IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 September 2023, accepted 4 December 2023, date of publication 8 December 2023,
date of current version 19 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3341093

RESEARCH ARTICLE

Factor Analysis of Learning Motivation Difference on Cybersecurity Training With Zero Trust Architecture

TAISHO SASADA[1,2], (Student Member, IEEE), MASATAKA KAWAI[3], YUTO MASUDA[3], YUZO TAENAKA[1], (Member, IEEE), AND YOUKI KADOBAYASHI[1], (Member, IEEE)

[1]Graduate School of Science and Technology, Nara Institute Science and Technology (NAIST), Ikoma 630-0192, Japan
[2]Japan Society for the Promotion of Science, Tokyo 102-0083, Japan
[3]NRI SecureTechnologies Ltd., Tokyo 100-0004, Japan

Corresponding author: Taisho Sasada (sasada.taisho.su0@is.naist.jp)

This work was supported in part by the Information-technology Promotion Agency (IPA)'s ICS-CoE Core Human Resources Development Program.

ABSTRACT Cloud computing technologies have increased the diversity and complexity of security expertise needed to prevent cyber attacks. decisionIn software and system architect area, The expertise of security personnel in these security technologies is highly valued. However, it is extremely challenging for companies to acquire such security personnel, leading to the proposal and increased attention towards cyber security training programs as an alternative to hiring new personnel. Many of the existing training programs focus on acquiring knowledge of security technologies and practicing incident response but often fail to provide the skills necessary for system architecture, such as system design and scaling. In the era of cloud computing, system architecture is indispensable, and there is a need for training programs that enable participants to acquire these related skills, regardless of their academic background in security technologies. In this study, we propose a novel cybersecurity training program that allows participants to learn as system architects, covering the entire process from design to implementation. We utilize the state-of-the-art system architecture model known as Zero Trust Architecture (ZTA) and expand it from a prototype of reverse proxy access control to encompass ZTA. This approach enables participants to acquire the skills necessary for system architects, including system scalability and security. Furthermore, we measure the educational effectiveness of the training program by collecting decision the ARCS questionnaire dataset from students and workers. The results of statistical tests and factor analysis conducted on the ARCS questionnaire confirm that the training program enhances learning motivation, regardless of the participants' academic background in security technology. Additionally, these tests help identify the differences in factors that influence learning motivation between students and working adults.

INDEX TERMS Cybersecurity training, zero trust architecture, system architecture, exploratory factor analysis, educational data analysis.

I. INTRODUCTION

Cyber-attacks on information systems are becoming increasingly diverse and complex, demanding a higher level of expertise in security technologies to effectively counter these attacks. Professionals with a deep understanding of these security technologies are highly valued as security personnel in the development of software and systems that handle confidential data. Typically, security personnel serve as Chief Information Security Officers (CISOs) or are members of Computer Security Incident Response Teams (CSIRTs) within organizations. As a result, it is challenging for companies to acquire such skilled security personnel. The demand for cybersecurity professionals in the information

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

technology field has been rapidly growing. According to reports from the Korean Communications Commission and the Information-technology Promotion Agency in Japan, there is a rising need for technical cybersecurity personnel, and enterprises are struggling to fill their open positions [1], [2].

Various cyber training programs have been developed to foster the development of security personnel rather than solely relying on their acquisition. One such program, proposed by Beuran et al., is CyTrONE, a cybersecurity training that combines hands-on training with interactive discussions. The instructor has the flexibility to modify various parameters, such as the number of virtual machines (VMs) and network configurations, in order to train participants in different scenarios. However, since the instructor handles the system architecture process, participants do not acquire design skills through this training. Another training program, proposed by Omiya et al., is the design of a training game called Secu-One. This game focuses on efficiently learning about IoT systems and aims to cultivate motivation for learning security technology through gamification. Participants engage in the training using a card game format, where they learn about cybersecurity related attacks and defenses. The absence of technical barriers in the game keeps participants motivated to learn throughout the training. However, similar to CyTrONE, Secu-One does not include system architecting as part of the game, and therefore participants do not acquire design skills. In summary, both the CyTrONE and Secu-One cybersecurity training programs primarily focus on enhancing technical skills, with participants practicing achieving specific conditions in a preconstructed system environment provided by the governing body or organization. Based on this, the research objectives of our study are as follows:

1) We design cybersecurity training that will provide participants with the necessary skills to become system architects, and do not limit the ablility of participants in the proposed training.
2) By conducting in-depth analyses of participants' motivation during the training, we aim to identify the imposition of learning motives and analyze motivational trends and common factors latent in the data so that future relevant studies can refine the training.

In this study, we propose a cybersecurity training program that offers participants both practical experience and motivation in system architecture. The proposed training is based on the Zero Trust Architecture (ZTA), a state-of-the-art security model, and aims to foster motivation for system architecting regardless of the participants' level of experience in learning security technologies. Our training program (CYTØRUS: Cybersecurity Training Material with Zero Trust) is designed as a three-stage system architect training that includes an introductory lecture, hands-on training, and discussion sessions. This comprehensive approach allows participants to learn essential skills for system architects, ranging from fundamental knowledge of access control, security, scalability, to effective communication with non-technical individuals.

