Learning Platform for Network Segmentation Education

Sam Woodall
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

Suhair Amer
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

Ridam Kaphle
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

ABSTRACT
Network segmentation is a fundamental cybersecurity practice that enhances network security by dividing a network into smaller, isolated segments to reduce the risk of unauthorized access and limit the spread of cyber threats. However, understanding its concepts and practical applications can be challenging for beginners due to the technical nature of the subject. This study presents the development of a web-based learning platform designed to provide an interactive and engaging approach to learning network segmentation. The platform incorporates structured learning modules, quizzes for knowledge assessment, and a gamification system that awards badges to motivate users and encourage continuous learning. Developed using modern web technologies, the system emphasizes usability, flexibility, and an intuitive user interface to improve the overall learning experience. The platform enables learners to study network segmentation concepts at their own pace while tracking their progress through achievements and assessments. Initial evaluations indicate that the integration of interactive content and gamification enhances user engagement and knowledge retention compared to traditional learning approaches. The developed platform demonstrates the potential of web-based educational systems in supporting cybersecurity education and promoting effective learning of network segmentation concepts.

Keywords
Network Segmentation, Cybersecurity Education, Web-Based Learning, Gamification, Interactive Learning Platform.

1. INTRODUCTION
Network segmentation is a key cybersecurity technique used to improve security by dividing a network into smaller, isolated segments. Despite its importance, it is often difficult for beginners to understand due to its technical complexity. This paper presents the development of a web-based learning platform designed to teach network segmentation through interactive lessons, quizzes, and gamification features such as badges. The system aims to enhance learner engagement and understanding by combining structured educational content with immediate feedback and progress tracking. The platform is designed to be responsive, user-friendly, and accessible through modern web browsers.

2. LITERATURE REVIEW
This paper provides innovative solutions to overcome the weaknesses of today's communication systems employed on battlefields, namely their flat structure, lack of network segmentation and vulnerability against cyber-attacks or poor network performance. The researchers suggest building network slicing-based architecture as an improvement of 5G communication systems. This framework comprises several segments, including intelligent network controller, decision support module, and a network slice orchestrator, allowing the creation of several secure virtual networks with high level of isolation from the physical one. As one of the innovations proposed by this paper, it should emphasize the role of effective network segmentation. According to the researchers' claims, network slicing can have two positive effects on security and quality of services provided by segmented networks in terms of mission success and protection from various types of cyber threats. In addition, it is stated that software defined networking, intrusion detection mechanisms and artificial intelligence-based models may contribute to network's reliability and robustness. However, some concerns associated with the development of such network architecture should be pointed out, including efficient design of decision-making systems, seamless integration of physical and virtual networks, and normal network state identification for abnormality detection [1]. This paper explains how network slicing can be used in 5G systems to support different types of services with very different requirements on the same network. The authors describe network slicing as creating multiple isolated virtual networks that run on a shared physical infrastructure, where each slice is designed for a specific use case like healthcare, IoT, or mobile broadband. A major focus of the paper is on the role of Software Defined Networking (SDN) and Network Function Virtualization (NFV), which together provide flexibility, programmability, and efficient resource management. The paper also explains important concepts like virtualization, orchestration, and isolation, where orchestration helps manage resources dynamically and isolation ensures that one slice does not affect others in terms of performance or security. Additionally, the integration of SDN and NFV architectures is discussed as necessary for full implementation of network slicing, especially in managing lifecycle and resources of slices. However, the study also points out several challenges such as maintaining performance in shared infrastructure, handling complex resource management, ensuring strong security and privacy, and developing new business models. Overall, this paper is important because it provides a detailed foundation of how network segmentation through slicing can be achieved in 5G networks and what issues still need to be solved [2].

This paper provides a comprehensive review of security and privacy concerns with network slicing in 5G and future networks. It states that network slicing enables multiple logical networks to coexist in one physical network; however, it presents some risks and threats as well. The authors describe various security threats that include life cycle security, inter-slice and intra-slice security, and shared resources and management systems' threats. Furthermore, the paper mentions numerous possible attack models that include data leakage, denial-of-service attacks, impersonation attacks, and side-channel attacks due to insufficient isolation among slices. Moreover, it describes various technologies that offer high flexibility and agility, which increases attack surfaces, such as software-defined networking, network function virtualization, and cloud computing. To solve these issues, the paper proposes various strategies, such as

utilizing artificial intelligence in security, employing blockchain technology, providing enhanced identity authentication mechanisms, and ensuring proper isolation among slices. This paper is valuable because it outlines the pros and cons of network segmentation using slicing and identifies the gaps for further research [3]. This research paper provides information about the importance of implementing network segmentation in the field of Industrial Internet of Things for improving their security. According to the authors, network segmentation refers to the division of the network into several sections where separate security policies and access control can be implemented for each segment in order to protect critical information and minimize the risk of any potential attacks. In addition to that, it is also mentioned that IIoT environments often have numerous devices in place, which contribute to higher vulnerability to attacks. Therefore, there is a need to implement some measures to minimize this problem, among which are micro-segmentation, firewall, network access control, and identity management. Moreover, the benefits of such strategy include minimizing the attack surface, improving regulatory compliance, and facilitating device management. However, there are also certain challenges associated with segmentation, including increased complexity, costs, and possible performance problems when proper segmentation cannot be implemented. This research paper provides good insight into network segmentation in the context of IIoT environment and shows what its benefits and challenges can be [4].

