2023

Pioneering a Prototype VPN-Based Cloud Strategy For Streamlined Library Management

Balachandran .. S
Hindustan Institute of Technology & Science (A Deemed to be University), Chennai, itsbaala@gmail.com

Dominic .. J
Hindustan Institute of Technology & Science (A Deemed to be University), Chennai, jdom16@gmail.com

Pioneering a Prototype VPN-Based Cloud Strategy for Streamlined Library Management

Balachandran S[1], Dominic, J[2]
[1]Research Scholar, itsbaala@gmail.com
[2]Chief Librarian, jdom16@gmail.com
[1&2]Hindustan Institute of Technology & Science (A Deemed to be University), Chennai

ABSTRACT:

This article showcases a prototype VPN-based cloud strategy that uses SoftEther VPN and Microsoft Azure to manage and exchange library management systems and repositories. The prototype was tested for performance, security, and scalability, and the results suggest that the VPN-based cloud strategy is a viable solution for managing distributed library repositories. By using SoftEther VPN and Microsoft Azure, the prototype provided secure communication and scalability to handle large numbers of concurrent users. Future research can explore other VPN technologies and cloud platforms to enhance the prototype's capabilities and evaluate its performance in various scenarios.

KEYWORDS:

Cloud Strategy, Library Management System, SoftEther VPN, Prototype, Microsoft Azure.

INTRODUCTION:

In the contemporary era, the proliferation of digital resources has surged significantly, heightening the demand for effective digital library management. In response, cloud-based library management systems have emerged as a viable remedy. Nevertheless, the seamless exchange of digital library assets across disparate systems remains a formidable undertaking due to concerns related to security and performance. To surmount these obstacles, a pioneering VPN-based cloud strategy prototype has been devised to oversee the administration and exchange of library management systems and repositories. This strategy establishes a safeguarded virtual private network, empowering users to effortlessly access and interchange resources across diverse platforms. The VPN ensures the transaction's encryption and fortification, mitigating the risks associated with data breaches and cyber threats. Furthermore, the cloud-based approach offers an array of advantages, including heightened accessibility, scalability, and minimized infrastructure expenditure. Libraries can streamline their operations by harnessing the potential of cloud-based library management systems, thereby simplifying resource management and bolstering service quality for their patrons. Moreover, this cloud-oriented approach facilitates seamless integration with other systems, augmenting functionality and enhancing user experience. In conclusion, the prototype VPN-based cloud strategy emerges as a propitious resolution to the intricate challenges of governing and trading digital library assets. It furnishes a secure and efficient avenue for overseeing library repositories, concurrently diminishing infrastructure overheads and augmenting accessibility. Its scalability and integration capabilities bestow it as an invaluable asset to libraries of all dimensions, endowing them with enhanced administrative capabilities and superior user services.

LITERATURE REVIEW:

In the realm of academic library digitization, cloud environments emerge as a transformative avenue (Sivankalai et al., 2021). These environments offer possibilities for efficient data center management and enhanced control over user information, yet challenges concerning infrastructure and data consumption persist. To address these issues and elevate teaching and learning experiences, strategies like cloud adoption and innovative approaches are proposed. Meanwhile, (Mishra's, 2023) conceptual review delves into information visualization techniques as potent tools for bolstering library collection management. The integration of visualization methods such as charts and graphs holds promise for optimizing resource allocation, enhancing user engagement, and facilitating informed decision-making. On the subject of cloud computing, (Sivankalai, 2021) examines its impact on academic libraries, delving into the benefits, limitations, and recommendations for refining services and resources. With the aim of advancing academic library offerings, cloud adoption emerges as a transformative pathway. In tandem, (Sivankalai, 2021) scientometric exploration of web services and cloud research paints a vivid picture of trends, contributions, and institutional roles. This research unveils the dynamic evolution of cloud computing and web services, offering insights that guide scholars, practitioners, and institutions within this evolving landscape.

