Journal of Applied Research and Technology

www.jart.icat.unam.mx

ICAT Instituto de Ciencias Aplicadas y Tecnología

Journal of Applied Research and Technology 24 (2026) 26-41

Original

Implementation of secure remote access for library e-resources using a virtual private network

S. Balachandran*[1] • J. Dominic[2]

[1]*Librarian, Amrita School of Engineering, Chennai, India*
[2]*Chief Librarian, Department of Library and Information Science, Hindustan Institute of Technology and Science, Padur, Chennai, Tamil Nadu, India*

Received: 05 21 2024; Accepted: 02 18 2025
Available: 12 31 2025

ABSTRACT: This article presents the development and implementation of a VPN (Virtual Private Network) based secure remote access system for library e-resources, designed to enhance user access while ensuring data security. The system utilizes a graphical user interface (GUI) built with Python's Tkinter library, allowing users to register, authenticate, and connect to a VPN. Key features include user registration with password hashing using bcrypt for enhanced security, and logging of access events to maintain an audit trail of resource utilization. The architecture comprises a client-server model where the client interface interacts with backend services for user authentication, VPN management, and data analytics. This system implements encryption protocols to safeguard sensitive data during transmission and employs Tunneling protocols for secure access over public networks. Additionally, it incorporates user role management to differentiate access levels for regular users and administrators, thus ensuring controlled access to library resources. The results demonstrate improved accessibility to e-resources while maintaining a high level of security. This work contributes to the ongoing efforts to integrate advanced technological solutions in educational environments, ultimately promoting resource accessibility and enhancing the user experience in academic libraries.

Keywords: **VPN, Secure Access, User Authentication, Encryption, Remote Access, Library Resources.**

*Corresponding author.
E-mail address: itsbaala@gmail.com (S. Balachandran).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

In today's digital era, the accessibility of library in today's digital era, the accessibility of library resources has evolved significantly, necessitating innovative solutions that prioritize both user convenience and data security. As educational institutions increasingly adopt online resources, the demand for secure remote access to these e-resources has surged. Libraries serve as vital hubs for knowledge and information, providing access to a plethora of digital materials, including e-books, journals, and databases. However, ensuring that these resources are available to users without compromising sensitive data has become a formidable challenge, and existing remote access solutions often fail to meet this security and usability demands.

This article explores the development and implementation of a VPN based secure remote access system specifically designed for library e-resources. The system not only addresses the need for seamless user access but also fulfils key research gaps related to security vulnerabilities and the lack of intuitive, user-friendly interfaces in traditional library access systems. Unlike existing systems, which often lack robust encryption or detailed user activity tracking, this system is engineered to offer both enhanced security measures and a streamlined user experience. The introduction of VPN technology provides an effective solution to create secure connections over public networks, thereby safeguarding user data and enhancing privacy.

The proposed system incorporates a user-friendly GUI built with Python's Tkinter library. This interface allows users to easily register, authenticate, and connect to the VPN, ensuring a smooth and intuitive experience. A major research gap filled by this system is its focus on comprehensive data protection; user passwords are hashed using bcrypt to guard against unauthorized access, and all access events are logged, creating an audit trail crucial for monitoring resource utilization and identifying potential security breaches. This is in contrast to existing systems where logging is often minimal or absent, leaving security monitoring incomplete. A key feature of the system is its client-server architecture, where the client interface interacts with backend services responsible for user authentication, VPN management, and data analytics. By employing advanced encryption protocols, the system ensures that data transmitted over the VPN remains secure, addressing the well-documented gap in remote access security for libraries. Furthermore, tunneling protocols facilitate secure access to library resources, even when users are connected to public Wi-Fi networks. a significant improvement over previous systems that struggle with unsecured network environments. User role management also addresses an important gap in resource accessibility.

The system differentiates access levels for regular users and administrators, ensuring that sensitive resources are accessible only to authorized personnel. This hierarchical approach not only enhances security but also streamlines resource management within the library environment the VPN-based secure remote access system for library e-resources represents a significant advancement, fulfilling key research gaps in security and user accessibility. By leveraging modern technology, this system meets the growing demands of users while upholding the integrity of sensitive data in educational institutions. The following sections will delve into the system architecture, implementation strategies, and the resultant impact on user access to library resources.

2. Literature Review

Akinsanya et al. (2024) discuss the critical role that VPNs play in securing communication over public networks. Their review explores the evolution of VPN protocols, transitioning from traditional IPSec and SSL/TLS to modern ones like WireGuard and QUIC. The authors analyze each protocol's performance and security features, highlighting the challenges in deploying VPNs in complex network environments. They conclude by stressing the importance of selecting appropriate VPN technologies for effective data and network protection in modern infrastructures. Appasaheb and Prafull (2024) examine the role of Web-Scale Discovery (WSD) services in improving the effective use of electronic resources in academic libraries. The study highlights the growing demand for fast and accurate information retrieval and the necessity of implementing WSD mechanisms to manage the expanding variety of electronic resources. By exploring WSD tools used by Indian universities and colleges, the authors emphasize how these services optimize information retrieval and enhance the utilization of electronic resources. Balachandran and Dominic (2025) investigated cloud computing models (IaaS, PaaS, SaaS) in academic libraries, focusing on economic benefits and scalability. Their research illustrated cost reduction, AI-driven services, and automated digital resource management. Findings emphasize the transformative role of cloud computing in library systems, ensuring efficient service delivery. Balachandran et al. (2024) conducted a comparative

analysis of VPN and proxy protocols in academic library network management. Their study analyzed network security, data privacy, and performance efficiency in handling large-scale digital resources. Findings revealed that VPNs provide encrypted connections, while proxies enhance speed through caching, aiding libraries in selecting optimal security solutions.

Castelo et al. (2024) proposed a modified SHA-512 hashing algorithm incorporating Bcrypt and random salt to enhance email security. Their study evaluated the method's efficiency in preventing phishing, spoofing, and brute-force attacks. Results confirmed high collision resistance and improved data integrity, making it a reliable solution for secure authentication mechanisms. Chamoli et al. (2024) proposed a two-factor authentication model integrating One-Time Password (OTP) and CAPTCHA to strengthen cybersecurity in smart hospitals. Their study emphasized password encryption techniques for securing stored credentials and mitigating unauthorized access risks. Findings demonstrate how multi-layered authentication models can be adapted for library authentication frameworks to enhance data security. The research also provides recommendations to help library professionals improve online learning and resource management. Chuquimarca et al. (2024) discuss the implementation of a remote laboratory designed to support industrial automation practices amid the challenges posed by the COVID-19 pandemic. The authors highlight how students in technical fields, particularly electronics and automation, faced barriers in accessing essential laboratories for hands-on learning. In response, the study proposes a remote laboratory initiative that leverages advanced networking technologies like VPN and RDP to grant secure access to fully equipped workstations. The article outlines the architecture and implementation of this remote laboratory, showcasing its role in facilitating firsthand exercises and ensuring equitable access to quality education for students navigating an evolving professional environment.