To evaluate the effectiveness of the training program, we recruited both students and workers as participants. After completing the training, we administered a questionnaire to measure the educational impact. The questionnaire is designed to assess whether there is a positive educational effect independent of the participants' academic or professional background, and to identify the factors that contribute to learning motivation. By conducting this study, we aim to demonstrate the effectiveness of our proposed training program in enhancing participants' understanding of system architecture, regardless of their years of study or work experience in the field of security technologies. In summary, this research makes the following contributions:

- Designing and implementing a novel cybersecurity training program aimed at equipping security personnel with the skills required to become system architects. This training fills the gap in existing programs by focusing on system design and architecture.
- Statistical tests conducted on the training participants demonstrate that the proposed program effectively motivates individuals to learn system architecture, irrespective of the number of years they have spent learning security technology. This finding highlights the positive impact of the training on participants' motivation.
- Our factor analysis conducted on the collected data reveals differences in the factors influencing the motivation to learn system architecture between students and working adults. This insight provides valuable information for tailoring future training programs to meet the specific needs and motivations of these distinct groups.

Overall, this research contributes to the field of cybersecurity training by introducing a comprehensive program that enhances participants' skills in system architecture, provides motivation for learning, and recognizes the differing factors driving motivation among students and working adults.

The structure of this paper is as follows: In Section II, we provide an overview of related work, including discussions on instructional design, ZTA, and references on cybersecurity trainings. In Section III, we present the design of our proposed training program, which aims to effectively teach system architecting skills while maintaining high levels of learning motivation among participants. In Section IV, we detail the development and implementation process of our training program, outlining the steps taken to create an immersive and engaging learning experience. In Section V, we discuss the methods used to measure and assess the educational effects of the training program. We present the results obtained from the evaluation and analyze the impact of the program on participants' learning outcomes. In the final Section VI, we summarize the key findings of this study and provide a comprehensive conclusion. Additionally, we discuss potential future research directions and unresolved issues that may warrant further investigation.

II. RELATED WORK

A. INSTRUCTIONAL DESIGN

To enhance the educational effectiveness of our training program, we utilize Instructional Design (ID) methodologies, which involve the systematic design of educational programs. Several ID models have been proposed, including the influential work by Gagné and Briggs [3], Smith and Ragan [4], and Sweller [5]. One widely recognized ID model is the ADDIE model, which stands for Analysis, Design, Development, Implementation, and Evaluation. This model enables a comprehensive review and reflection on various aspects of the educational process at each stage. It follows a five-step process, ensuring efficient and effective learning outcomes [6]. The ADDIE model has gained attention in both academic and corporate education settings as a method to enhance the effectiveness and efficiency of educational activities. It enables quality control in education by providing a structured approach to instructional design and evaluation. By incorporating the principles of Instructional Design, specifically the ADDIE model, into our training program, we aim to optimize the educational experience and ensure high-quality learning outcomes for our participants.

In order to effectively design a cybersecurity training program that facilitates the acquisition of system architect skills, this study will follow the ADDIE model for instructional design and development. However, evaluating the effectiveness of system architecture training presents unique challenges compared to other cybersecurity training programs. For instance, when addressing unauthorized access, one can quantitatively evaluate factors such as response time, the percentage of successfully defended resources, and the effectiveness of specified defense solutions like firewalls, intrusion detection systems, and anti-malware tools. On the other hand, system architecture evaluation is more nuanced and multifaceted, encompassing factors like response requirements, throughput, scalability, and security. The assessment of artifacts in this context varies based on these diverse considerations, making quantitative evaluation difficult. Therefore, in areas where quantitative evaluation of artifacts is challenging, the focus shifts to evaluating learning motivation instead. Learning motivation is frequently assessed as it allows for the measurement of participant satisfaction with the training and self-evaluation. By examining these aspects, we can gauge the effectiveness of the training program in terms of participant engagement and motivation. In this study, we will adopt this approach by evaluating the learning motivation of participants, providing valuable insights into the impact of the training program beyond traditional quantitative assessments.

To define and assess learning motivation, this study adopts the ARCS motivational model proposed by Keller [7]. The ARCS model focuses on four key elements: Attention, Relevance, Confidence, and Satisfaction. These elements are crucial for fostering motivation to learn and ensuring continuous engagement. In this research, the effectiveness of the proposed training program in motivating participants to learn is investigated through evaluation methods based on the ARCS motivational model. This evaluation may involve questionnaires, design reviews, and other relevant techniques. By leveraging the ARCS model, we can assess the extent to which the training program effectively motivates participants to engage in the learning process. The ARCS model is integrated with the ADDIE model, which is utilized to design and evaluate the effectiveness of the training program in terms of learning motivation. The ARCS evaluation sheet, widely used in various training programs [8], [9], [10], [11], is employed in this study to assess learning motivation. By employing the ADDIE model for instructional design and development and incorporating the ARCS evaluation sheet for assessing learning motivation, this study aims to design and implement a training program that effectively motivates participants to learn and evaluates its effectiveness accordingly. In the next subsection, we describe ZTA that is the subject of our training.