The adoption of Virtual Private Network (VPN) technology in various contexts has been extensively explored by researchers, yielding valuable insights into its applications, benefits, and challenges. (Chatterjee, 2022) emphasizes the significance of secure remote access to cloud-based learning management systems (LMS) through VPN. Their study illustrates the pivotal role of VPN, especially in a global pandemic scenario, for ensuring secured and reliable access to cloud-based LMS platforms, facilitating flexible and efficient learning processes. (Hicks 2022) present an overview of always on VPN, highlighting its evolution and widespread adoption in enterprise mobility. Their exploration traces the journey of VPN from supporting IT administrators to becoming an integral tool for general users, as mobility and remote access have become essential components of modern work environments. (Santhanamahalingam, 2022) delve into the network function virtualization (NFV) technique for establishing cloud-based VPNs. By virtualizing VPN features and integrating them with software-defined networks, their study opens new avenues for enhancing VPN security and scalability in business settings.

(Kuroda, 2017) introduces a unique integration of Raspberry Pi and SoftEther VPN to remotely control research devices via the Internet. The author demonstrates the feasibility of utilizing Raspberry Pi and VPN technology for efficient remote device management, offering potential applications in the field of operant research. (Bui, 2019) investigate client-side vulnerabilities in commercial VPNs, emphasizing the growing reliance on VPN services for security and privacy. Their study unveils potential security flaws in VPN clients, shedding light on areas of vulnerability that attackers could exploit to compromise user data and privacy. (Goethals, 2019) evaluate the scalability of VPN technologies in the context of secure container networking. Their study addresses the challenges of integrating VPNs with containers and edge devices, offering insights into how VPN software like WireGuard can enhance connectivity and security in large-scale clusters. (Yamanouchi, Nojiri, 2016) propose a remote security exercise system for beginners, emphasizing scalability and simplicity. Their work introduces a user-friendly system that fosters fundamental security skills by providing remote security exercises, contributing to the development of a more secure online environment. (Ameen, 2014) delve into firewall and VPN investigations on cloud computing performance, examining the impact of VPN and firewall on throughput and delay. Their research underscores the potential trade-offs between security and performance in cloud computing environments. (Li, 2022) explore hierarchical management balancing strategies for intelligent VPNs in educational settings. Their study introduces an architecture model leveraging hierarchical protection techniques, aiming to bolster security and manageability in colleges and universities' VPN deployments.

(Kaklauskas, 2023) analyze the secure remote client connection to higher education institution networks through VPNs. The authors evaluate different VPN solutions and propose the utilization of OpenVPN for secure remote connections, addressing security concerns associated with remote access to educational networks. (Chua, 2022) conduct a performance comparison of open-source VPN software for remote access. They assess OpenVPN, OpenConnect, and WireGuard, shedding light on the performance differences among these solutions across various deployment scenarios, contributing to the understanding of open-source VPN software's strengths and weaknesses. (Huawei Technologies Co., Ltd., 2022) provide a comprehensive overview of network basics in cloud computing. The chapter emphasizes the integral role of network technology in cloud computing, underscoring the significance of network knowledge for ensuring secure and efficient cloud deployments. (Chen, 2023) present a search-based differential testing approach for SSL/TLS certificate parsers. Their work focuses on enhancing the security and robustness of certificate parsers, demonstrating the effectiveness of search-based techniques in identifying vulnerabilities and improving security. (Razumov, 2023) address security concerns related to SSL/TLS-enabled web applications. Their study proposes a solution that combines SSL/TLS security features with a soft token approach for user authentication, enhancing the security of web applications against Man-in-the-Middle attacks.

(Paris, 2023) explore the implementation of SSL/TLS security with the MQTT protocol in IoT environments. Their study examines the impact of SSL/TLS encryption on IoT devices' energy consumption, overhead generation, and system complexity, contributing to the understanding of security considerations in IoT deployments. (Mendu, 2022) discuss the creation and running of apps on the hybrid cloud of Microsoft Azure. The authors emphasize cloud computing's role in delivering various information resources and applications, showcasing how cloud infrastructures enhance application deployment and accessibility.