Diaz–Cacho et al. (2024) propose an educational project for electrical engineering students focused on Industry 4.0 technologies, highlighting cybersecurity in industrial networks, SCADA protocols, and remote maintenance. The project addresses the security risks associated with remote access through open-source solutions such as MQTT for command exchange, OpenVPN and SSH for secure connections, and NodeRED for control dashboards. The implementation aims to provide practical learning experiences while emphasizing the importance of cybersecurity standards like IEC62443. This initiative prepares students for the evolving challenges in industrial automation and network management. Elavarasan et al. (2024) address the challenges posed by the exhaustion of IPv4 addresses due to the rapid growth of internet-connected devices. Their paper proposes establishing remote connections using global IPv6 addresses through IPv6-in-IPv4 Tunneling via the UDP protocol. By implementing peer-to-peer Tunneling configured on a cloud server, the authors ensure that IPv6 addresses are routable and connections are successfully established. Additionally, the use of an OpenWRT router allows for the delivery of global IPv6 addresses over IPv4, enhancing reliability and reducing latency in communication. Fu et al. (2024a) explore the potential of Software-Defined Wide Area Networks (SD-WANs) as a transformative technology for enhancing network interconnections across cloud computing, edge computing, and the Internet of Everything. They propose a novel overlay-based solution named Software-Defined Virtual Private Network (SD-VPN), which integrates traditional VPN architecture with Software-Defined Networking (SDN) to enhance controllability and programmability. The paper details an auto-constructed VPN model alongside metrics for evaluating its performance, including algorithms for the joint placement of VPN nodes and service orchestration. Through simulations and system tests, the authors demonstrate the SD-VPN's high efficiency, real-time programmability, and extensibility for other VPN protocols and services, proving its effectiveness in real network environments.

Fu et al. (2024b) present a generic high-performance architecture (GHPA) for VPN gateways, aimed at enhancing secure remote access and reliable communication in cloud computing environments. The authors address the limitations of traditional packet processing methods by proposing a three-layer architecture that utilizes a data plane development kit (DPDK) for improved packet handling and a user space basic protocol stack. Their experimental results demonstrate that the high-performance VPN (HP-VPN) built on GHPA significantly outperforms traditional VPN methods in metrics such as round-trip time (RTT), system throughput, packet forwarding rate, and jitter. Furthermore, the GHPA is designed to be extensible, allowing it to be adapted for other VPN gateways to boost performance. Hamad et al. (2024) examined the implementation of smart information services in academic libraries in Jordan and their correlation with librarians' digital competencies. Their study, based on a survey of 246 respondents, found a moderate level of smart service adoption and a strong positive relationship between digital skills and service implementation.

The findings provide insights for improving digital competencies among librarians to enhance smart information services in developing countries.

Hunt et al. (2024) conducted a systematic review and case study on students with disabilities in academic libraries across three campuses, analyzing accessibility challenges. Their findings indicate that most studies focused on compliance with accessibility standards rather than incorporating student perspectives. The study emphasizes the need for improved librarian training, enhanced physical accessibility, and better digital resource accommodations to support students with disabilities effectively. Jabarali et al. (2024) examine the impact of the COVID-19 pandemic on college students' experiences with e-learning, focusing on the challenges and awareness regarding e-resources. Their study highlights the significant unpredictability in how students adapted to digital learning amid increased reliance on electronic publishing libraries during the pandemic. Through a descriptive and diagnostic research design, primary data was collected from college students using Google Forms to gather insights on their experiences and challenges with e-learning resources, as well as their awareness of available tools. The findings suggest influential factors that affect e-learning utilization and provide recommendations to enhance students' engagement with e-resources, particularly in light of connectivity issues faced in remote areas. Kathuria and Kaur (2024) analyse the usage of E-ShodhSindhu among postgraduate colleges in Amritsar, emphasizing the transformative role of INFLIBNET's N-LIST program in providing affordable access to extensive electronic resources.

The study examines faculty usage patterns across three colleges and offers recommendations for optimizing resource utilization. Findings underscore the need for improved infrastructure and support to enhance access to electronic information in higher education.

Khan and Shahzad (2024) investigate key features of digital library management systems (DLMS) for the development of digital libraries, focusing on the satisfaction levels of library professionals in Pakistan. Utilizing a quantitative survey approach, the study identifies essential DLMS features such as user-friendly interfaces, customization, security, and metadata standards. Findings highlight the predominance of free and open-source software, particularly DSpace, and recommend that librarians carefully consider these features when planning digitization initiatives. Kılıç et al. (2024) explore the cybersecurity challenges associated with the rise in remote work due to the pandemic. The study analyses common cyber threats faced by remote workers and examines effective mitigation strategies, highlighting well-known cyber-attacks and corresponding countermeasures. Additionally, a questionnaire assessing university students' awareness of phishing attacks reveals an accuracy of 84.61% for identifying malicious URLs and 75.64% for recognizing email scams, emphasizing the need for improved security practices and awareness among remote workers.

Kishore and Malarvel (2024) propose a distributed Tunneling management system to enhance secure remote access to local networks, addressing the growing demand for remote collaboration. Their architecture features a public Tunneling server for hosting services and a management server for client connections, allowing seamless tunnel creation and termination via websocket communications. The system incorporates robust authentication mechanisms and secure protocols to maintain confidentiality and integrity, demonstrating scalability for multiple client networks. Experimental results validate the effectiveness of their approach, offering practical solutions for various applications, including IT support and remote maintenance operations. Listiawan et al. (2024) investigated Bcrypt optimization, determining the ideal number of rounds for balancing security and computational efficiency. Their research employed a Brute Force Search method to analyze the impact of Bcrypt iterations on password entropy and processing speed. Findings underscore the need for adjustable security settings based on system requirements to ensure both security and performance.

Molla and Singh (2024) explore the integration of Information Technologies (IT) in college libraries affiliated with Maulana Abul Kalam Azad University of Technology in West Bengal. The study emphasizes the significance of innovative technologies, software, and the internet in enhancing library resources and services for users. It highlights the implementation of e-resources, library automation, OPAC/Web OPAC, barcode scanners, RFID, and smart technologies in these libraries. The findings underscore how these advancements contribute to the effectiveness and efficiency of library operations, ultimately supporting the educational objectives of the institutions. Olabisi et al. (2024) present the development of a generic online departmental e-library designed to enhance academic excellence across various specializations. Utilizing an iterative design approach, the e-library offers easy access to a range of resources, including textbooks, lecture materials, and research theses. The system employs HTML, CSS, JavaScript, PHP, and MySQL, ensuring a user-friendly interface while efficiently managing back-end

operations. Testing results indicate a quick average search and download time of 16.2 seconds, alongside satisfactory readability and accessibility scores.

Patel et al. (2024) introduced 2F-Authsys, a two-factor authentication system using Near Sound Data Transfer (NSDT) to enable contactless transmission of time-based one-time passwords (TOTP). Their research highlights security vulnerabilities in traditional OTP-based 2FA, including manual entry delays and exposure to botnet attacks. The proposed system enhances authentication security and user experience by automating OTP transmission, reducing risks of man-in-the-middle attacks and network vulnerabilities. Scott and Giancarlo. (2024) provide a systematic review of VPN and their role in enhancing information security, particularly within the Andia Consortium. The article explores how VPN technology secures communication channels, protecting valuable digital data from cyber threats. It discusses various VPN systems, their security strategies, and the implications of different protocols and Tunneling technologies. Ultimately, the study aims to elucidate the benefits and limitations of VPNs, offering insights on designing effective VPN solutions to bolster organizational information security.