The paper describes how SDN technology transforms the implementation of security in computer networks through the separation of control plane and data plane in networking and the centralization of the entire network. The centralization facilitates improved visibility and monitoring of the network infrastructure, traffic flow, potential threats, and implementation of dynamic security policies. The paper outlines how security functions may be integrated into software applications in an SDN environment, leading to enhanced flexibility and scalability compared to conventional networking systems. Nevertheless, the paper outlines some of the security challenges introduced by SDN technology such as attacks targeting the controller component of the SDN, DoS attacks, and threats in inter-layer communications within a network architecture. In particular, the authors indicate that SDN poses a variety of application-, control-, and data-plane security problems, and each type requires specific solutions. The paper discusses various approaches towards enhancing security in an SDN network architecture such as access control, authentication mechanisms, distribution of controllers, and traffic analysis. Overall, the paper provides valuable insights regarding the security challenges associated with SDN technologies [5]. This paper provides a detailed overview of SDN by explaining its architecture, key components, and major research challenges. It discusses how traditional networks are complex due to tightly connected control and data planes, and how SDN improves this by separating them and centralizing control through a controller. The paper explains the three main layers of SDN application, control, and infrastructure and how they interact using different interfaces, which makes network management more flexible and programmable. It also introduces a layered taxonomy that organizes research issues such as performance, scalability, security, and correctness across these layers, helping researchers understand where problems exist. The authors further describe different SDN controllers, programming approaches, and real-world use cases, while also highlighting challenges like controller bottlenecks, flow table limitations, and policy conflicts. In addition, the paper explains how concepts like network virtualization and centralized control can improve innovation but also create new risks if not properly managed. Overall, this paper is important because it gives a structured understanding of SDN and clearly organizes existing research along with future directions [6].

This paper focuses on the problem of security policy conflicts in Software Defined Networking, especially in distributed cloud environments where multiple controllers and applications interact. It explains that because SDN allows dynamic insertion of flow rules by different modules or tenants, conflicts can easily occur, which can reduce security and cause incorrect network behavior. To solve this, the authors propose a framework called Brew that detects and resolves conflicts between flow rules, including complex cases like cross-layer conflicts and conflicts across multiple controllers. The framework works by extracting flow rules, analyzing them, and then classifying conflicts into different types such as redundancy, shadowing, correlation, and imbrication. It also introduces methods to automatically resolve some conflicts and provides strategies like priority-based decisions and security rules to handle more complex cases. In addition, the paper highlights how visualization tools can help administrators understand and manage these conflicts better in large systems. Overall, this work is important because it shows a structured way to manage network segmentation and security policies in SDN environments, making the system more reliable and easier to maintain [7]. This study explores how the emergence of ZTA is shifting the approach to cybersecurity away from the assumption that users or devices that are inside the network are trustworthy. The paper describes how zero trust architecture adheres to the concept of "never trust, always verify." All user access requests must therefore be verified and validated. IAM, MFA, ZTNA, and micro-segmentation are some of the critical aspects of ZTA. The paper explains that micro-segmentation is essential for limiting attacker lateral movement, which is directly relevant to network segmentation concepts. Additionally, it discusses methods such as least privilege access control and constant verification as strategies for implementing ZTA. The paper acknowledges potential challenges such as implementation costs and the complexities associated with integrating legacy systems. This paper is significant since it provides insights into why ZTA is important. This includes its capacity to enhance cyber-security in hybrid and cloud environments [8].