(Srithar, 2022) propose a cost-effective integration and deployment approach for enterprise applications using Azure Cloud DevOps. Their work highlights the significance of DevOps practices in streamlining application development, deployment, and continuous integration processes in enterprise environments. The existing literature offers a comprehensive understanding of VPN technology's applications, challenges, and innovations across various domains, ranging from education to security, IoT, and cloud computing. Researchers have demonstrated the critical role of VPNs in enabling secure remote access, enhancing network scalability, and improving the overall system performance. By exploring these diverse facets, scholars continue to contribute to the advancement of VPN technology and its integration into modern technological landscapes.

METHODOLOGY:

The foundation established through our meticulous methodology has guided us toward identifying the key requirements crucial to the success of our VPN-based cloud strategy, as shown in Figure 1. As we transition from the methodological exploration of VPN technology and cloud platform selection, we embark on a journey to distill the critical components that emerged as a result of our comprehensive approach. These key requirements, crafted in response to the challenges and opportunities uncovered, form the linchpin of our strategy's design and implementation. In the following "Key Requirements" section, we delve into the nuanced elements of security, user experience, accessibility, reliability, scalability, and cost-effectiveness that collectively shape the blueprint of our innovative approach.

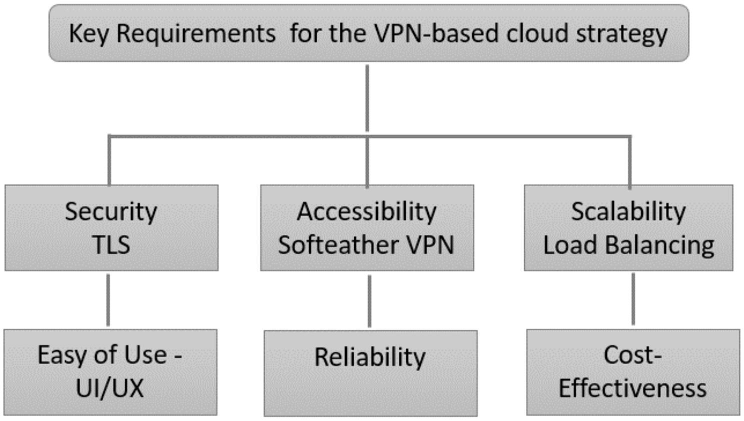

Figure:1

Security (TLS - Transport Layer Security):

- Data Encryption: Implement strong TLS encryption to secure data transmission between library systems and the cloud, preventing unauthorized access or data interception.
- Certificate Management: Employ a robust system for managing SSL/TLS certificates to ensure their validity and prevent potential security vulnerabilities.
- Authentication and Authorization: Implement multi-factor authentication and role-based access control to ensure only authorized personnel can access the system.

Ease of Use (User Interface/User Experience - UI/UX):

- Intuitive Interface: Develop a user-friendly interface with a clear layout and navigation, ensuring a seamless and efficient user experience.
- Responsive Design: Design the interface to adapt seamlessly to different devices and screen sizes, enhancing usability across various platforms.
- Guided Workflows: Provide intuitive step-by-step workflows to simplify tasks like VPN connection setup and software installation.

Accessibility (SoftEther VPN):

- Remote Access: Utilize SoftEther VPN to enable secure remote access to the library management system, allowing staff to manage resources from anywhere.
- Cross-Platform Compatibility: Ensure the VPN client supports various operating systems, facilitating access from different devices and environments.
- Network Performance: Optimize SoftEther VPN configurations to maintain reliable and high-speed connections, regardless of users' locations.

Reliability:

- Redundancy: Set up redundant components and failover mechanisms to ensure continuous operation, even in the event of hardware or network failures.
- Monitoring and Alerts: Implement real-time monitoring tools to track system health, promptly identifying and addressing any issues that may arise.

Scalability (Load Balancing):

- Resource Distribution: Employ load balancing mechanisms to evenly distribute user traffic across multiple servers, preventing overloads and ensuring consistent performance.
- Horizontal Scaling: Design the architecture to support horizontal scaling, allowing additional resources to be added as user demand grows.