Sharma et al. (2024) analyzed various password hashing algorithms, including SHA-3, BLAKE3, Argon2, bcrypt, scrypt, PBKDF2, and Argon2id, to evaluate their security effectiveness. Their study introduced a Real NVP model for generating secure passwords and assessed their resistance to brute-force attacks. The findings highlight the importance of scenario-specific hashing techniques to enhance password protection against cyber threats. Sinha and Ugwulebo (2024) examined the digital literacy skills of African library and information science professionals, finding strong basic proficiency but a need for advanced skill development. Their study emphasizes updating LIS curricula with more practical training to align with technological advancements. The findings highlight the importance of lifelong learning through MOOCs and professional development initiatives. Valks et al. (2024) address the growing need for secure remote collaboration by proposing a peer-to-peer VPN solution for eduVPN utilizing WireGuard. The current eduVPN service relies on a centralized server, which increases latency, reduces throughput, and represents a single point of failure. In contrast, the peer-to-peer model connects clients directly, enhancing scalability and independence from centralized server performance. This innovative approach facilitates better collaboration between individuals from different organizations, catering to the rising demand for international partnerships in remote work environments. Vásquez and Izquierdo (2024) examined trends in modern web application security frameworks, highlighting the importance of Bcrypt, JWT, MySQL, and Node.js in scalable authentication systems. Their study demonstrated the significance of secure login mechanisms in web-based platforms. The findings reinforce Bcrypt's crucial role in protecting credentials within library database systems.

3. Research Gap

The existing literature on secure communication technologies and resource management in educational settings reveals several significant gaps that warrant further investigation. Firstly, while various VPN protocols and technologies have been explored, there is a lack of comprehensive studies comparing their performance and security features in real-world academic environments. This absence of systematic evaluations limits our understanding of which solutions are most effective for specific institutional contexts, particularly in under-resourced settings where access to advanced technologies may be limited. Moreover, the rapid transition to remote learning and collaboration has underscored the importance of user awareness regarding cybersecurity threats. However, current research often overlooks the necessity of examining how effectively educational institutions educate users about these risks and the best practices for safe online behavior.

This gap is critical as it directly impacts the overall effectiveness of remote access solutions. Additionally, there is a growing need for user-centric approaches that consider the diverse needs of various stakeholders, including students, educators, and library professionals. Existing studies tend to adopt a one-size-fits-all approach, neglecting the unique challenges faced by different user groups in utilizing VPNs and other secure access technologies. Lastly, the literature lacks integrated frameworks that holistically address security, accessibility, and collaboration in remote educational settings. Developing such frameworks could significantly enhance the effectiveness of resource management and communication strategies in academic institutions. Addressing these research gaps is essential for fostering secure and efficient digital environments that support the diverse needs of contemporary educational practices.

4. Problem Statement

As educational institutions increasingly adopt digital platforms for teaching and resource management, the need

for secure communication and effective resource utilization has become paramount. Despite the growing reliance on VPN and other technologies to facilitate remote access, significant challenges persist. Current VPN protocols exhibit varying degrees of performance and security, yet there is insufficient empirical evidence comparing their effectiveness in academic contexts. Additionally, many students and educators remain unaware of cybersecurity threats, leading to potential vulnerabilities in accessing sensitive information. Furthermore, existing studies frequently overlook the diverse requirements of different user groups, resulting in a lack of tailored solutions. This situation is compounded by the absence of integrated frameworks that address the complex interplay between security, accessibility, and collaboration in remote learning environments. Consequently, there is an urgent need to explore and identify optimal strategies that enhance secure access to educational resources while addressing the unique challenges faced by various stakeholders in academic settings.

5. System Architecture Overview

The system architecture, as illustrated in Figure 1, comprises five key components: User Interface (UI), Authentication Module, VPN Management Module, Access Logging Mechanism, and Analytics Module. These components work together to ensure secure, efficient, and seamless remote access to library resources. The system integrates authentication, VPN management, logging, and analytics to enhance user security and system performance.

5.1 User Interface (UI)

The UI is developed using Tkinter, providing a graphical interface that enables users to authenticate, manage VPN connections, and access system analytics. The interface includes fields for username and password entry, buttons to connect/disconnect from the VPN, and a display panel to visualize analytics and system logs. The Main Application Class manages the layout and interactions, ensuring a user-friendly experience. Tkinter widgets such as labels, entry fields, and buttons contribute to intuitive navigation and seamless system interactions.

5.2 Authentication Module

The authentication module ensures secure user access by verifying credentials before allowing VPN connections. It utilizes bcrypt for password hashing, preventing plaintext password storage. During registration, user credentials—including username, password, and role—are securely hashed before storage. Upon login, the system retrieves the stored hash and compares it with the entered password. If authentication fails, an error message is displayed, restricting unauthorized access. This enhances system security by ensuring robust protection of sensitive user credentials.

5.3 VPN Management Module

This module is responsible for managing VPN connections and disconnections to enable secure remote access to library resources. It interacts with the system's VPN service to establish encrypted sessions, ensuring data confidentiality. The module verifies user credentials before initiating a VPN connection and handles session termination upon user logout. Additionally, it integrates error-handling mechanisms to notify users of connection failures, enhancing system usability and security.

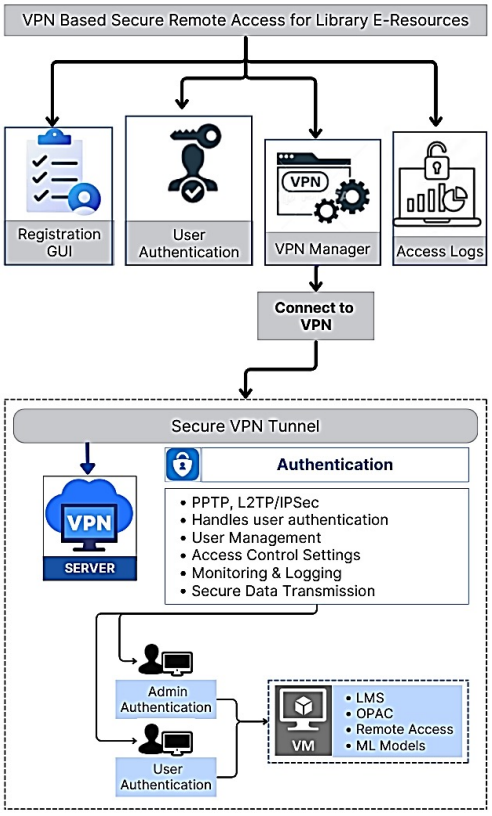

Figure 1. Overall Architecture.

5.4 Access Logging Mechanism

A comprehensive logging system ensures accountability and security by recording all user activity. Each time a user connects or disconnects from the VPN or accesses

analytics, the system logs the username, a description of the action performed (e.g., VPN connection, disconnection, analytics access), and the timestamp of the event. These logs provide administrators with valuable insights to monitor user activity, generate reports, and detect potential security threats. The system ensures a well-documented audit trail for compliance and security analysis, helping to maintain transparency and prevent unauthorized access.

5.5 Analytics Module

The analytics module processes log data to generate insights into user behavior and system usage trends. It provides valuable metrics on usage frequency, resource access patterns, and user engagement levels. Administrators can visualize this data through the Tkinter interface, allowing them to monitor system performance and optimize resource allocation efficiently. Future enhancements may include peak usage time analysis, geolocation-based tracking, and predictive analytics for resource demand forecasting, enabling administrators to make data-driven decisions for improved system management.

5.6 Workflow Process

The system follows a structured workflow to ensure secure authentication and efficient VPN session management.