B. ZTA ON NIST SPECIAL PUBLICATION 800-207

Zero Trust Architecture (ZTA) is a novel security model that aims to enhance the protection of sensitive data and systems by encrypting communications between endpoints and servers. It operates under the assumption that all users, terminals, and connection sources are untrustworthy, requiring verification of their legitimacy and security before granting access to sensitive resources. ZTA serves as a preventive measure against malware infection and data leakage. The logical structure of ZTA is depicted in Figure 1 and is proposed in NIST Special Publication 800-207. Compliance with NIST SP800-207 in training allows participants to accurately learn standardized ZTA. It involves the separation of the data plane, which handles communication for access requests, and the control plane, which manages communication for access control. Within this framework, the Policy Decision Point (PDP) plays a crucial role in determining whether a given policy conforms to the protection requirements of critical resources. On the other hand, the Policy Enforcement Point (PEP) is responsible for granting or denying access based on the decisions made by the PDP. Overall, ZTA represents a modern approach to security architecture that prioritizes verification and access control to safeguard sensitive data and systems, preventing potential threats such as malware infections and data breaches.

ZTA has found application in access control, leading to the proposal of various access control mechanisms for cloud computing [12], [13], [14], [15], [16]. These mechanisms leverage ZTA principles to enhance the security of access control in cloud environments. In practice, major industry players like Google have implemented BeyondCorp, an access control system based on ZTA. Similarly, cloud vendors such as Amazon's AWS and Microsoft's Azure

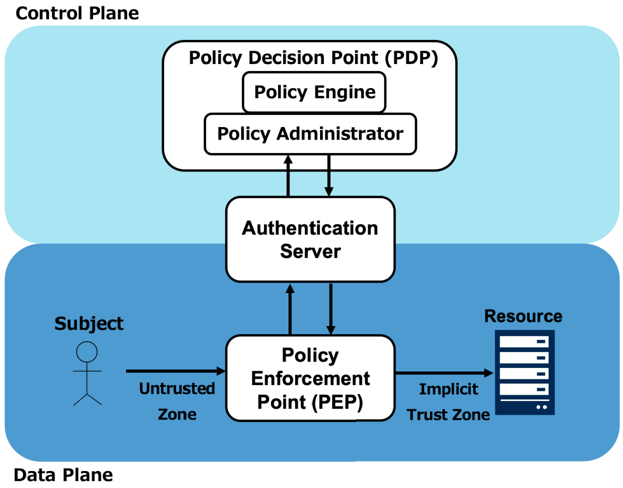

FIGURE 1. ZTA defined on NIST special publication 800-207.

also offer ZTA services to their customers. However, it is important to note that the design of suitable remote access frequency and access time restrictions within a ZTA framework can vary across departments, individual organizations, and different types of companies. Therefore, it is necessary to consider not only access control mechanisms but also understand various cyber attack methods in order to design effective and customized security measures.

C. CYBERSECURITY TRAINING

The US Department of Homeland Security (DHS) has developed the "Homeland Security Exercise and Evaluation Program (HSEEP)" [17] to effectively address emergencies, ranging from local incidents to national security issues. HSEEP categorizes trainings into two types: operations-based and discussion-based. This program has also served as a reference for cybersecurity trainings. Several cybersecurity training programs have been proposed, taking inspiration from HSEEP. For instance, the National Institute of Information and Communications Technology (NICT) in Japan has introduced the "Strategy for Cybersecurity (NISC)" and the "CYber Defense Exercise with Recurrence (CYDER)" [18], which align with the principles of HSEEP. Additionally, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) has developed the "Critical Infrastructure Incident Response Exercise" [19], which is another notable cybersecurity training program in Japan. These programs, influenced by HSEEP, aim to enhance preparedness and response capabilities in cybersecurity incidents. They provide practical exercises and discussions that enable participants to develop and strengthen their cybersecurity skills. By incorporating principles from successful programs like HSEEP, these cybersecurity training initiatives contribute to the overall preparedness of organizations and government agencies in responding to cyber threats.

While well-known cybersecurity training programs offer valuable learning experiences, they often lack the ability to provide participants with exposure to a wide range of training patterns. This limitation arises from the invariant nature of the training environment, including factors such as adversary capabilities, attack methods, and the characteristics of resources that defenders must protect. In contrast, a training program called CyTrONE, proposed by Beuran et al. [20], addresses this limitation by automatically adapting the training environment settings to generate scenarios that vary in complexity and characteristics. By allowing the instructor to modify parameters such as the number of virtual machines (VMs) and network configurations, CyTrONE can train participants in a diverse range of scenarios. However, one drawback of CyTrONE is that participants do not acquire design skills as the instructor handles the parameter changes, thereby bypassing the system architecting process. This implies that while participants gain hands-on experience and knowledge of specific cybersecurity scenarios, they do not develop the skills necessary for designing robust systems. Moreover, maintaining participants' motivation to learn is crucial for cybersecurity training involving various scenarios, especially for novice security technicians who may encounter technical barriers that hinder their learning progress. Overcoming these technical barriers and sustaining motivation can be challenging. Addressing these challenges and maintaining learning motivation among participants, particularly novices, is an important aspect to consider when designing effective and comprehensive cybersecurity training programs.

