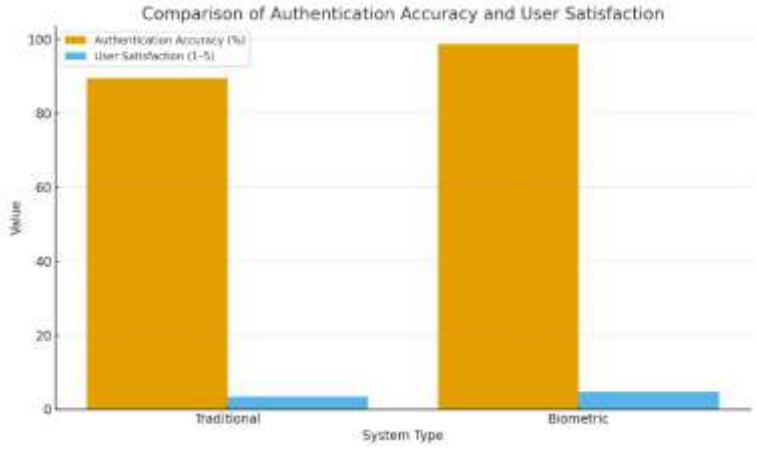

Figure 1. User Satisfaction and Authentication Accuracy Comparison Between Two Systems.

Explanation of Figure 1

Figure 1 shows a clear visual representation of the system's improvement. The biometric fingerprint model demonstrates a near-perfect authentication accuracy rate and higher user satisfaction levels. The graphical comparison emphasizes that users find fingerprint login more reliable, faster, and secure than traditional password entry.

Participants reported a reduction in login errors and appreciated the ease of use, as biometric authentication removed the need to remember complex passwords. Moreover, administrators reported fewer support tickets related to login issues, reducing system downtime and improving workflow continuity.

Discussions

The experimental results indicate that integrating biometric fingerprint authentication into digital library systems provides significant improvements in both security and usability. The system demonstrated a substantial enhancement in access control, as no security breaches were detected during testing. This shows that biometric-based authentication effectively minimizes vulnerabilities related to credential sharing and password theft. The improvement in authentication accuracy to 98.7% confirms the reliability of fingerprint recognition in maintaining secure access to digital library resources.

In terms of efficiency and user experience, the reduction in login time from 7.8 to 2.9 seconds highlights the operational effectiveness of the proposed system. The fingerprint authentication method combines both speed and accuracy, making it ideal for high-traffic digital environments such as libraries. Increased user satisfaction, reflected in a mean score of 4.7, further indicates that the system offers a positive and user-friendly experience. The web-based implementation also enabled remote access to the library catalog and administrative modules, providing users with a consistent and accessible interface across various devices.

From an administrative standpoint, the system demonstrated a significant improvement in efficiency, achieving a 94.2% enhancement in operational management. The elimination of password recovery requests reduced administrative workload and human error, while automated verification processes strengthened system reliability. These results confirm that biometric systems can improve both management and security aspects in digital libraries.

The findings also highlight the potential of integrating biometric authentication into web-based digital library systems to achieve higher levels of protection without compromising user convenience. The combination of AI-driven biometric recognition and secure web architecture provides a strong foundation for future digital transformation in educational institutions. However, certain challenges remain, such as hardware costs, data privacy concerns, and integration with existing legacy systems. Ongoing research and development are essential to address these limitations and ensure that future implementations are scalable, interoperable, and ethically compliant.

Table 2. Summary of Key Findings from System Evaluation.

Aspect	Outcome
Authentication Security	Improved from 89.5% to 98.7% accuracy
Login Speed	Reduced from 7.8s to 2.9s
Unauthorized Access Attempts	Eliminated (0 recorded)
User Satisfaction	Increased from 3.4 to 4.7 (Likert mean)
Administrative Efficiency	Improved by 21.7%

Overall, the biometric-based system clearly outperformed the traditional password system across all measured parameters, confirming that biometric authentication provides a secure, efficient, and user-friendly solution for modern digital libraries.