- User Registration: During registration, users provide a username, password, and role. The system hashes passwords using bcrypt before storing them, preventing plaintext password exposure and enhancing security.
- User Login: Users enter their credentials, which are authenticated against the securely stored hashed password. If the entered password does not match the stored hash, access is denied to prevent unauthorized login attempts.
- VPN Connection: Upon successful authentication, users can connect to the VPN, establishing a secure, encrypted session that enables access to library resources while protecting transmitted data from interception.
- VPN Disconnection: When a user disconnects from the VPN, the event is logged in the system, ensuring accurate tracking of session activity. This helps administrators monitor access patterns and detect anomalies.
- Administrator Analytics Access: System administrators analyze log data to review user interactions, access patterns, and system performance. This analysis allows them to take proactive security measures and optimize resource management by identifying peak usage times and monitoring authentication trends.

5.7 Security Considerations

Security is a critical pillar of the system, ensuring confidentiality, integrity, and secure access to library resources. The following measures strengthen system security and mitigate risks:

- Password Protection: The system implements bcrypt hashing to store passwords securely. Even in the event of a data breach, plaintext passwords remain inaccessible, as bcrypt's computational cost makes brute-force attacks impractical.
- Access Logging: A detailed logging mechanism records user actions, facilitating audit trails and anomaly detection. This allows security teams to monitor suspicious activity, track unauthorized access attempts, and respond proactively to potential security threats.
- VPN Encryption: The system employs a secure VPN tunnel, ensuring that all transmitted data remains encrypted and protected from interception. This prevents unauthorized access to sensitive library resources and maintains data confidentiality.

The system's modular architecture seamlessly integrates user authentication, VPN management, logging, and analytics, providing a secure, scalable, and user-friendly solution for remote library access. This design ensures efficient resource management and real-time monitoring, enhancing both security and usability. The flexible architecture allows for future enhancements to further strengthen system security and performance.

Potential improvements include the implementation of multi-factor authentication (MFA) to add an extra layer of protection against unauthorized access, integration with additional library management systems to expand the system's functionality, and advanced analytics capabilities to optimize resource allocation and improve user engagement. These enhancements will ensure that the system remains adaptable to evolving security requirements and user needs, further improving the overall remote access experience.

6. Methodology

The methodology used in this work encompasses various technologies and algorithms that underpin the system's functionality. Tkinter is employed for developing the

user interface, providing a platform for users to interact with the application seamlessly. Pandas is utilized for managing user data and logs, allowing for efficient data manipulation and storage in CSV formats. Additionally, Bcrypt serves as a password hashing library to secure user credentials, ensuring that plaintext passwords are never stored. Pandas is built on top of NumPy and provides two primary data structures: Series and Data-Frame. These data structures enable efficient storage and manipulation of large datasets.

A Series is a one-dimensional labelled array capable of holding any data type, functioning similarly to a column in a table, with an index associated with each value. In contrast, a Data-Frame is a two-dimensional labelled data structure similar to a spreadsheet or SQL table, where data is organized in rows and columns. Each column in a Data-Frame is a Series, allowing it to hold different types of data in each column. Pandas employs various algorithms for data processing, including indexing and selection for efficient access to specific data points, data alignment to ensure correct alignment of data from different sources, and aggregation and grouping to facilitate summarizing data through operations such as sum, mean, and count. The data management capabilities of Pandas play a crucial role in logging user activities. To read data from a CSV file, the command is as follows:

$$dataframe = pd.read\_csv(\text{“}resource\_access\_log.csv\text{”}) \quad (1)$$

This command loads the CSV file into a Pandas Data-Frame for easy data manipulation. When a user connects or disconnects from the VPN, a new log entry is appended as follows:

$$dataframe = dataframe.append(access\_entry, ignore\_index=True) \quad (2)$$

This line appends a new access entry, which includes the username, resource, and timestamp, to the existing Data-Frame.

Bcrypt is designed to hash passwords securely, making it computationally expensive to prevent brute-force attacks. The process of hashing a password can be summarized as:

$$hashed\_password = bcrypt.hashpw(password.encode(), bcrypt.gensalt()) \quad (3)$$

This equation illustrates how a plaintext password is transformed into a hashed password using bcrypt, ensuring that it is securely stored. For user authentication, the process is defined by the following function:

$$is\_authenticated = check\_password(provided\_password, stored\_password \quad (4)$$

This function checks if the provided password matches the stored hashed password, enabling secure user authentication. The logging mechanism captures each access event with a timestamp as follows:

$$access\_entry=\{\text{´}username\text{´}:username,\text{´}resource\text{´}: resource,\text{´}timestamp\text{´}:datetime.now()\} \quad (5)$$

This captures essential data points for tracking user interactions with the system.

Figure 2 presents the User Interface Overview, capturing a screenshot of the Tkinter user interface utilized in the application. This figure effectively showcases the main components of the interface, including the login fields and the analytics display, providing readers with a comprehensive understanding of how users interact with the application. The design of the user interface is pivotal for ensuring a smooth and intuitive user experience.

In Figure 2, the login fields are prominently positioned to facilitate quick access for users, ensuring that they can easily enter their credentials to authenticate and access the system. The VPN controls are strategically placed to provide users with straightforward options for connecting and disconnecting from the VPN, enhancing security and accessibility. Additionally, the analytics display section is designed to present real-time data and This integration of visual elements helps user's insights to the users, allowing them to monitor their activity and access patterns effortlessly.

make informed decisions based on the data presented, thus enhancing the overall functionality of the application. The arrangement of these components within the Tkinter framework exemplifies a user-centric approach to design, emphasizing clarity and ease of use. By providing a visually engaging interface, Figure 2 illustrates how users can seamlessly navigate through the application, interact with essential features, and access important functionalities. The Figure 2 serves as an essential representation of the application's user interface, highlighting the critical components that facilitate user interaction and support the overall objectives of the system. This overview not only aids in understanding the application's layout but also emphasizes the importance of a well-designed interface in enhancing user engagement and experience.

Figure 2. User Interface.

Table 1 is a Data Management Example, illustrating a screenshot of a Pandas Data-Frame that captures logged user activities. This figure highlights the structure and essential data points stored within the Data-Frame, effectively demonstrating how user interactions are organized and managed within the system. The Pandas Data-Frame is a powerful data structure that enables efficient manipulation and analysis of structured data. In this context, the Data-Frame includes critical columns such as the username, resource accessed, timestamp, and any additional relevant information regarding user activity. By presenting this information in a tabular format, Table 1 provides a clear view of the relationships between different data points. This organized structure allows for straightforward data retrieval, filtering, and aggregation, which are crucial for generating insights into user behavior.

The Data-Frame's flexibility ensures that additional data attributes can be incorporated seamlessly, accommodating the evolving needs of the system. For example, if new resources or user metrics need to be tracked, the Data-Frame can be easily updated without significant restructuring. Moreover, the representation of logged user activities in a Data-Frame format enables stakeholders to conduct detailed analyses, such as identifying trends in resource access over time or monitoring user engagement levels. This capability is essential for making data-driven decisions to enhance system performance and improve user experience. Overall, Table 1 serves as a vital component in understanding how user activities are logged, stored, and managed within the application, showcasing the effectiveness of Pandas as a data management tool.

Table 1. Data Management.