This paper focuses on improving network segmentation in Industrial IoT environments using a Zero Trust approach. It explains that traditional segmentation methods are often static, centralized, and not suitable for complex IIoT systems where devices are diverse and constantly changing. To solve this, the authors propose a framework called EFAH-ZTM, which combines federated learning, hypergraph modeling, clustering techniques, and explainable AI. The framework teaches device behavior without sharing raw data, which helps maintain privacy, and then groups devices into micro-segments based on their communication patterns. It also introduces a risk-based policy system that decides whether to allow or block communication between devices. One important contribution is the use of explainable AI methods like LIME and SHAP to show why certain decisions are made, making the system more transparent and trustworthy. The results show that this approach can create highly accurate and secure segmentation with very low errors and strong separation between normal and malicious behavior. Overall, this paper is important because it shows a more advanced and practical way to implement network segmentation using Zero Trust principles in modern IIoT environments [9]. The paper provides information on the utilization of network segmentation as a security strategy employed in enterprise systems. Segmentation is defined as partitioning a network into smaller isolated segments that limit the spread of attacks in large

enterprises and help prevent lateral movement in the organization. The research methodology of the paper consists of a literature review, cases studies, and data analysis to evaluate the effectiveness of the segmentation strategy. Some advantages of segmentation include better access control, protecting confidential information, increasing compliance with regulatory policies, and enhancing the ability of companies to monitor their network activities. At the same time, there are several issues associated with the employment of segmentation in enterprise systems, including its complexity, high costs, management overhead, and possible misconfiguration. In addition, recent technological changes, namely, cloud-based systems and the Internet of Things (IoT), have made network segmentation even more necessary in order to secure corporate networks against cyber threats. Therefore, this paper is significant for furthering the understanding of the importance of network segmentation [10].

This paper presents a modern network design that uses micro-segmentation and zero trust principles to secure cloud environments. It explains that traditional network security methods are not enough for today's distributed systems, especially with the rise of cloud computing, microservices, and multi-cloud architectures. The authors propose a layered architecture that separates networks at multiple levels, including business functions, resources, and applications, to provide better control and isolation. The design uses open-source tools like Istio and Calico to enforce security policies such as authentication, authorization, and encrypted communication between services. It also highlights how service mesh technology helps manage communication between different components while maintaining security. The paper demonstrates through a prototype that micro-segmentation can effectively control traffic, restrict unauthorized access, and enforce secure communication using techniques like mutual TLS. However, it also mentions that managing such systems can become complex due to multiple layers of policies and configurations. Overall, this paper is important because it shows how network segmentation can be applied in cloud environments using zero trust principles to achieve scalable and secure architectures [11]. This paper focuses on improving network security by moving protection closer to devices, especially in IoT environments. It explains that traditional centralized security methods like firewalls and IDS are no longer enough because modern networks include many untrusted devices such as IoT gadgets, mobile devices, and cloud-connected systems. To solve this, the authors propose a distributed architecture where security policies are enforced at the network edge using components like traffic policers, a policy database, and a network discovery system. The system uses DNS as a distributed database to store and share security policies, which allows all devices in the network to follow consistent rules. It also supports fine-grained control by applying different policies based on device type and behavior, which is similar to micro-segmentation. The paper highlights that this approach can reduce unwanted traffic, limit internal threats, and improve overall network visibility. However, it also mentions challenges such as handling heterogeneous devices, dependency on accurate device discovery, and managing complex policies. Overall, this paper is important because it shows how network segmentation can be improved by combining edge-based security and distributed policy enforcement in modern IoT networks [12].

This paper provides a detailed study of how network slicing is implemented in modern open radio access networks. It explains that O-RAN is designed to make network systems more flexible, open, and intelligent by separating hardware and software and allowing multiple vendors to work together. The paper highlights network slicing as an important concept where a single physical network is divided into multiple virtual networks, each designed for different applications like high-speed internet, low-latency communication, or IoT services. It also discusses how technologies like SDN, NFV, and AI/ML help manage and optimize these slices efficiently. The study explores different deployment models, architectures, and real-world use cases, showing how slicing can support various industries with different requirements. At the same time, it points out challenges such as resource allocation, maintaining isolation between slices, managing complexity, and ensuring interoperability between different systems. Overall, this paper is important because it gives a complete understanding of how advanced network segmentation through slicing works in 5G and future networks, along with its benefits and challenges [13]. This paper explains how network slicing works across the entire 5G system, including radio access, core, and transport networks. It highlights that traditional networks cannot handle the diverse needs of modern applications, so network slicing allows multiple virtual networks to run on the same physical infrastructure with different performance requirements. The paper focuses on building a complete end-to-end (E2E) model by combining different standards from organizations like ETSI, 3GPP, and IETF, since each of them only covers part of the system. It describes the overall architecture, key components like tenants, providers, and agents, and explains how a network slice is created, deployed, and managed throughout its life cycle. The paper also discusses different approaches such as service graphs and templates for requesting slices, along with detailed models for RAN, core, and transport domains. Additionally, it highlights challenges like lack of standardization, complexity in coordination across domains, and difficulty in managing resources efficiently. Overall, this paper is useful because it gives a complete understanding of how 5G network slicing works end-to-end and what challenges still need to be solved for real-world implementation [14].