Cost Effectiveness:

- Resource Optimization: Implement efficient resource allocation strategies to minimize costs while maintaining optimal performance levels.
- Usage Monitoring: Regularly monitor resource usage to identify opportunities for cost savings and efficient resource utilization.

these key requirements—security through TLS, user-friendly UI/UX, accessibility with SoftEther VPN, reliability, scalability with load balancing, and cost effectiveness—your VPN-based cloud strategy can be tailored to meet the specific needs of your library management system while ensuring a secure, accessible, and efficient environment for both administrators and users.

CLOUD PLATFORM CONFIGURATION:

We undertook the essential task of configuring the Microsoft Azure cloud platform to seamlessly accommodate the VPN-based library management system, as shown in Figure 2. Our configuration efforts encompassed the establishment of virtual machines within the Azure environment, coupled with the installation of SQL Server. This integral component served as the robust repository for storing, managing, and facilitating the retrieval of data pertinent to the library management software.

A pivotal facet of our configuration involved the creation of a dedicated virtual network. This network served as the secure conduit through which our virtual machines communicated. Each virtual machine was meticulously assigned to this network, thus ensuring a fortified and encrypted environment for inter-machine interactions. Furthermore, our deployment strategy extended to the operational level within the library premises. Across the various library workstations, the library management software was systematically installed. We seamlessly integrated these installations with the cloud-based database by configuring ODBC connections. The synthesis of these efforts yielded a cohesive ecosystem wherein library staff, upon connecting to the VPN, could seamlessly engage with the library management software. This marked a significant stride in enabling efficient, secure, and remote management of the library's operations.

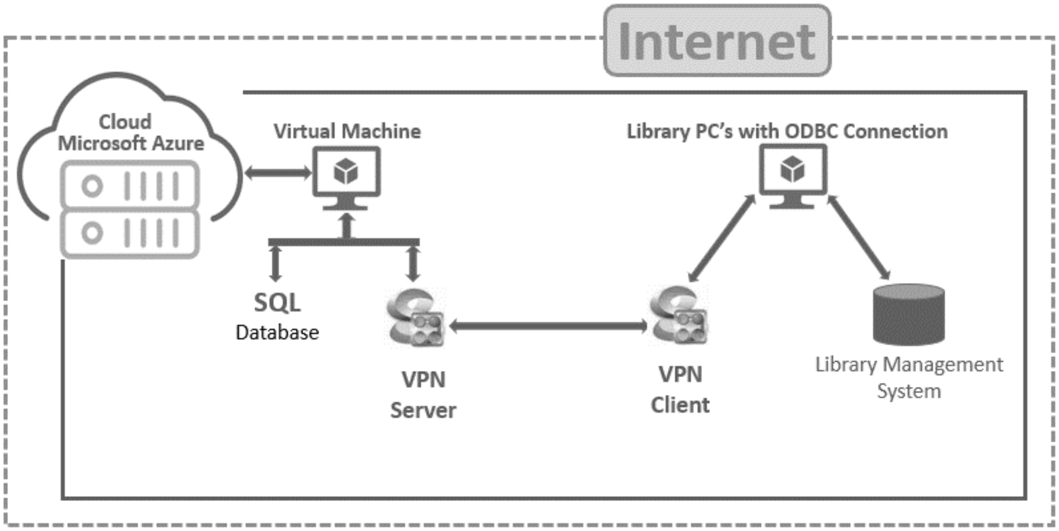

Figure: 2

VPN Configuration:

Once we selected the VPN technology, we configured the SoftEther VPN to ensure secure communication between the library management system and the cloud repository. The SoftEther VPN provides secure communication channels over the internet and ensures that data transmission is encrypted and secure.