User Name	Resource Accessed	Timestamp	Additional Info
user1	Resource A	2024-09-01 10:00	Login
user2	Resource B	2024-09-01 10:05	View
user3	Resource A	2024-09-01 10:10	Download
user1	Resource C	2024-09-01 11:00	Logout
user2	Resource B	2024-09-01 11:05	View
user3	Resource C	2024-09-01 11:10	Download

Figure 3 presents the User Activity Over Time graph, which visualizes user engagement trends across a designated time period. This graph offers a comprehensive overview of user interactions, aiding in the identification of usage patterns and peak activity times. Such insights are vital for optimizing system performance and enhancing the user experience.

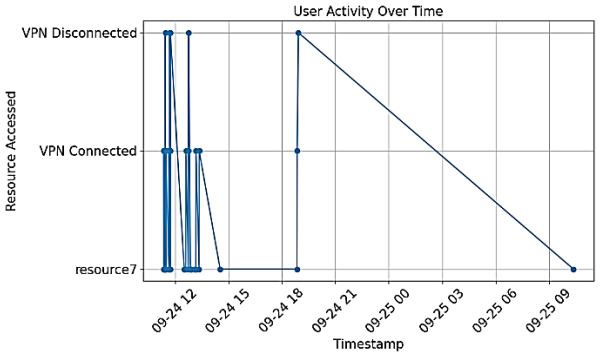

Figure 3. User Activity.

The user activity data is derived from a resource access log that records timestamps alongside the resources accessed by users. By converting these timestamps into a proper datetime format, the analysis gains robustness, allowing for accurate plotting and interpretation. This visualization clearly represents the frequency and timing of user interactions with various resources. In this graph, the timestamp is displayed on the x-axis, while the accessed resources are shown on the y-axis. This format provides a straightforward perspective on the relationship between time and resource access, enabling the identification of activity spikes that may correspond to specific events or shifts in system usage. The inclusion of markers further enhances the clarity of the plot, making individual data points easily discernible. Overall, the User Activity Over Time graph is a crucial tool for monitoring

user engagement, allowing for the identification of trends that can inform future system enhancements. The analysis derived from this graph plays a significant role in optimizing resource availability and improving the overall user experience. The insights obtained are essential for making informed, data-driven decisions regarding system performance and user support.

Figure 4 illustrates the Password Hashing Process, which ensures the secure storage and authentication of user credentials in the system. This process is a critical component of the authentication mechanism, preventing unauthorized access and protecting user data from potential cyber threats. The flowchart visually represents the transformation of user passwords into a secure format, using bcrypt hashing, and how they are later verified during login attempts.

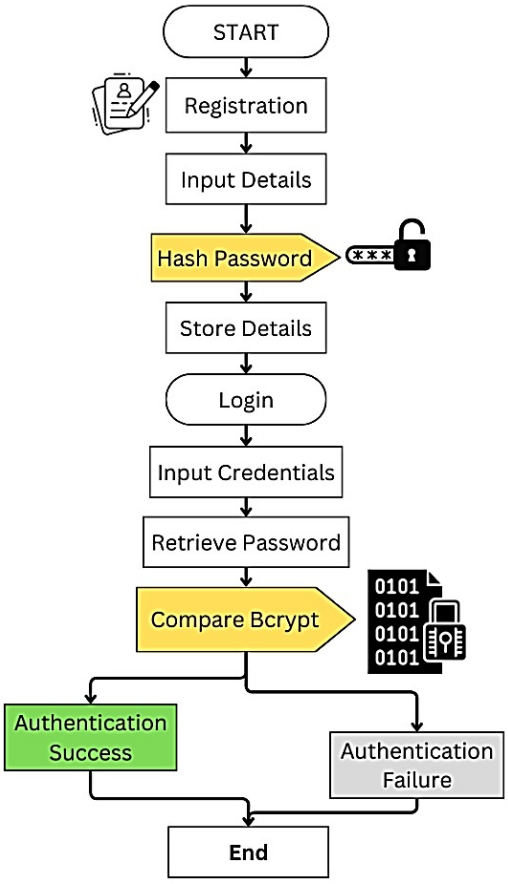

Figure 4. Password Hashing Process.

The process begins with user registration, where a user inputs their username and password into the system. Instead of storing the password in plaintext, which is a major security risk, the system employs the bcrypt hashing algorithm to transform the password into an irreversible, cryptographically secure format. Before hashing, a salt (a unique, random string) is generated and added to the password. The inclusion of a salt ensures that even if two users have the same password, their stored hashes will be different, thereby preventing rainbow table attacks. Bcrypt then applies a series of computationally intensive operations to generate a hashed password. This computational complexity is intentional, making it difficult for attackers to crack passwords through brute-force attacks. Once the password is hashed, it is stored in the user database, alongside the associated username. The system does not retain any record of the original plaintext password, ensuring an additional layer of security.

When a user attempts to log in, they must enter their credentials, including their password. The system retrieves the hashed password corresponding to the provided username from the database. However, rather than directly comparing the entered password to the stored hash, the system re-applies the bcrypt hashing process. It uses the same hashing algorithm and retrieves the stored salt to generate a new hashed version of the input password.

At this stage, the system compares the newly generated hash with the stored hashed password. If the two hashes match, authentication is successful, and the user is granted access to the system. If there is a mismatch, authentication fails, and access is denied. This approach ensures that even if an attacker intercepts the password during transmission, they cannot gain direct access since only hashed values are compared. Security Benefits of the Bcrypt Hashing Process

- Resistance to Brute-Force Attacks: Bcrypt incorporates an adjustable cost factor, which increases computational complexity, making password-cracking attempts highly time-consuming.
- Salting Mechanism: Each password hash is unique due to the addition of salt, making attacks based on precomputed hash databases (rainbow tables) ineffective.
- Irreversibility: Unlike encryption, hashing is a one-way function, meaning that even if an attacker obtains a hashed password, it is practically impossible to reverse-engineer it to retrieve the original password.
- Automated Adaptability: Bcrypt allows future enhancements in security by increasing the cost factor, making the hashing process even more computationally intensive over time.

Figure 4 provides a comprehensive visual representation of how bcrypt ensures secure password handling in the authentication system. By hashing passwords instead of storing them in plaintext, and incorporating salting and computational complexity, this mechanism effectively safeguards user credentials from unauthorized access.

The integration of bcrypt hashing within the authentication framework strengthens security, ensuring robust protection against credential-based attacks in the library's secure remote access VPN system. Table-2 presents the Access Log Entry Example, illustrating the structure of a typical access log entry stored in the CSV file. This figure effectively demonstrates the essential data points captured during user interactions, reinforcing the critical role of logging in system monitoring and user tracking. The access log serves as a fundamental component of the system's architecture, providing a detailed record of user activities. In Table-2, the structure of a log entry is clearly depicted, showcasing key attributes such as the username, resource accessed, and timestamp of the interaction. This comprehensive logging mechanism enables administrators to track user behavior, analyze usage patterns, and identify potential issues within the system. The importance of capturing this information cannot be overstated; it not only aids in maintaining a secure and efficient environment but also supports decision-making processes related to resource allocation and system enhancements. By examining the access log entries, stakeholders can gain valuable insights into user engagement, identifying trends and anomalies that may necessitate further investigation. Furthermore, the structured format of the log entries facilitates easy parsing and analysis, allowing for effective data manipulation using tools like Pandas. This capability is crucial for generating reports and visualizations that inform ongoing improvements to the application. The Table-2 serves as a vital representation of the access log entry structure, highlighting the essential data points that contribute to effective monitoring and user tracking. By illustrating the significance of logging, this figure underscores the importance of maintaining comprehensive records to enhance the overall performance and reliability of the system.