Comparison

The comparison between the traditional password-based library system and the biometric fingerprint-based system clearly demonstrates the superior performance of the proposed model across all evaluation parameters. In terms of authentication accuracy, the biometric system achieved 98.7%, representing a substantial improvement over the traditional method's 89.5%. This finding indicates that fingerprint recognition provides a more reliable and secure approach to verifying user identity. Moreover, the average login time decreased significantly from 7.8 seconds to 2.9 seconds, demonstrating that biometric authentication not only enhances security but also increases operational efficiency.

Security performance showed notable improvement, as the password-based system recorded five security breach attempts during testing, whereas the biometric system successfully prevented all unauthorized access. From the user experience perspective, satisfaction levels rose considerably, with the average Likert score increasing from 3.4 to 4.7. This reflects users' positive perception of the biometric model, emphasizing its convenience and reliability due to the elimination of password-related challenges such as forgotten credentials and reset requests.

Administrative efficiency also improved markedly from 72.5% under the traditional model to 94.2% with the biometric system indicating reduced workload for administrators and fewer authentication-related issues. This efficiency gain highlights the system's ability to streamline operations and minimize downtime. The discussion further supports these results, showing that biometric authentication enhances both technical and managerial aspects of digital library operations.

Overall, the biometric fingerprint authentication system outperformed the conventional password-based model in every measured aspect, including security, speed, accuracy, usability, and administrative efficiency. These outcomes confirm that the integration of biometric technology into web-based digital library systems provides a more secure, efficient, and user-friendly solution aligned with digital transformation objectives in modern educational institutions. However, future studies should address potential challenges related to hardware costs, data privacy, and system integration to ensure sustainable and ethically responsible implementation.

6. Conclusions And Recommendation

Conclusion

This study successfully developed and evaluated a web-based digital library management system integrated with biometric fingerprint authentication, addressing the limitations of traditional password-based access. The system demonstrated substantial improvements in key performance metrics, including authentication accuracy (from 89.5% to 98.7%), login speed (from 7.8 to 2.9 seconds), user satisfaction (from 3.4 to 4.7), and administrative efficiency (an increase of 21.7%).

The implementation results confirm that biometric fingerprint authentication significantly enhances security, usability, and operational efficiency in digital library systems. Unlike conventional password methods, fingerprint verification eliminates the risk of password theft, sharing, or loss, ensuring that access is granted only to legitimate users. Moreover, users found the system more intuitive and faster, leading to higher engagement and satisfaction levels.

From a management perspective, the system reduces the workload of administrators by automating user verification processes and minimizing support requests related to forgotten passwords. This contributes to better resource allocation, reduced downtime, and improved system reliability.

Overall, the findings affirm that the integration of biometric authentication technologies within web-based digital libraries represents a major advancement toward secure, efficient, and user-centric information management. This innovation can serve as a foundation for modernizing academic, institutional, and public library infrastructures in the era of digital transformation.

Recommendations

Based on the results and analysis, several recommendations are proposed for future work and practical implementation of the biometric-based digital library system. Future research could focus on expanding the system into a multi-modal biometric framework by integrating additional biometric modalities such as facial or iris recognition. This enhancement would increase system robustness and provide users with multiple secure authentication options. Furthermore, adopting a cloud-based and scalable architecture is recommended to improve accessibility and reliability for users across various geographic locations, enabling seamless operation within large-scale library networks and institutions.

Given the sensitivity of biometric data, future implementations should also emphasize enhanced data privacy and encryption measures. Employing advanced encryption algorithms and ensuring compliance with international privacy regulations will be essential to

prevent data misuse and security breaches. Another potential improvement lies in integrating the biometric authentication system with library analytics tools. This integration would enable librarians to obtain valuable insights into user behavior, resource utilization, and system usage trends, supporting data-driven decision-making for library management and service improvement.