To address the challenge of maintaining learning motivation, Omiya and Kadobayashi [21] propose a training program called Secu-One, which focuses on gamification. Secu-One is specifically designed to facilitate efficient learning of IoT systems while keeping participants motivated to learn security technology. Secu-One utilizes a gamification approach, employing a card game format as a training method. Participants engage in the game and learn about various cyber attacks and defense strategies related to cybersecurity. The absence of technical barriers in the game helps to sustain participants' motivation throughout the training program. However, similar to CyTrONE, Secu-One primarily focuses on system operations and does not include system architecture in the gameplay. As a result, participants do not acquire design skills for developing secure and robust systems. Furthermore, it is important to note that experienced security experts may struggle to maintain their motivation to learn if the content of the training is not novel or challenging to them. For these experts, who already possess a high level of knowledge and experience, it becomes essential to provide engaging and advanced training materials that can keep them motivated to further enhance their skills and stay up-to-date with the latest developments in the field of cybersecurity.

III. METHODOLOGY

A. OVERVIEW

In this section, we present our proposal for a cybersecurity training focused on Zero Trust Architecture (ZTA). We call

TABLE 1. Summary of cybersecurity training programs.

Program	Description	Strengths	Weaknesses
HSEEP [17]	Developed by DHS for emergency response training. It categorizes training into two types: operations-based and discussion-based. It serves as a reference for cybersecurity training programs.	- Addresses a wide range of emergencies, from local incidents to national security issues. - Provides structured training approaches.	- Doesn't focus specifically on cybersecurity, making it less tailored to cyber threats.
CYDER [18]	Japanese programs inspired by HSEEP principles. NISC focuses on cybersecurity strategy, while CYDER aligns with HSEEP in enhancing preparedness and response capabilities.	- Enhance preparedness and response capabilities in cybersecurity incidents. - Provide practical exercises and discussions for skill development.	- May not cover the full spectrum of cybersecurity scenarios, potentially leaving gaps in preparedness.
CIIREX [19]	Another cybersecurity training program in Japan, developed by NISC. It focuses on critical infrastructure incident response exercises.	- Provides practical exercises and discussions to develop cybersecurity skills. - Addresses critical infrastructure security.	- Limited exposure to various training patterns due to the invariant nature of scenarios.
CyTrONE [20]	A training program designed to adapt the training environment to generate scenarios varying in complexity and characteristics. The instructor can modify parameters for diverse scenarios.	- Offers a wide range of cybersecurity scenarios, improving adaptability. - Allows customization of scenarios by the instructor.	- Participants may not acquire system design skills as the instructor handles parameter changes. - Dependency on the instructor for scenario creation may limit participant independence.
Secu-One [21]	Utilizes gamification in a card game format to facilitate efficient learning of IoT systems in the context of cybersecurity.	- Sustains participant motivation throughout training, thanks to gamification. - Eliminates technical barriers for learning security technology.	- Primarily focuses on system operations, neglecting system architecture and design skills.
Advanced Expert Training	Addresses the needs of experienced security experts who require advanced and engaging training materials to enhance their skills and stay updated.	- Provides advanced and engaging materials suitable for experienced experts. - Ensures experts stay up-to-date with the latest developments in cybersecurity.	- May not be suitable for beginners or those new to cybersecurity due to its advanced nature. - Requires ongoing novel content to maintain motivation among experienced experts.

our cybersecurity training material with zero trust as "CYTØRUS", and our training program is designed following the ADDIE model, a widely recognized instructional design model (see Section II-A). In this section, we will primarily focus on the Analysis, Design, and Development stages of the ADDIE model, outlining the key considerations and steps taken during each phase.

During the Analysis phase, we conduct a thorough assessment of the training needs and requirements. This involved identifying the target audience, their existing knowledge and skills related to security technologies, and their specific needs in terms of system architecture. We also analyze the characteristics of ZTA and its relevance to the training objectives.

Based on the findings from the Analysis phase, we proceed to the Design phase. Here, we formulated the overall structure and content of the training program. We define the learning objectives, determined the sequencing and organization of the training materials, and identified the instructional strategies and activities that would effectively convey the knowledge and skills related to system architecture using ZTA. Additionally, we consider the motivational aspects of the training to ensure participants' engagement and sustained learning.

The Development phase involve creating the actual training materials and resources based on the design specifications. We develop the instructional materials, including presentations, hands-on exercises, and case studies, to facilitate participants' understanding and application of system architecture principles using ZTA. We also incorporate interactive elements, such as simulations and group discussions, to enhance the learning experience and promote active participation.

In the subsequent sections, we will delve deeper into each phase of the ADDIE model, providing detailed insights into the analysis, design, and development of our cybersecurity training program based on ZTA.