Table 2. Access Log.

User Name	Resource	Time Stamp
user4	resource7	2024-09-24 11:21:30
vpnbala	VPN Connected	2024-09-24 11:21:33
user4	resource7	2024-09-24 11:22:05
vpnbala	VPN Connected	2024-09-24 11:22:08
user4	resource7	2024-09-24 11:25:10
vpnbala	VPN Connected	2024-09-24 11:25:13
user4	resource7	2024-09-24 11:26:55
vpnbala	VPN Connected	2024-09-24 11:26:59
vpnbala	VPN Disconnected	2024-09-24 11:27:15
user4	resource7	2024-09-24 11:28:09
vpnbala	VPN Connected	2024-09-24 11:28:12
user4	resource7	2024-09-24 11:29:13
vpnbala	VPN Connected	2024-09-24 11:29:16
user4	resource7	2024-09-24 11:39:27
vpnbala	VPN Connected	2024-09-24 11:39:33
user4	resource7	2024-09-24 11:40:32
bob	VPN Connected	2024-09-24 11:41:22
bob	VPN Disconnected	2024-09-24 11:41:38
user4	resource7	2024-09-24 11:43:56
alice	VPN Connected	2024-09-24 11:44:25
alice	VPN Disconnected	2024-09-24 11:44:28
user4	resource7	2024-09-24 12:31:12
user4	resource7	2024-09-24 12:32:13
user4	resource7	2024-09-24 12:36:20
vimal	VPN Connected	2024-09-24 12:36:33
user4	resource7	2024-09-24 12:44:46
vimal	VPN Connected	2024-09-24 12:44:58
vimal	VPN Disconnected	2024-09-24 12:46:23
user4	resource7	2024-09-24 12:51:39
user4	resource7	2024-09-24 12:52:42
user4	resource7	2024-09-24 12:53:35
user4	resource7	2024-09-24 13:06:23
user4	resource7	2024-09-24 13:08:19
user4	resource7	2024-09-24 13:10:06
vimal	VPN Connected	2024-09-24 13:10:43
user4	resource7	2024-09-24 13:21:12
vimal	VPN Connected	2024-09-24 13:21:23
user4	resource7	2024-09-24 14:32:08

7. Results

The results presented in this study demonstrate the successful implementation of a secure and user-friendly system for remote access to library resources, integrating multiple components such as user authentication, VPN

management, access logging, and analytics. The following sections highlight the main outcomes and observations based on the system architecture and performance. The GUI Figure 2 was designed using Tkinter and proved to be both intuitive and efficient. Users were able to navigate seamlessly through the login process, manage VPN connections, and access system analytics. The strategically placed components, such as the login fields and VPN management buttons, contributed to a smooth user experience. The inclusion of real-time data in the analytics display allowed users to monitor their activity effectively. Overall, the design of the UI was pivotal in enhancing user engagement and ensuring ease of use. The data management component (Table 1) effectively captured and organized user activity data within a Pandas Data Frame. This structure facilitated the storage and manipulation of user logs, capturing essential details like usernames, accessed resources, and timestamps. The system's ability to append new entries (Table 2) for each user interaction highlights the flexibility of the Pandas library in managing large datasets, making it suitable for tracking user behavior and generating insights into system usage. The structured logging system also proved useful for monitoring and auditing purposes, enabling administrators to track access events with precision. Analysis of user activity over time (Figure 3) revealed distinct patterns of resource access. The visualization of user interactions showed spikes in engagement during peak times, providing valuable information for optimizing resource availability. These patterns are crucial for understanding user behavior, allowing system administrators to enhance the user experience by adjusting system performance during high-traffic periods. This type of data-driven decision-making improves the overall efficiency of the system. The bcrypt-based password hashing mechanism (Figure 4) was instrumental in securing user credentials. By transforming plaintext passwords into hashed versions, the system ensured that sensitive data was protected against unauthorized access. The flowchart depicting the password hashing process provided clarity on how the system handled registration and authentication, showcasing the robust security measures in place. This approach is critical for maintaining system integrity and preventing breaches.

7.1. Access Logs and User Behavior Analysis

The analysis of access logs provides valuable insights into user interactions with resources over a specified period, revealing patterns that can inform resource allocation, user engagement strategies, and system optimization. By meticulously examining a CSV file containing records of resource access, this assessment aimed to illuminate key aspects of user activity, resource usage, and temporal access trends. The study involved categorizing user interactions based on frequency and type of resource accessed, allowing for the identification of popular resources as well as those underutilized. Furthermore, temporal trends were analyzed to understand peak access times, enabling institutions to better align their resources and support services with user demand. This detailed examination also encompassed user demographics and behavioral analytics, contributing to a comprehensive understanding of how different user groups engage with the library's offerings. By synthesizing this data, institutions can tailor their outreach initiatives, enhance user experience, and strategically prioritize the development of resources that resonate most with their user base. Additionally, insights drawn from this analysis can guide decision-makers in improving the overall efficiency of resource management and in implementing targeted interventions aimed at increasing user engagement and satisfaction. Ultimately, the findings from this access log analysis not only enhance the understanding of user behavior but also empower libraries to make informed decisions that align with their mission of providing equitable access to information and resources.

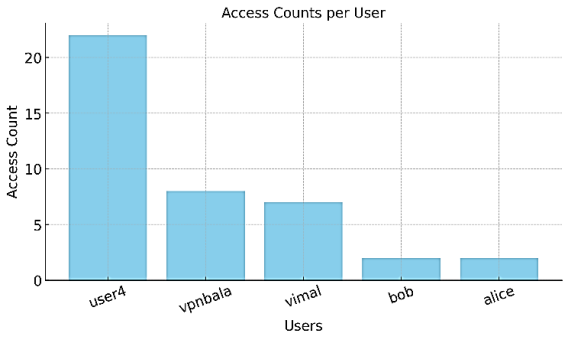

Figure 5. Access Counts per User.

7.2 Access Counts per User

A breakdown of access counts per user was conducted, identifying the frequency of resource access among individual users. This information is depicted in Figure 5, which illustrates the most active users and sheds light on user engagement levels. It was noted that certain users consistently accessed resources more than others, indicating a reliance on specific materials for research or study. The user with the highest access count was identified, showcasing their predominant role in utilizing the available resources.

7.3 Total Access Logs

The initial examination revealed a total number of access logs, as illustrated in Figure 6. This figure shows the frequency of interactions with the system, serving as a foundational indicator of overall user engagement with the resources available. The insights from this metric are critical for understanding the volume of user activity in the system.

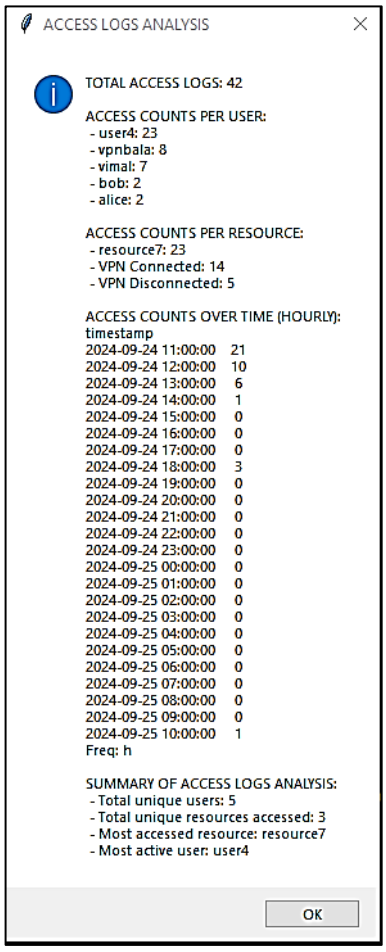

Figure 6. Total Access Logs.