This paper explains how network segmentation has evolved from traditional methods like VLANs and firewalls to more advanced micro-segmentation and Zero Trust approaches. It highlights that older security models based on fixed network boundaries are no longer effective in modern environments with cloud systems, containers, and dynamic workloads. The paper provides a detailed analysis of different micro-segmentation techniques, including host-based, network-based, container-native, and kernel-level approaches like eBPF, showing how each method works and where it is used. It also explains how Zero Trust principles have made micro-segmentation more important by requiring continuous verification and identity-based access instead of relying on network location. Additionally, the study discusses real-world challenges such as performance overhead, policy complexity, and difficulty in managing large-scale systems, even though newer technologies have improved efficiency. The paper also identifies different implementation patterns and compares their advantages and limitations based on factors like scalability, performance, and security. Overall, this paper is important because it shows the transition toward AI-driven and identity-based segmentation and helps understand how modern networks can be secured more effectively using micro-segmentation and Zero Trust concepts [15].

3. CLASSIFICATION OF RELATED LITERATURE ON NETWORK SEGMENTATION

Table 1 groups the studies into clear categories, making it easier for readers to identify the contribution of each paper. It also highlights a common research trend: the evolution of network segmentation from traditional VLAN and firewall-based

approaches toward intelligent, software-defined, Zero Trust, and AI-assisted segmentation techniques, which supports the motivation for developing an educational platform focused on network segmentation concepts.

Table 1. Classification of Related Literature on Network Segmentation

Ref.	Research Focus	Key Technologies/ Concepts	Main Contribution	Limitations/ Challenges
[1]	Battlefield communication networks	5G, Network Slicing, SDN, AI, IDS	Proposed secure network slicing architecture for military communication	Integration complexity, abnormality detection, decision-making challenges
[2]	5G Network Slicing	SDN, NFV, Virtualization, Orchestration	Explained implementation of isolated virtual network slices	Resource management, security, performance, business models
[3]	Security of Network Slicing	AI, Blockchain, SDN, NFV	Reviewed security and privacy threats in network slicing	Slice isolation, data leakage, DoS attacks
[4]	IIoT Network Segmentation	Micro-segmentation, Firewalls, NAC	Demonstrated segmentation for Industrial IoT security	Increased complexity, cost, performance issues
[5]	SDN Security	SDN Controller, Authentication, Traffic Analysis	Discussed SDN security architecture and mitigation strategies	Controller attacks, DoS, inter-layer threats
[6]	SDN Architecture	SDN Layers, Controllers, Virtualization	Comprehensive review of SDN architecture and research taxonomy	Scalability, controller bottlenecks, policy conflicts
[7]	SDN Security Policies	Brew Framework, Flow Rule Analysis	Proposed automated conflict detection and resolution in SDN	Complexity in distributed controller environments
[8]	Zero Trust Architecture	IAM, MFA, ZTNA, Micro-segmentation	Explained Zero Trust principles and importance of micro-segmentation	Legacy system integration and implementation cost
[9]	Zero Trust for IIoT	Federated Learning, Explainable AI, Hypergraph Clustering	Proposed intelligent Zero Trust micro-segmentation framework	Computational complexity and deployment challenges
[10]	Enterprise Network Segmentation	Access Control, Segmentation	Demonstrated segmentation benefits in enterprise environments	Management overhead, misconfiguration, deployment cost
[11]	Cloud Security	Zero Trust, Istio, Calico, Service Mesh	Proposed layered cloud micro-segmentation architecture	Complex policy management
[12]	IoT Security	Edge Security, DNS Policy Distribution	Proposed distributed security policy enforcement	Device heterogeneity and policy complexity
[13]	O-RAN Network Slicing	O-RAN, AI/ML, SDN, NFV	Reviewed network slicing implementation in Open RAN	Resource allocation and interoperability challenges
[14]	End-to-End 5G Network Slicing	ETSI, 3GPP, IETF Standards	Presented complete end-to-end network slicing architecture	Standardization and cross-domain coordination
[15]	Modern Network Segmentation	Micro-segmentation, Zero Trust, eBPF	Reviewed evolution from traditional segmentation to AI-driven segmentation	Policy complexity and performance overhead

4. SYSTEM DESIGN

The developed system is a web-based educational platform designed to introduce learners to the fundamentals of network segmentation through interactive lessons, formative assessments, and gamification. The primary objective of the platform is to provide an accessible learning environment that combines instructional content with quizzes and achievement-based rewards to improve learner engagement and knowledge retention. The application was designed to be lightweight, responsive, and compatible with web hosting services, allowing it to be deployed through GitHub Pages while remaining accessible from desktop and mobile devices.