B. ANALYSIS

In the initial phase of designing our cybersecurity training program, we conduct an analysis of the target participants. We consider that the technical knowledge and skills of the trainees would vary based on their work experience and the amount of independent study they have undertaken. To ensure the effectiveness and inclusivity of the training, we carefully considered these factors. The primary target participants for our training program are students and working professionals who aspire to become system architects (or security personnel in system security field) in the future. These individuals possess a certain level of motivation to learn cybersecurity technology and become security personnel through the training. We specifically chose this target audience to focus on individuals who are actively seeking to enhance their knowledge and skills in the field. To avoid any bias resulting from differences in work experience or the number of years of study, we have designed the training program to accommodate participants at various levels of expertise. By doing so, we aim to provide a valuable learning experience for both novice learners and those with more extensive experience in the field. The training program will cater to the specific needs and aspirations of individuals who are committed to developing their skills in security technology and becoming proficient system architects. By targeting students and working professionals who share a common goal of pursuing a career in system architecture and who possess a predetermined level of motivation to learn security technology, our training program aims to provide a comprehensive and engaging learning experience. In the following sections, we will outline the specific components and strategies employed in our training program, taking into account the diverse backgrounds and motivations of the participants.

In our analysis of the training requirements for system architects, we have identified several key skill sets that are essential for their role. These skill sets are based on the definitions provided by Downey et al. [22] and the insights of Omiya et al. [21] regarding the importance of communication and collaboration skills.

1) Understanding of System Design and Architecture: System architects need to have a solid understanding of system design principles and architecture. This includes knowledge of software, network, hardware, database, and storage components and how they interact to form a cohesive system.
2) Understanding of Scalability: System architects should possess knowledge of scalability considerations. They need to understand how to design systems that can handle increased workload and user demand, both in terms of hardware scalability (e.g., adding more servers) and software scalability (e.g., implementing load balancing).
3) Understanding of Security: System architects must have a foundational understanding of security principles. This includes identifying potential security risks, defining security requirements, and incorporating appropriate security controls into the system design to protect against threats and vulnerabilities.
4) Understanding of Project Management: System architects should have a basic knowledge of project management concepts and practices. This includes defining project scope, creating timelines, identifying and managing risks, and effectively coordinating and collaborating with team members and stakeholders throughout the project lifecycle.
5) Communication Skills: Effective communication is crucial for system architects. They need to be able to clearly convey technical information to both technical and non-technical stakeholders. Strong communication skills enable them to articulate complex concepts in an understandable manner and facilitate effective collaboration within the team and with project stakeholders.
6) Awareness of Technology Trends: System architects should stay informed about emerging technology trends in the industry. This includes keeping up to date with advancements in areas such as cloud computing, machine learning, deep learning, and the Zero Trust Architecture. This awareness allows system architects to incorporate relevant technologies into their designs and make informed decisions.

By incorporating these skill sets into our training program, we aim to equip participants with the knowledge and abilities necessary to become competent system architects.

C. DESIGN

Based on the analysis conducted in Section III-B, we have designed a cybersecurity training program that addresses the specific needs and requirements of aspiring system architects. To ensure that the training is effective and caters to participants with varying levels of proficiency in security technology, we have incorporated elements from the ZTA security model, which is a contemporary and widely recognized approach to system security. Recognizing that a single training program may not encompass all six skill sets required for system architects, we have structured the proposed training into three distinct programs: an introductory lecture, hands-on training, and discussion training. Each program focuses on different aspects of the skill sets, providing participants with a comprehensive learning experience. The specific skill sets covered in each training program are described in detail in their respective subsections.

1) INTRODUCTORY LECTURE

To accommodate participants from diverse backgrounds and varying levels of security experience, our training program includes an introductory lecture that can be attended by individuals with different levels of knowledge. This ensures that all participants have a common understanding of the fundamental concepts and principles of access control and ZTA.

The introductory lecture aims to provide participants with a comprehensive overview of access control methods, including the classic approaches such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). By explaining the advantages and disadvantages of each access control model, participants can develop a deeper understanding of their functionalities and use cases. Furthermore, the lecture introduces the concept of ZTA, which is formulated in NIST SP800-207, and Zero-Trust Access Control (ZTAC). Participants will learn about the principles and benefits of ZTA and how it differs from traditional access control models. This discussion will help participants grasp the core concepts of ZTA and understand its relevance in modern cybersecurity. To summarize the content covered in the introductory lecture, we have provided a detailed breakdown in Table 2.[1] This table serves as a reference guide for participants, highlighting the key topics and concepts

[1] The content of Table 2 is not provided in the current text. Please refer to the table separately for the detailed summary.

discussed during the lecture. By providing this comprehensive introduction, we aim to ensure that participants, regardless of their background knowledge or security experience, are equipped with the necessary foundation to fully engage in the subsequent training sessions.

Through the introductory lectures, participants can gain an understanding of system design and architecture, security and scaling methods, and ZTA and ZTAC. The lectures also cover technology trends such as machine/deep learning and cloud computing such as AWS, GCP, and Azure, which are often used in conjunction with ZTAC, to achieve skill sets 1, 2, 3, and 6.