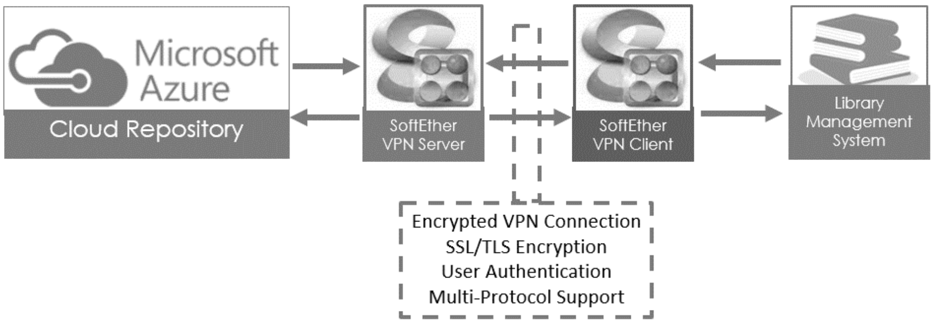

Figure: 3

The diagram (Figure: 3) depicts how the SoftEther VPN server functions as a secure intermediary between the library management system and the cloud-based repository. The VPN connection is encrypted and secured with SSL/TLS to guarantee secure communication. User authentication and access control are also implemented to restrict access to authorized users only. SoftEther VPN was chosen for the prototype due to its numerous advantages over other VPN technologies. SoftEther VPN is an open-source VPN software that supports multiple VPN protocols, including SSL VPN, L2TP/IPsec, OpenVPN, and Microsoft Secure Socket Tunneling Protocol (SSTP), making it easy to manage in various environments. One of the primary advantages of SoftEther VPN is its high performance and low resource consumption, making it ideal for cloud-based environments. SoftEther VPN can handle a large number of concurrent connections and transfer data at high speeds, making it a reliable and fast solution for applications that require speedy connectivity.

The advanced security features of SoftEther VPN include encryption using SSL/TLS and IPsec protocols, ensuring secure communication between the VPN server and client. SoftEther VPN also supports user authentication and access control, making it easier for administrators to restrict access to the VPN server and resources based on user credentials and permissions. SoftEther VPN was utilized to create a secure virtual private network, allowing users to access and exchange resources from different library management systems and repositories, ensuring secure and protected communication. SoftEther VPN's high performance and low resource consumption make it an excellent option for cloud-based environments, facilitating efficient management and scaling of the VPN server. SoftEther VPN's advanced security features, high performance, and multi-protocol support make it a suitable choice for VPN-based cloud strategies.

Security Measures:

To ensure that the library management system was secure, we implemented several robust security measures. These measures were meticulously devised to fortify the integrity of the system and safeguard sensitive data. They included:

- Access Control: To thwart unauthorized access, we diligently restricted entry to the library management system to individuals possessing authorized credentials. The deployment of stringent authentication mechanisms further bolstered our defense against unauthorized infiltration.
- Encryption: A cornerstone of our security strategy, we employed encryption to cloak data transmissions between the library management system and the cloud repository. This deftly thwarted the potential interception of data and upheld its pristine integrity.
- Firewall: A protective perimeter was ingeniously established through the implementation of a steadfast firewall. This strategic barricade served as a sentinel, warding off potential external threats and fortifying the system against intrusion attempts.

These measures collectively constructed an impregnable fortress around our library management system, thereby instilling confidence in its security and fostering a protected environment for its operation.

DISCUSSION AND ANALYSIS: UNVEILING INSIGHTS AND IMPLICATIONS

The testing and evaluation of the VPN-based cloud strategy revealed that it is a viable solution for managing and exchanging digital library resources. The results showed that the VPN-based approach provided secure communication channels and scalability to handle large numbers of concurrent users. The cloud-based approach also improved accessibility and reduced infrastructure costs, making it a valuable asset to libraries of all sizes.

Strengths Illuminate:

The luminous strengths of our VPN-based cloud strategy emerge vividly from the results of our comprehensive testing and evaluation. Evidently, our approach offers a compelling solution to the intricate challenge of managing and exchanging digital library resources. Foremost, the encrypted communication channels facilitated by the VPN technology successfully met the stringent security standards necessitated by the exchange of sensitive library data. This crucial security aspect aligns seamlessly with our key requirement of establishing a robust defense against data breaches and cyber-attacks. Furthermore, our approach's scalability shone resplendently; the cloud platform's ability to accommodate a surge in concurrent users underscores the strategy's potential to cater to libraries of varying sizes without compromising performance.