4.1 Design Goals

The platform was developed with four primary design goals:

- Usability: Create an intuitive interface that enables users to easily navigate between lessons, quizzes, progress tracking, and achievements with minimal learning effort.
- Content Organization: Present educational materials in a clear, structured, and visually organized format to improve readability and comprehension of network segmentation concepts.
- Learner Engagement: Incorporate gamification through badges, progress indicators, and immediate quiz feedback to encourage continuous participation and motivation.
- Responsiveness and Flexibility: Ensure that the application adapts to different screen sizes and devices while maintaining consistent functionality and performance.

4.2 User Requirements

The platform was designed to satisfy the learning requirements of beginner users with little or no prior knowledge of network segmentation. The system enables users to:

Access structured learning modules covering network segmentation concepts.

Complete quizzes after each lesson to assess understanding.

Receive immediate feedback and explanations for every quiz question.

Monitor lesson completion and overall learning progress.

Earn and collect achievement badges based on completed learning activities.

View quiz outcomes and return to the main dashboard to continue learning.

These requirements provide learners with both instructional support and continuous performance monitoring throughout the learning process.

4.3. System Functionalities

To satisfy the identified requirements, the platform implements the following core functionalities:

- Display a personalized dashboard summarizing learning progress.
- Present instructional lessons are organized into individual learning modules.
- Deliver three-question quizzes following each lesson.
- Provide immediate feedback, including the correct answer and explanatory information after every question.
- Record quiz completion and determine whether the learner has successfully passed the assessment.
- Award achievement badges for completed lessons and milestones.
- Maintain learner progress throughout the learning process.
- Allow users to navigate efficiently between lessons, quizzes, badges, and the dashboard.

These features create an integrated learning environment that combines educational content with formative assessment and motivational elements.

5. IMPLEMENTATION

The web-based learning platform was implemented using modern front-end web development technologies to create an interactive, responsive, and maintainable application. The system was designed as a single-page application (SPA), enabling users to navigate between lessons, quizzes, badges, and the dashboard without requiring full page reloads, thereby improving the overall user experience.

5.1. Development Tools

The implementation utilized the following technologies:

- React served as the primary front-end framework. React's component-based architecture enabled the application to be divided into reusable interface components such as the navigation bar, lesson pages, quiz modules, dashboard, and badge displays. This modular design simplified development, maintenance, and future expansion of the platform.
- JavaScript was used to implement the application's core functionality, including quiz logic, navigation between lessons, progress tracking, badge unlocking, and user interaction. Event-driven programming allowed the application to respond dynamically to user actions and update the interface in real time.
- HTML5 provided the structural foundation for the application's content, organizing educational materials, quizzes, buttons, and navigation elements into a semantic and accessible layout.
- CSS3 was used to create a responsive and visually consistent user interface. Grid layouts and flexible styling techniques ensured compatibility across different screen sizes while maintaining readability and usability. Color schemes, typography, spacing, animations, and visual feedback were also implemented using CSS to enhance user engagement.
- Icon Libraries were incorporated throughout the interface to improve visual communication and usability. Icons were used within navigation menus, badges, progress indicators, and action buttons, allowing users to quickly recognize important functions while contributing to the overall aesthetic of the platform.

5.2 Development Environment

Development was performed using CodeSandbox, an online integrated development environment (IDE) that supports React-based projects. CodeSandbox provided rapid prototyping capabilities, live preview functionality, and automatic compilation, allowing interface components and application logic to be tested immediately during development. This environment facilitated iterative design improvements and simplified debugging throughout the implementation process. Version control and project deployment were managed using GitHub. GitHub was used to store the project's source code, monitor development changes, and maintain version history throughout the implementation process. Upon completion, the application was deployed using GitHub Pages, providing a publicly accessible hosting platform without requiring additional server-side infrastructure. This deployment approach made the educational platform easily accessible through a standard web browser while simplifying future updates and maintenance.

5.3 GUI

To run the system, user will go to the dashboard to check progress

By checking the learning progress box to see what has been done [Figure 1]. Then user can activate or start the lesson as in Figure 2. The user can then read the lesson [figure 3]. Once done the user will take the quiz [Figure 4]. Finally, the user can check their progress or badges [Figure 5].