2) HAND-ON TRAINING

In order to further enhance the proficiency in skill sets 1, 2, 3, and 6, hands-on training sessions will be designed to provide practical experience in system architecture and security. These sessions will build upon the knowledge gained from the introductory lectures and focus on implementing concepts discussed in those lectures. The hands-on training will be centered around BeyondCorp, Google's Zero-Trust Access Control (ZTAC) model, which is widely recognized for its effectiveness. Participants will have the opportunity to implement a proxy access to Nginx using an Identity Aware Proxy (IAP). By programming the IAP, participants will gain practical experience in implementing secure access controls and understanding how ZTAC can be applied to real-world scenarios.

Through this hands-on training, participants will deepen their understanding of system design and architecture (Skill Set 1), as they will be actively involved in configuring and implementing the proxy access. They will also enhance their knowledge of security (Skill Set 3) by implementing secure access controls and gaining insights into the importance of identity verification in preventing unauthorized access. Additionally, the hands-on training will provide participants with practical exposure to scaling methods (Skill Set 2), as they will be working with Nginx, a popular web server known for its scalability features. Participants will gain hands-on experience in configuring Nginx for scalability and load balancing, thereby strengthening their skills in this area. Finally, the training will also touch upon technology trends such as cloud computing (Skill Set 6). Participants will utilize cloud platforms (GCP) to deploy and test their implementation, gaining familiarity with these technologies in the context of ZTAC and system architecture. By combining theoretical knowledge from the introductory lectures with hands-on implementation in the training sessions, participants will have a comprehensive learning experience that deepens their proficiency in skill sets 1, 2, 3, and 6.

In the proposed training, the implementation process follows the steps outlined in Figure 2. Each step is described below, corresponding to the numbers in the figure: ① The user initiates an access request to the Policy Enforcement Point (PEP) for a web page that contains confidential information. ② Upon receiving the request, the PEP checks whether the user is authenticated or not. If the user is not authenticated, the PEP redirects the user to a login form and prompts them to enter their login credentials. ③ The user enters their ID and password as authentication information on the login form. ④ The PEP validates the received ID and password by comparing them with the stored credentials in the database. ⑤ After verifying the match between the received ID/password and the stored credentials, the PEP forwards the content of the access request to the Policy Decision Point (PDP) for authorization or denial. ⑥ The PDP consults a database containing user information to make an informed decision. ⑦ In order to assess the user information and make an authorization decision, the PDP displays the contents of the access request and the relevant user information. ⑧ Based on the trust decision made by the PDP, it sends an approval or denial response to the PEP. ⑨ Finally, the PEP, based on the trust decision from the PDP, accesses the web page (the requested resource) on behalf of the user. By following this implementation process, participants in the training will gain practical experience in the flow of access requests, authentication, authorization, and trust decisions in a ZTAC-based system architecture. This hands-on experience will help reinforce their understanding of the concepts discussed in the introductory lectures and enhance their proficiency in the relevant skill sets.

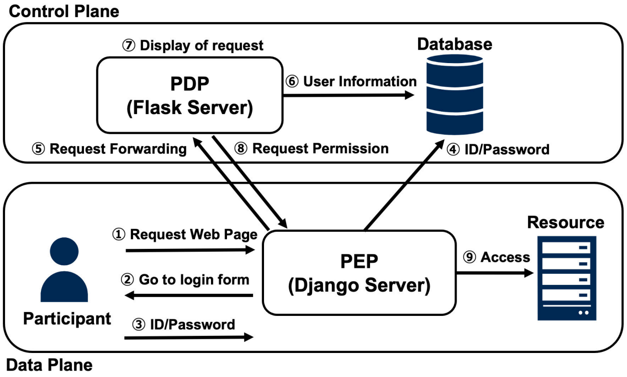

FIGURE 2. ZTAC to be implemented by participants in hands-on training.

In order to ensure effective and motivating hands-on learning, it is important to approach the implementation of Zero-Trust Access Controls (ZTAC) in a way that accommodates the varying skill levels and potential errors of the participants. The proposed training avoids the use of waterfall development, where participants are given a detailed set of requirements for the finished product and are expected to implement them all at once. This approach can be overwhelming, especially for beginners, and errors in the implementation process may lead to frustration and a loss of motivation. Similarly, adopting an agile development approach, which requires the same level of quality as a production system, can also lead to a loss of motivation if participants struggle to meet those high standards.

Instead, the training employs a hands-on approach through prototype development, starting with a simple prototype and

TABLE 2. Content of introductory lectures on access control schemes.