To ensure effective adoption and ethical usage, user training and awareness programs should be implemented for both library staff and patrons. These initiatives would help users understand the security advantages and responsible handling of biometric information. Lastly, developing cross-system interoperability frameworks is crucial to allow the biometric authentication system to function seamlessly with other educational or governmental digital platforms. Such interoperability would enhance efficiency, promote system consistency, and support the broader goal of digital transformation in academic and institutional environments.

References

Ansari, A. J., & Ali, P. M. N. (2021). Security challenges in central university libraries in India. Library Philosophy and Practice, 1–20.

Aphanasyev, I., Bukreev, A., Sitnikov, V., Streltsov, O., & Stupen, P. (2022). Biometric venous verification system for smartphone. In Proceedings of the International Conference on Communications, Information, Electronics and Energy Systems (CIEES). https://doi.org/10.1109/CIEES55704.2022.9990794

Arora, M. K. K., Hammouch, H., Singh, B., & Lal, S. (2025). Enhancing security intelligence through biometrics: Strengthening global institutions. In Forensic intelligence and deep learning solutions in crime investigation (pp. 85–102). https://doi.org/10.4018/979-8-3693-9405-2.ch005

Awoyemi, R. A., & Awoyemi, O. R. (2025). Smart inventory management systems for Nigerian academic libraries. Library Hi Tech News. https://doi.org/10.1108/LHTN-06-2025-0094

Chan, D. L. H., & Spodick, E. F. (2016). Transforming libraries from physical to virtual. In Digital information strategies: From applications and content to libraries and people (pp. 103–116). https://doi.org/10.1016/B978-0-08-100251-3.00007-X

Cunha, M. B. da. (2008). From conventional to digital libraries: Differences and convergences. Perspectivas em Ciência da Informação, 13(1), 2–17. https://doi.org/10.1590/s1413-99362008000100002

Dass, S. C. (2013). Fingerprint-based recognition. International Statistical Review, 81(2), 175–187. https://doi.org/10.1111/insr.12017

Dass, S. C., & Jain, A. K. (2007). Fingerprint-based recognition. Technometrics, 49(3), 262–276. https://doi.org/10.1198/004017007000000272

Ekere, J. N., Akor, P. U., & Akor, S. O. (2019). The use of ICT for security and theft prevention in two university libraries in Nigeria. Library Philosophy and Practice, Article 2366.

Fons, M., Fons, F., Cantó, E., & López, M. (2012). FPGA-based personal authentication using fingerprints. Journal of Signal Processing Systems, 66(2), 153–189. https://doi.org/10.1007/s11265-011-0629-3

Fu, J., Xiao, W., Lv, J., & Gao, G. (2012). Research on network security of digital library. Lecture Notes in Electrical Engineering, 113, 1119–1126. https://doi.org/10.1007/978-94-007-2169-2_132

Grigor, G. (2023). Biometric identification: Comparative analysis of current methods. Review of Economics and Finance, 21, 2279–2286. https://doi.org/10.55365/1923.x2023.21.244

Hota, P. K., Hota, L., & Dash, P. K. (2022). Blockchain in digital libraries: State of the art, trends, and challenges. In Machine learning adoption in blockchain-based intelligent manufacturing (pp. 17–32). https://doi.org/10.1201/9781003252009-2

Ismail, R., & Zainab, A. N. (2013). Assessing the status of library information systems security. Journal of Librarianship and Information Science, 45(3), 232–247. https://doi.org/10.1177/0961000613477676

Kabir, M. A. A., & Elmedany, W. (2022). An overview of the present and future of user authentication. In Proceedings of the 4th IEEE Middle East and North Africa Communications Conference (MENACOMM) (pp. 10–17). https://doi.org/10.1109/MENACOMM57252.2022.9998304

Kanta, A., Coisel, I., & Scanlon, M. (2024). A comprehensive evaluation on the benefits of context based password cracking for digital forensics. Journal of Information Security and Applications, 84, Article 103809. https://doi.org/10.1016/j.jisa.2024.103809

Kasemsap, K. (2016). Mastering digital libraries in the digital age. In E-discovery tools and applications in modern libraries (pp. 275–305). https://doi.org/10.4018/978-1-5225-0474-0.ch015

Kasemsap, K. (2017). Mastering digital libraries in the digital age. In Library science and administration: Concepts, methodologies, tools, and applications (Vols. 1–3, pp. 52–82). https://doi.org/10.4018/978-1-5225-3914-8.ch003

Khan, M. S. (2025). Online biometrics: Recent advances and new perspectives. In Modern intelligent techniques for image processing (pp. 269–283). https://doi.org/10.4018/979-8-3693-9045-0.ch011

Larson, P. D., & Williams, S. F. (2010). Web technology – Centralized and collaborative estimating. AACE International Transactions, 1, 442–453.