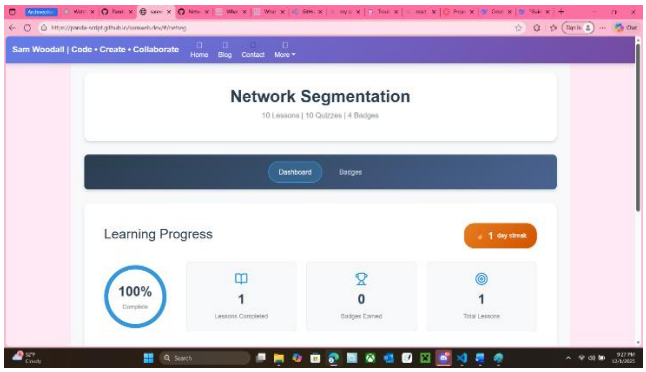

Fig 1: Dashboard

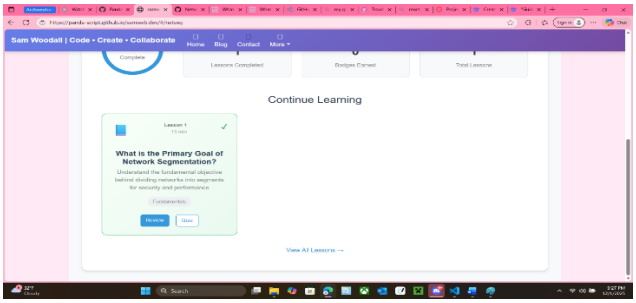

Fig 2: start a lesson

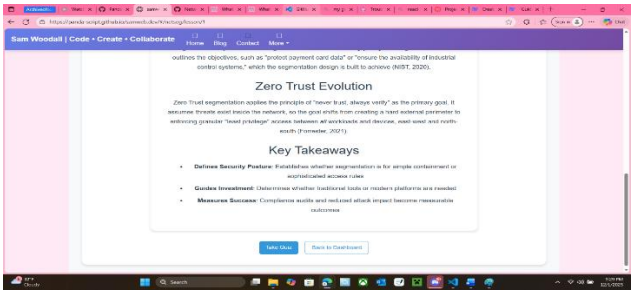

Fig 3: Lesson content

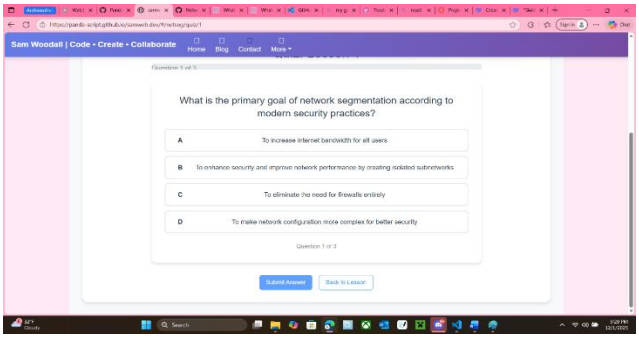

Fig 4: completing a lesson

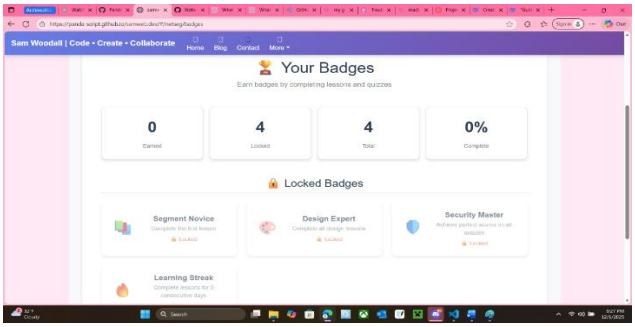

Fig 5: Badges

6. ANALYSIS

6.1 Quantitative Analysis

Participants evaluated the web-based learning platform across five usability and learning-related criteria using a five-point Likert scale.

Next are the questions completed by users.

1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

- The website's navigation (menus, buttons, links) was clear and intuitive, making it easy to move between lessons and quizzes.
- The visual design (colors, fonts, layout) was attractive, professional, and appropriate for the topic.
- The quizzes were fun, engaging, and effectively reinforced the lesson content.
- The website was responsive and functioned correctly on my device (computer, tablet, or phone).
- After completing the 10 lessons and quizzes, I feel more knowledgeable about Network Segmentation.

Overall, the platform received positive ratings, with all categories achieving mean scores above 3.50 [Figure 6]