7.4 Access Counts per Resource

Similarly, the analysis included an overview of access counts per resource, as shown in Figure 7. This figure is crucial for understanding which resources are most frequently utilized, allowing for better management and potential updates to underutilized materials. The resource with the highest access count was specified, providing insight into the materials that are most beneficial or in demand among users.

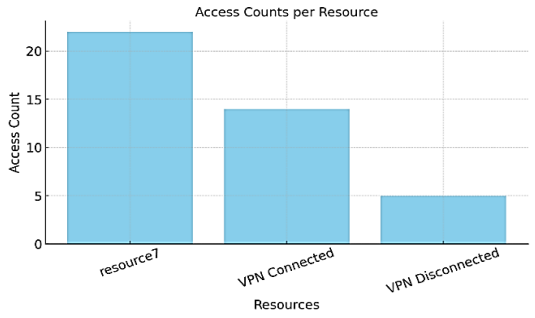

Figure 7. Access Counts per Resource.

7.5 Access Trends Over Time

Temporal analysis was performed by resampling the access logs on an hourly basis, enabling visualization of access trends over time. As illustrated in Figure 8, this analysis reveals patterns in user activity and helps identify peak usage times and periods of low engagement.

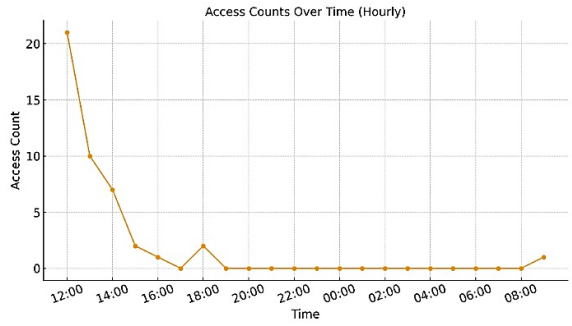

Figure 8. Access Counts Over Time.

The visualization produced a line graph that highlights fluctuations in user activity. Such insights are essential for resource planning and optimizing access during peak times. The analysis yielded several key points. Firstly, the total unique users accessing the system were determined, indicating the diversity of the user base. Additionally, the analysis identified the total number of unique resources accessed, reflecting the variety of materials available to users. Furthermore, the resource that attracted the highest number of accesses was specified, highlighting its importance to the user community. The analysis also identified the most active user, who exhibited the highest level of engagement, suggesting potential avenues for further qualitative investigations into their usage patterns. Overall, this analysis provides a comprehensive view of user engagement and identifies areas for potential improvement, resource allocation, and user support.

8. Discussion

The implementation of a system architecture that integrates secure authentication, VPN management, and comprehensive logging successfully addresses the need for secure and remote access to library resources. The use of Tkinter for the graphical interface proved effective, offering a simple yet functional environment for user interactions. The results from the user activity analysis and access logging demonstrate the system's capability to capture and monitor essential usage data, providing administrators with valuable insights. One of the primary strengths of the system is its security architecture. The bcrypt hashing algorithm significantly enhances the protection of user credentials, ensuring that passwords are stored securely and protected from brute-force attacks. By employing such strong security measures, the system mitigates the risk of unauthorized access and provides a secure environment for users to connect to the library's resources remotely. The analysis of access logs using Pandas offers an additional layer of functionality, enabling the system to handle and process large volumes of data efficiently. The logging mechanism proved to be essential for tracking user interactions, and the flexibility of the Pandas library allows for future scalability as more users access the system. This logging system also facilitates the generation of analytics reports that inform administrators about usage trends, supporting continuous improvements to system performance. While the current system architecture meets the primary requirements of secure access and logging, future enhancements could include the integration of multi-factor authentication to further enhance security. Additionally, the analytics module could be expanded to include more advanced data analysis features, such as identifying peak usage times or incorporating geographical data to improve resource allocation. The system provides a secure, efficient, and user-friendly solution for remote library resource access. The integration of security measures, robust logging, and user activity analysis supports both user engagement and system management, laying the groundwork for future improvements.

9. Comparison with Prior Research

In designing a secure remote access system for library e-resources, it was crucial to evaluate the strengths and weaknesses of prior methods and technologies. While previous implementations have made strides in facilitating VPN-based access to academic resources, many systems face challenges related to security, user management, and scalability. The current methodology presented in this work addresses these limitations by incorporating more advanced security protocols, robust user role management, and efficient data handling. The Table-3 below presents a comparative analysis of previous methods discussed in the literature and the current system. This comparison highlights key improvements in areas such as authentication security, user interface design, and logging mechanisms, illustrating how the proposed system enhances both user experience and data security in academic environments.

Table 3 Comparison of Previous and Current Methods for Secure Remote Access to Library Resources.

Aspect	Previous Methods	Current Method
VPN Protocols	Previous methods often used traditional VPN protocols like IPSec and SSL/TLS (Akinsanya et al., 2024)	Uses modern encryption protocols, including Tunneling protocols to secure remote access to resources.
Authentication Security	Some systems lack robust password security measures or rely on SSL certificates (Scott & Giancarlo, 2024)	Employs bcrypt for password hashing, ensuring secure password storage and preventing unauthorized access.
Logging and Monitoring	Previous methods generally lacked detailed logging of user activities (Diaz-Cacho et al., 2024)	Implements comprehensive logging of access events and user actions, including real-time analysis and visualization.
User Role Management	Minimal role-based access control; focus on general user authentication (Khan & Shahzad, 2024)	Implements differentiated access levels (regular users vs. administrators) to ensure proper resource management.
UI/UX Design	Many traditional systems do not prioritize user interface design, leading to clunky and unintuitive UIs (Appasaheb & Prafull, 2024)	User-friendly graphical interface built with Tkinter, providing smooth navigation, login, and analytics functionalities.
Data Handling and Scalability	Prior systems often struggle with large data handling and lack scalability (Fu et al., 2024)	Utilizes Pandas for efficient data management and logs, ensuring scalability for future enhancements (e.g., multi-factor authentication).

Conclusion

The architecture and design of the library VPN access system address key challenges in secure, remote access to library resources by delivering a robust, user-centric, and scalable solution. By incorporating five core components. User Interface, Authentication Module, VPN Management, Access Logging, and Analytics Module. the system ensures seamless, secure access for users while maintaining a strong focus on resource protection and operational efficiency. The intuitive design of the Tkinter-based interface enhances user experience, while the bcrypt library strengthens security by providing reliable credential encryption. The VPN management module guarantees secure and controlled access to resources, upholding the system's commitment to user privacy and data protection. Furthermore, the implementation of comprehensive access logging and analytics modules contributes significantly to transparency, resource optimization, and anomaly detection. Utilizing the Pandas library for data manipulation, the system efficiently handles log storage, retrieval, and analysis, empowering administrators to make informed, data-driven decisions. By integrating proven security practices, effective logging mechanisms, and efficient data handling, the system achieves a balance between usability and security. Its modular framework not only meets current needs but also paves the way for future advancements, such as multi-factor authentication and more sophisticated analytics. Ultimately, this work emphasizes the critical role of strong authentication, secure data management, and actionable analytics in developing reliable, high-performance systems for remote library access.