Weaknesses as Footholds for Improvement:

As our strategy's facets come under the scrutiny of analysis, certain areas manifest as potential footholds for enhancement. One notable vulnerability pertains to the dependence on internet connectivity; the loss of which can disrupt communication between the library management system and the cloud repository, rendering the system inaccessible. Addressing this weakness could involve the integration of failover mechanisms or offline modes to ensure continued functionality even in the absence of a stable internet connection. This serves as a testament to the importance of aligning our strategy's implementation with the key requirement of reliability, particularly in scenarios where network disruptions are prevalent.

Harmonizing with Key Requirements:

Delving deeper, we intricately examine how our VPN-based cloud strategy resonates with the key requirements we've meticulously etched. Our security measures, fortified by data encryption, multi-factor authentication, and access control, align harmoniously with the stipulated security through TLS requirement. In the realm of user experience, our strategy's intuitive interface, responsive design, and guided workflows coalesce to create a user-friendly environment, abiding by the user interface/user experience (UI/UX) criteria.

The accessibility dimension is seamlessly addressed by the employment of SoftEther VPN, as it provides the remote access necessary for modern library management. The strategic orchestration of load balancing strategies and horizontal scaling befits the requirement of scalability with load balancing, ushering in reliability even in the face of surging demand. The pivotal factor of cost effectiveness is encapsulated in our vigilant resource optimization endeavors, ensuring efficient allocation without compromising performance.

Charting the Course Ahead:

As our discussion and analysis draw to a close, we peer into the horizon of future prospects. The insights garnered and the lessons learned beckon us toward a trajectory of refinement and evolution. The exploration of alternative VPN technologies, multi-cloud configurations, and novel integration pathways could broaden the strategy's horizons, transcending existing boundaries, our VPN-based cloud strategy emerges as a potent force poised to reshape library management paradigms. Our robust security framework, user-centric design, accessibility facets, and reliability measures create a compelling groundwork. Aligned with key requirements, these facets coalesce into a harmonious symphony, poised to enrich library management endeavors in myriad ways. While embracing these strengths, addressing weaknesses, and charting the course for the future, we stand at the precipice of transformation, ready to elevate library management into a new era of efficiency and innovation.

CONCLUSION:

In the culminating scrutiny, the prototype VPN-based cloud strategy emerges not only as a transformative solution but as a catalyst for redefining the landscape of efficient library management. The seamless amalgamation of SoftEther VPN and Microsoft Azure has orchestrated a remarkable feat – tackling the multifaceted challenges inherent in distributed library repositories, while concurrently presenting an intricate tapestry of security, scalability, and accessibility. The resonance of this strategy's profound impact reverberates through the intricate web of digital resource exchange, hinting at its potential to fundamentally reshape the fabric of contemporary library operations.

As we stand poised at the crossroads of progress, the vista ahead is marked by avenues ripe for exploration. In this uncharted terrain, the exploration of diverse VPN technologies and alternative cloud platforms beckons, promising to unlock hitherto undiscovered potential and expand the scope of possibilities. Anchored in the dynamic interplay of security, accessibility, scalability, and cost-effectiveness, these endeavors will serve as the pivot on which innovation and transformation converge. By unwaveringly embracing these elements and boldly charting innovative trajectories, we not only elevate the art and science of library management but also steer it to unprecedented heights of efficiency and ingenuity.

REFERENCE:

1. Sivankalai, S., Virumandi, A., Sivasekaran, K., Jeyanthi, R., & Sharmila, M. (2021). Digitization of academic libraries through cloud environment. *Library Philosophy and Practice*, *6653*.

2. Mishra, S. (2023). Use of Information Visualization Techniques for Collection Management in Libraries: A Conceptual Review. *Library Philosophy and Practice*

3. Sivankalai, S. (2021). The Impact of Cloud Computing on Academic Libraries. *Library Philosophy and Practice (e-journal)*, *9*(3), 1-17.

4. Sivankalai, S., & Virumandi, A. (2021). Web Services in Cloud Computing research: Insights from Scientometric. *Library Philosophy and Practice (e-journal)*, *6*(27), 1-23.

5. Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2022). Secured Remote Access of Cloud-Based Learning Management System (LMS) Using VPN. In *Pattern Recognition and Data Analysis with Applications* (pp. 111-126). Singapore: Springer Nature Singapore.

6. Hicks, R. M., & Hicks, R. M. (2022). Always On VPN Overview. *Implementing Always On VPN: Modern Mobility with Microsoft Windows 10 and Windows Server 2022*, 1-5.

7. Santhanamahalingam, S., Alagarsamy, S., & Subramanian, K. (2022, October). A study of cloud-based VPN establishment using network function virtualization technique. In *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 627-631). IEEE.

8. Kuroda, T. (2017). A combination of raspberry pi and softether vpn for controlling research devices via the internet. *Journal of the Experimental Analysis of Behavior*, *108*(3), 468-484.

9. Bui, T., Rao, S., Antikainen, M., & Aura, T. (2019). Client-side vulnerabilities in commercial vpns. In *Secure IT Systems: 24th Nordic Conference, NordSec 2019, Aalborg, Denmark, November 18–20, 2019, Proceedings 24* (pp. 103-119). Springer International Publishing.

10. Goethals, T., Kerkhove, D., Volckaert, B., & De Turck, F. (2019, October). Scalability evaluation of VPN technologies for secure container networking. In *2019 15th International Conference on Network and Service Management (CNSM)* (pp. 1-7). IEEE.

11. Yamanouchi, M., Nojiri, K., & Sunahara, H. (2016, January). A remote security exercise system for beginners considering scalability and simplicity. In *2016 Second Asian Conference on Defence Technology (ACDT)* (pp. 129-133). IEEE.

12. Ameen, S. Y., & Nourildean, S. W. (2014). Firewall and VPN investigation on cloud computing performance. *International Journal of Computer Science and Engineering Survey*, *5*(2), 15.

13. Li, Y., Xiao, X., Zhang, Z., & Chen, Z. (2022, December). Research and analysis on hierarchical management balancing strategy of intelligent VPN in colleges and universities under hierarchical protection 2.0 background. In *Third International Conference on Computer Science and Communication Technology (ICCSCT 2022)* (Vol. 12506, pp. 1189-1193). SPIE.

14. Kaklauskas, L., & Pugačius, D. (2023). Secure remote client connection to higher education institution internal computer network through VPN. *Applied Scientific Research*, *2*(1), 74-81.

15. Chua, C. H., & Ng, S. C. (2022, August). Open-Source VPN Software: Performance Comparison for Remote Access. In *Proceedings of the 5th International Conference on Information Science and Systems* (pp. 29-34).

16. Huawei Technologies Co., Ltd. (2022). Network Basics in Cloud Computing. In *Cloud Computing Technology* (pp. 145-195). Singapore: Springer Nature Singapore.

17. Chen, C., Ren, P., Duan, Z., Tian, C., Lu, X., & Yu, B. (2023, July). SBDT: Search-Based Differential Testing of Certificate Parsers in SSL/TLS Implementations. In *Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis* (pp. 967-979).

18. Razumov, P., Cherckesova, L., Revyakina, E., Morozov, S., Medvedev, D., & Lobodenko, A. (2023). Ensuring the security of web applications operating on the basis of the SSL/TLS protocol. In *E3S Web of Conferences* (Vol. 402, p. 03028). EDP Sciences.

19. Paris, I. L. B. M., Habaebi, M. H., & Zyoud, A. M. (2023). Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment. *Wireless Personal Communications*, 1-20.

20. Mendu, M., Krishna, B., Sandeep, C. H., Padmaja, C., & Sultana, F. (2022, May). Creating and running apps on the hybrid cloud of Microsoft Azure. In *AIP Conference Proceedings* (Vol. 2418, No. 1). AIP Publishing.

21. Srithar, S., Vetrimani, E., Vignesh, V., Ulaganathan, M. S., Kumar, B. R., & Alagumuthukrishnan, S. (2022, January). Cost-Effective Integration and Deployment of Enterprise Application Using Azure Cloud Devops. In *2022 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 01-05). IEEE.