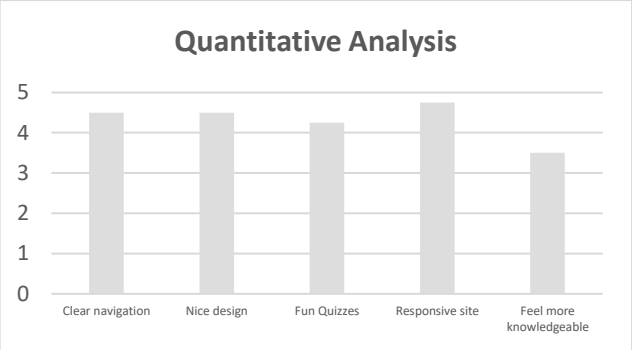

Fig 6: Quantitative Analysis results

The highest-rated criterion was site responsiveness (M = 4.75), indicating that participants perceived the website as reliable, fast, and technically stable during use. This finding suggests that the platform provided a smooth user experience with minimal performance issues. Both clear navigation (M = 4.50) and website design (M = 4.50) received similarly high ratings. These results demonstrate that participants found the interface intuitive, visually appealing, and easy to navigate, supporting the project's objective of creating a user-friendly educational platform. The quiz experience also received a favorable rating (M = 4.25), suggesting that participants considered the quizzes engaging and enjoyable. This result aligns with the qualitative feedback, where participants highlighted the quizzes and the explanations provided after each question as effective learning features. The lowest-rated criterion was feeling more knowledgeable after using the website (M = 3.50). Although this score remains above the midpoint of the scale, it indicates that participants perceived a more moderate improvement in their understanding of network segmentation. This finding is consistent with the qualitative responses, which suggested that the lesson content could be better organized and supported with additional examples to improve comprehension. Overall, the quantitative findings indicate that the platform successfully achieved its usability goals, particularly in terms of responsiveness, navigation, visual design, and user engagement. However, the comparatively lower learning outcome score suggests opportunities to enhance the instructional content and lesson presentation, which may further improve users' knowledge acquisition in future iterations of the platform.

6.2 Qualitative Analysis

The qualitative feedback from participants revealed several recurring themes regarding the usability, effectiveness, and potential improvements of the web-based learning platform. Next are the questions completed by users:

1. What did you like most about the website and its quizzes? Why?

2. What did you like least, or what felt confusing or frustrating? Please suggest an improvement.

3. Describe one specific moment where the quiz or lesson was particularly effective in helping you understand a concept.

4. Was there any technical issue (e.g., a button not working, a page loading slowly, a quiz not submitting)? If yes, please describe it.

5. If you could add one new feature to this website (e.g., a leaderboard, more question types, downloadable summaries), what would it be and why?

From user input the following patterns are identified [Table 2]

- User Experience and Interface Design: Participants consistently reported positive impressions of the website's interface, emphasizing its clean aesthetic, intuitive layout, and ease of navigation. Three of the four participants specifically highlighted the visual design and straightforward navigation as major strengths, suggesting that the platform successfully met its usability objectives. One participant specifically noted appreciating the ability to navigate freely through the website, indicating that the interface supported an effective user experience.
- Learning Effectiveness: A prominent theme across responses was the value of the immediate feedback provided after quiz questions. Three participants stated that the explanations accompanying both correct and incorrect answers helped reinforce their understanding of network segmentation concepts. Another participant appreciated having access to lesson materials before attempting the quizzes, indicating that the combination of instructional content and formative assessment supported learning. These responses suggest that explanatory feedback was one of the platform's most effective educational features.
- Areas for Improvement: Although participants responded positively overall, multiple respondents identified the presentation of lesson content as an area requiring improvement. Three participants commented that the lesson layout could be better organized, with suggestions including repositioning headings and improving the overall arrangement of instructional information. One participant also mentioned that the subject matter was unfamiliar, highlighting the importance of presenting beginner-friendly explanations and examples to improve accessibility for users with limited prior knowledge.
- Technical Performance: Most participants reported that the website functioned smoothly without technical issues. However, one participant experienced problems with the lesson pages not displaying correctly, which aligned with implementation issues identified during development. Aside from this isolated issue, the platform demonstrated satisfactory technical stability during evaluation.
- Suggested Future Features: Participants expressed interest in expanding the platform's functionality. Two participants recommended adding a leaderboard or ranking system to increase engagement through friendly competition, while another suggested implementing streak tracking similar to popular educational applications. Additional recommendations included increasing the number of quiz questions and incorporating practical examples or visual illustrations within lessons instead of relying primarily on text. These suggestions indicate that users value both enhanced educational content and additional gamification features.

Overall, the qualitative findings indicate that participants perceived the platform as visually appealing, easy to navigate, and effective in supporting learning through quizzes and explanatory feedback. The primary areas identified for future improvement involve reorganizing lesson content, expanding instructional materials, incorporating more visual examples, and introducing additional gamification elements such as leaderboards and streaks. Addressing these recommendations could further improve both user engagement and learning outcomes in future versions of the platform.

Table 2. Overall Interpretation of Qualitative Findings

Dimension	Overall Finding	Strengths Identified	Priority for Future Development
Usability	Participants generally found the platform easy to use and navigate.	Clean interface, intuitive navigation, visual appeal	Low–Moderate
Educational Effectiveness	The platform effectively supported learning through quizzes and immediate explanatory feedback.	Feedback, quizzes, access to lessons before assessment	Low–Moderate
Content Presentation	Lesson organization could be improved to make information easier to understand.	Availability of instructional content	High
Accessibility	Users unfamiliar with the topic may require additional scaffolding.	Basic instructional structure	Moderate–High
Technical Performance	The platform was generally technically stable, although one lesson-display problem was reported.	Smooth operation for most participants	Moderate
Engagement	Participants showed interest in additional motivational and interactive features.	Existing quizzes	Moderate–High
Future Functionality	Users recommended more questions, visual examples, leaderboards, and streak tracking.	Potential for expanded learning and engagement	High