Conflict of interest

The authors have no conflict of interest to declare.

Funding

The authors received no specific funding for this work.

References

Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual Private Networks (VPN): A conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, 5(4), 1452-1472. https://doi.org/10.51594/estj.v5i4.1076

Appasaheb, N., & Prafull, M. (2024). Role of Web-Scale Discovery in the effective use of Electronic Resources. *Journal of Indian Library Association*, *60*(01), 24-37. https://doi.org/10.5860/crl-137

Balachandran, S., & Dominic, J. (2025). A comprehensive analysis of cloud computing models for academic library systems. *International Journal of Library and Information Science (IJLIS), 14*(1), 1-24. https://doi.org/10.5281/zenodo.14864318

Balachandran, S., Dominic, J., & Sivankalai, S. (2024). A Comparative Analysis of VPN and Proxy Protocols in Library Network Management. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).

Castelo, S. E. S., Apostol IV, R. J. L., Cortez, D. M. A., Dioses, R. M., Blanco, M. C. R., & Agustin, V. A. (2024). Modification of SHA-512 using Bcrypt and salt for secure email hashing. *Indonesian Journal of Electrical Engineering and Computer Science, 33*(1), 398-404. http://doi.org/10.11591/ijeecs.v33.i1.pp398-404

Chamoli, A., Kirsali, A., & Sharma, S. (2024). Cyber attack prevention method for enhanced privacy of patients digital healthcare data in smart hospitals. In *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)* (Vol. 1, pp. 54-59). IEEE. https://doi.org/10.1109/ICCPCT61902.2024.10672954

Chuquimarca, L., Torres, W., Sánchez, J., & Amaya, L. (2024). Implementation of a remote laboratory focused on the development of industrial automation practices. *Journal of applied research and technology*, *22*(4), 479-487. https://doi.org/10.22201/icat.24486736e.2024.22.4.2389

Diaz–Cacho, M., Falcón, P., Acevedo, J. M., & Domínguez, A. P. (2024). Educational project for remote access to industrial networks. In *2024 IEEE Global Engineering Education Conference (EDUCON)* (pp. 01-06). IEEE. https://doi.org/10.1109/EDUCON60312.2024.10578673

Elavarasan, S. R., Florence, S. M., & Natrajan, S. (2024). IPv6 Tunneling Using Peer-to-Peer VPN. In *2024 2nd International Conference on Networking and Communications (ICNWC)* (pp. 1-3). IEEE. https://doi.org/10.1109/ICNWC60771.2024.10537420

Fu, C., Wang, B., Liu, H., & Wang, W. (2024a). Software-defined virtual private network for SD-WAN. *Electronics*, *13*(13), 2674. https://doi.org/10.3390/electronics13132674

Fu, C., Wang, B., Wang, W., Mu, R., Sun, Y., Xin, G., & Zhang, Y. (2024b). A Generic High-Performance Architecture for VPN Gateways. *Electronics*, *13*(11), 2031. https://doi.org/10.3390/electronics13112031

Hamad, F., Al-Fadel, M., & Shehata, A. M. K. (2024). The level of digital competencies for the provision of smart information service at academic libraries in Jordan. *Global Knowledge, Memory and Communication*, *73*(4/5), 614-633. https://doi.org/10.1108/GKMC-06-2022-0131

Hunt, L. K. C., Cromwell, J. C., & Creel, S. (2024). Students with disabilities perceptions on the library and college: Systematic review and case study. *The Journal of Academic Librarianship*, *50*(1), 102827. https://doi.org/10.1016/j.acalib.2023.102827

Jabarali, A. K., Sathya Kumar, H., & Barak, Y. S. (2024). Analyzing the COVID-19 Pandemic's Effects on College Students: E-Learning Experience, Challenges and Resource Awareness. *Journal of Library & Information Services in Distance Learning*, 1-20. https://doi.org/10.1080/1533290X.2024.2332806

Kathuria, K., & Kaur, A. (2024). Use of E-ShodhSindhu in PG Colleges of Amritsar District: An Analytical Study. *Journal of Applied Information Science*, *12*(1).

Khan, S. A., & Shahzad, K. (2024). Key features of digital library management system (DLMS) for developing digital libraries: An investigation from LIS practitioners in Pakistan. *Journal of Librarianship and Information Science,* 56(1), 29-42. https://doi.org/10.1177/0961000622112703

Kılıç, C., Uzun, İ. B., Ardoğan, A. T., Saleem, W., & Sezen, A. (2024). Security Issues of Remote Work Environments and Alternative Solution Approaches. *International Journal of Multidisciplinary Studies and Innovative Technologies,* 8(1), 46-51.

Kishore, P., & Malarvel, M. (2024). Secure Remote Access to Local Network with Distributed Tunnel Management. *In 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ADICS58448.2024.10533475

Listiawan, I., Zaidir, Z., Winardi, S., & Diqi, M. (2024). Optimising Bcrypt Parameters: Finding the Optimal Number of Rounds for Enhanced Security and Performance. *Compiler*, *13*(1), 1-10. http://doi.org/10.28989/compiler.v13i1.2111

Molla, S., & Singh, S. (2024). Role of Information Technologies in the College Libraries Affiliated to Maulana Abul Kalam Azad University of Technology in West Bengal. https://doi.org/10.26761/IJRLS.10.2.2024.1748

Olabisi, P. O., Ogunkanmi, O. A., & Abdullahi, H. I. (2024). Development of a Generic On-Line Departmental E-Library using the Iterative Design Approach. *Arid Zone Journal of Engineering, Technology and Environment*, 20(1), 173-186.

Patel, D., Trivedi, D., Raval, U., & Dennisan, A. (2024). 2F-Authsys: A hyperlocal two-factor authentication system using Near Sound Data Transfer. *Journal of Applied Research and Technology*, *22*(2), 197-205. https://doi.org/10.22201/icat.24486736e.2024.22.2.2244

Scott, V. A. B., & Giancarlo, S. A. (2024). Designing the VPN with Top-Down to Improve Information Security. *International Journal of Advanced Computer Science & Applications*, 15(6). https://doi.org/10.14569/ijacsa.2024.0150620

Sharma, A., Thapliyal, S., Wazid, M., Mishra, A. K., Kumar, P., & Giri, D. (2024). A secure mechanism for password hash value generator with the security analysis of various hashing algorithms. In *2024 4th International Conference on Computer, Communication, Control & Information Technology (C3IT)* (pp. 1-6). IEEE. https://doi.org/10.1109/C3IT60531.2024.10829444

Sinha, P., & Ugwulebo, J. E. (2024). Digital literacy skills among African library and information science professionals–an exploratory study. *Global Knowledge, Memory and Communication*, *73*(4/5), 521-537. https://doi.org/10.1108/GKMC-06-2022-0138

Valks, M., Slot, R., Spoor, R., Wijenbergh, J., & Kooman, F. (2024). Peer-to-peer VPN solution for eduVPN using WireGuard.

Vásquez, D. A. P., & Izquierdo, J. F. L. (2024). A Literature Review Focused on Current Trends and Practices in Web Application Development. In *X Congreso Internacional de Ciencia, Tecnología e Innovación para la Sociedad (CITIS 2024)*.