Access Control	Features	Pros	Cons	Examples
DAC	Control method based on login user information and resource ownership information	Easy to assign or change access rights	Possibility of granting inappropriate access rights due to accident/malicious intent	Linux/UNIX
MAC	A method to enforce access restrictions according to security policies on all users and processes, including the root user	Strict access restrictions are possible because even root user cannot bypass	May interfere with middleware installation and version upgrades	SELinux
RBAC	A method of control by granting privileges to users according to their roles, called roles	Easy to manage because there is no need to consider permissions on a per-user basis	Complicated role allocation in the case of a complex organization with a complicated role structure due to dual roles, etc.	Azure RBAC
ZTAC	A method to control all communications to a resource by assuming all access as untrusted.	Flexible control of authorization or denial on a per-access basis	Need to design with an understanding of the circumstances of the organization, constituents, and data	BeyondCorp

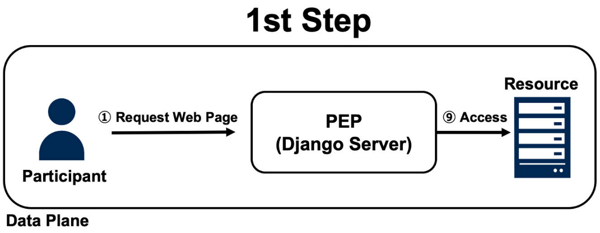

FIGURE 3. 1st Step (Proxy access via PEP).

gradually expanding its functions. This approach is illustrated in Figure 3 to Figure 5. By incrementally adding functionality to the prototype, participants can focus on understanding and implementing each component of the ZTAC, such as the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). In 1st step, participants implement a program to access the resource Ngix by proxy using Django, a web framework library (See Figure 3). In the 2nd step, participants extend the program from the 1st step to a program that centrally manages and authorizes/denies access requests with a Flask Server (See Figure 4). In the 3rd step, participants finally extend the program to ZTAC that actually performs request validation using user information (See Figure 5). This incremental approach not only facilitates a deeper understanding of the individual functions but also allows for easier detection and identification of participants who may be struggling or making errors. By providing timely feedback and support, the training can prevent participants from losing motivation due to their inability to keep up with the hands-on exercises. Overall, the hands-on training with gradual functional expansion provides a more engaging and manageable learning experience, ensuring that participants can effectively grasp the concepts and implementation of ZTAC while maintaining their motivation throughout the training process.

3) DISCUSSION TRAINING

The introductory lectures and hands-on training provided depth in skills 1, 2, 3, and 6. However, up to this point, the participants had only learned the content given to them, so they had not acquired skill sets 4 and 5, which are project management skills necessary for system architects to organize and summarize requirements and to share them effectively with other engineers/managers. Therefore, the proposed training will create groups consisting of multiple participants, and each group will conduct discussion-based system design.

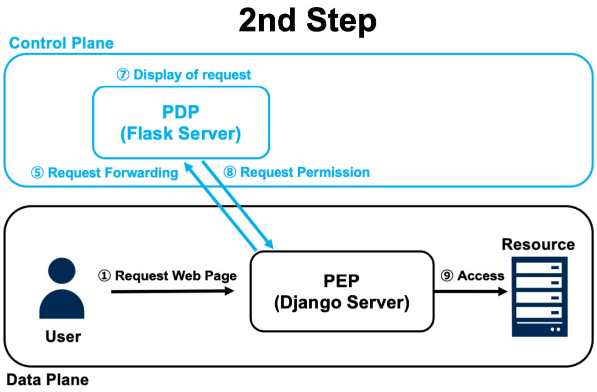

FIGURE 4. 2nd Step (Display access request on PDP).

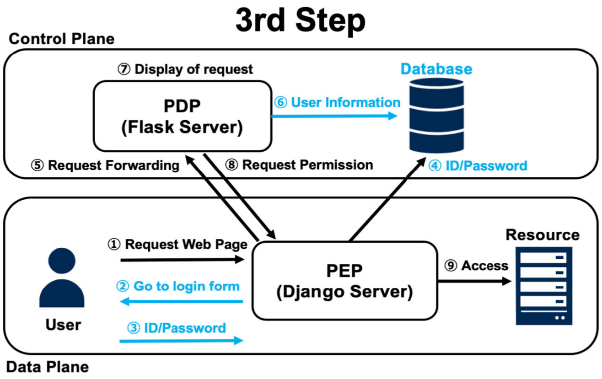

FIGURE 5. 3rd Step (Verify access request on PDP).

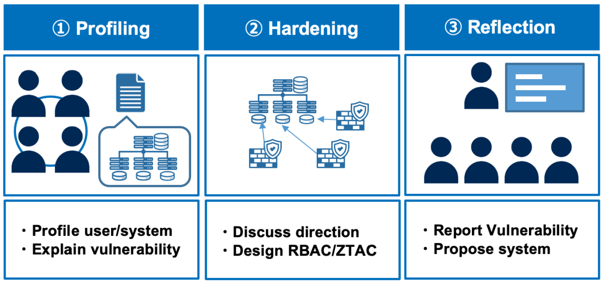

FIGURE 6. The overall flow of implementing our training.

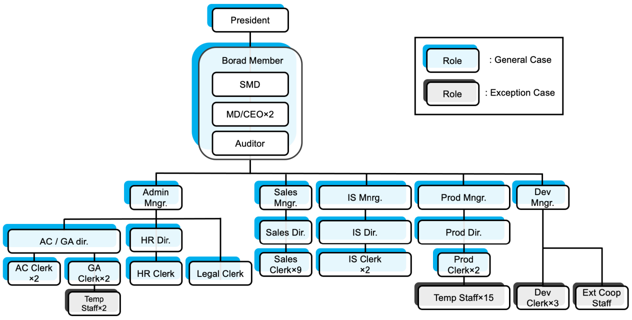

FIGURE 7. Hypothetical organization construction setting in scenario-based training.