7. CONCLUSION

This study presented the development of a web-based learning platform designed to teach users the fundamentals of network segmentation through interactive lessons, assessments, and a badge-based gamification system. The platform was developed with usability, accessibility, and user engagement as primary design objectives. During the development process, several implementation challenges were encountered, including issues with lesson rendering and navigation. These challenges were addressed by restructuring the application's layout and refining

its routing system, resulting in a more stable and user-friendly platform. Feedback from evaluators highlighted strengths in the platform's visual design and overall user experience while identifying opportunities to improve the organization and presentation of instructional content. These findings suggest that although the platform successfully provides an engaging learning environment, the educational materials can be enhanced to improve clarity, comprehension, and learning effectiveness.

Future work will focus on refining the lesson structure, expanding the learning content, and incorporating additional interactive features such as simulations, practical exercises, and adaptive quizzes. Further usability testing with a larger and more diverse group of users will also be conducted to evaluate learning outcomes and guide continuous improvements. These enhancements are expected to strengthen the platform's effectiveness as an educational tool for teaching network segmentation and supporting cybersecurity education.

8. REFERENCES

[1] A. Castañares, D. K. Tosh and C. A. Kamhoua, "Slice Aware Framework for Intelligent and Reconfigurable Battlefield Networks," *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, San Diego, CA, USA, 2021, pp. 489-494, doi: 10.1109/MILCOM52596.2021.9653025.

[2] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," in *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80-87, May 2017, doi: 10.1109/MCOM.2017.1600935.

[3] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu and M. Liyanage, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," in *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 534-570, Firstquarter 2024, doi: 10.1109/COMST.2023.3312349.

[4] V. V. Baligodugula, A. Ghimire, and F. Amsaad, "An Overview of Secure Network Segmentation in Connected IIoT Environments," *Computing & AI Connect*, vol. 1, p. 1, Aug. 2024, doi: 10.69709/CAIC.2024.193182.

[5] I. Ahmad, S. Namal, M. Ylianttila and A. Gurtov, "Security in Software Defined Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2317-2346, Fourthquarter 2015, doi: 10.1109/COMST.2015.2474118.

[6] Y. Jarraya, T. Madi and M. Debbabi, "A Survey and a Layered Taxonomy of Software-Defined Networking," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1955-1980, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320094.

[7] S. Pisharody, J. Natarajan, A. Chowdhary, A. Alshalan and D. Huang, "Brew: A Security Policy Analysis Framework for Distributed SDN-Based Cloud Environments," in *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 1011-1025, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2726066.

[8] M. Rakhra, B. Kaur, G. Aggarwal, D. Ather, R. Kler and K. Jairath, "The Zero Trust Paradigm: Revolutionizing Network Security," *2025 International Conference on Networks and Cryptology (NETCRYPT)*, New Delhi, India, 2025, pp. 1714-1719, doi: 10.1109/NETCRYPT65877.2025.11102576.

[9] M. L. Gambo and A. Almulhem, "An Explainable Federated Framework for Zero Trust Micro-Segmentation in IIoT Networks," *arXiv preprint arXiv:2603.24754*, 2026.

[10] N. Kotha, "Network Segmentation as a Defense Mechanism for Securing Enterprise Networks," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 11, pp. 3023–3030, 2020.

[11] S. Arora and J. Hastings, "Microsegmented Cloud Network Architecture Using Open-Source Tools for a Zero Trust Foundation," *arXiv preprint*, 2024, doi: 10.1109/SIN63213.2024.10871361.

[12] L. Deri and A. Del Soldato, "An Architecture for Distributing and Enforcing IoT Security at the Network Edge," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 211-218, doi: 10.1109/Cybermatics_2018.2018.00065.

[13] K. Alam *et al.*, "A Comprehensive Tutorial and Survey of O-RAN: Exploring Slicing-Aware Architecture, Deployment Options, Use Cases, and Challenges," *arXiv preprint*, 2024, doi: 10.1109/COMST.2025.3598406.

[14] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, and K. Ghoumid, "A Comprehensive Survey on the E2E 5G Network Slicing Model," *IEEE Transactions on Network and Service Management*, vol. PP, pp. 1–1, Dec. 2020, doi: 10.1109/TNSM.2020.3044626.

[15] S. Chennamsetty and S. A. Averineni, "From Network Segmentation to AI-Driven Zero Trust: A Systematic Survey of Micro-segmentation Technologies," *2025 7th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT)*, Guangzhou, China, 2025, pp. 111-117, doi: 10.1109/ECNCT66493.2025.11172491.