Lee, Y.-C. (2012). A secure password-based authentication scheme against guessing attack. Lecture Notes in Electrical Engineering, 165, 1255–1260. https://doi.org/10.1007/978-1-4419-8849-2_161

Li, Y. (2024). Multi-layered security technology for campus library systems based on internet technology. In Proceedings of the 5th International Conference on Information Science and Education (ICISE-IE 2024) (pp. 137–146). https://doi.org/10.1109/ICISE-IE64355.2024.11025405

Macmillan, D. (2004). Web-based worksheets in the classroom. Journal of Library and Information Services in Distance Learning, 1(2), 43–51. https://doi.org/10.1300/J192v01n02_05

Nath, R. (2021). Electronic security systems (ESSs) in academic libraries. Library Philosophy and Practice, 1–18.

Okubanjo, A., Okandeji, A., Osifeko, O., Onasote, A., & Olayemi, M. (2022). Development of a hybrid radio frequency identification (RFID) and biometric based library management system. Gazi University Journal of Science, 35(2), 567–584. https://doi.org/10.35378/gujs.834087

Pan, H.-T., Wu, C.-C., Yang, C.-Y., & Hwang, M.-S. (2018). The weaknesses of the virtual password authentication protocol with cookie. IOP Conference Series: Materials Science and Engineering, 466(1), Article 012009. https://doi.org/10.1088/1757-899X/466/1/012009

Papaspirou, V., Maglaras, L., Ferrag, M. A., Kantzavelou, I., Janicke, H., & Douligeris, C. (2021). A novel two-factor honeytoken authentication mechanism. In Proceedings of the International Conference on Computer Communication and Networks (ICCCN). https://doi.org/10.1109/ICCCN52240.2021.9522319

Ravi, T., Vasanthakumar, M., Manjunatha, P. S., & Khyamaling, R. (2024). Use of the Internet of Things as increase in the productivity of a library system. In Proceedings of the Asian Conference on Intelligent Technology (ACOIT). https://doi.org/10.1109/ACOIT62457.2024.10939275

Saravanan, V., & Sindhuja, R. (2013). Iris authentication through Gabor filter using DSP processor. In Proceedings of the IEEE Conference on Information and Communication Technologies (ICT 2013) (pp. 568–571). https://doi.org/10.1109/CICT.2013.6558159

Sharma, M. K., & Kumar, R. (2011). WEBtop (operating systems on web). AIP Conference Proceedings, 1414, 154–158. https://doi.org/10.1063/1.3669948

Subitha, D., Rahul, S. G., & Uddin, P. Md. (2024). Artificial intelligence in biometric systems. In AI based advancements in biometrics and its applications (pp. 47–67). https://doi.org/10.1201/9781032702377-3

Tebbetts, D. R. (2021). Building the digital library infrastructure: A primer. In Information technology planning (pp. 5–23). https://doi.org/10.4324/9781315862347-2

Tedd, L. A., & Large, A. (2005). Digital libraries: Principles and practice in a global environment. https://doi.org/10.1515/9783598440052

Trabelsi, S., & Missaoui, C. (2018). Dissuading stolen password reuse. Lecture Notes in Computer Science, 11263, 116–128. https://doi.org/10.1007/978-3-030-04372-8_10

Yu, Y., et al. (2023). A review of fingerprint sensors: Mechanism, characteristics, and applications. Micromachines, 14(6), Article 1253. https://doi.org/10.3390/mi14061253