In the discussion training, we assume a hypothetical company and a hypothetical system, and have the participants discuss the introduction of ZTAC and detailed considerations (e.g., creation of PDP policy, behavior management after approval, advantages and disadvantages of ZTAC for each department in the hypothetical company, etc.) per group. The training flow is shown in Figure 6, the role structure of the hypothetical company is shown in Fig. 7 and the system design is shown in Fig. 8. A series of training in Figure 6 has been introduced with Exercises to gain Skills 1 - 6. The training management sets the access privileges required for each system in terms of work content, department, and job position, and the participants design a trust score calculation method that satisfies these requirements. By designing these systems themselves, the participants can design appropriate policies for each group, and recognize points for improvement in the organizational structure/hypothetical system (See Figure 7 and Figure 8) and problems in conventional access control through discussions.

The discussion training component of the proposed cybersecurity training consists of four scenarios, each focusing on the implementation of ZTAC in a different department. These scenarios provide participants with practical examples to analyze and discuss the specific requirements and considerations for each department.

Scenario 1 is the sales department implementation. In this scenario, the sales department requires the internal network to be accessible from an external network, which includes an environment with potential security risks, such as open

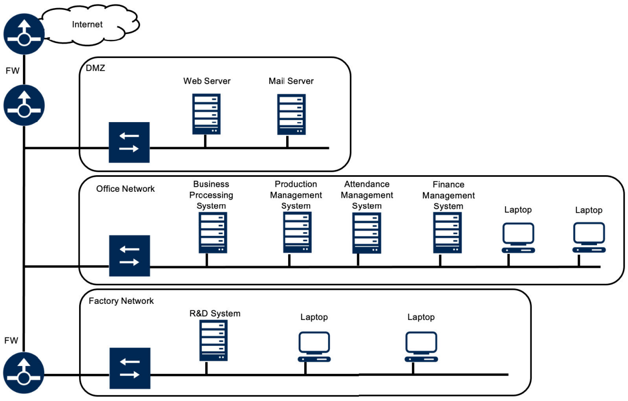
Internet
FW
DMZ
Web Server
Mail Server
Office Network
Business Processing System
Production Management System
Attendance Management System
Finance Management System
Laptop
Laptop
Factory Network
R&D System
Laptop
Laptop
FW

FIGURE 8. Logical configuration diagram of virtual system in scenario-based training.

Wi-Fi provided by a restaurant. Participants will discuss how to design an access control system that allows secure external access to the internal network while addressing the vulnerabilities associated with open Wi-Fi.

Scenario 2 is the manufacturing department implementation. For the manufacturing department, the scenario introduces specific requirements related to contract employees. Participants will analyze the challenges associated with managing access for contract employees who work for a limited period of three months. They will also address the issue of lacking ethics training for contract employees and the absence of distinction between permanent and contract employee accounts.

Scenario 3 is manufacturing department (factory) implementation. Similar to Scenario 2, this scenario focuses on the manufacturing department, but the requirements are now centered on the factories owned by the department. Participants will discuss the design of an access control system that allows access to common office systems and production management systems from devices installed in the factory. Additionally, they will explore the need for constant monitoring and maintenance of the production line through a logged-in state and seamless integration with the historian server where production information is recorded.

Scenario 4 is development department implementation. In this scenario, the development department is introduced, and participants will address the requirement of granting access to a researcher from a hypothetical university, who is a joint development partner. The discussion will revolve around designing a secure access control system that enables the researcher to access confidential company resources for development purposes while ensuring the protection of sensitive information.

Through these scenario-based discussions, participants will gain a deeper understanding of the practical challenges and considerations involved in implementing ZTAC in various departments and contexts. They will have the opportunity to analyze different access control requirements, identify potential risks, and propose appropriate security controls

TABLE 3. OS/CPU and software version in development.

Name	Value
CPU model	Intel®Core i9 CPU@2.30GHz
Memory size	16 GB
OS	macOS Monterey
macOS version	12.6.6
Docker	Docker Desktop for Mac
Python	3.8
Ngix	1.15.2

to achieve the objectives of each scenario. This exercise enhances participants' problem-solving skills, critical thinking, and ability to apply ZTAC principles to real-world scenarios.

IV. EXPERIMENT

In this section, we explain how to develop and implement our proposal (CYTØRUS) for participants (SecCap/ICSCoE).

A. DEVELOPMENT

In the development phase of the ADDIE model, it is important to consider the setup of the training contents based on the participants' devices. These specifications, including the CPU model, memory size, operating system, and software versions, are summarized in Table 3.

Compatibility issues, such as the proposed system not working with Python 2.x systems, can arise and cause significant time and effort in error handling, which may impact the evaluation of the training program. To address these challenges, this study adopts Docker, a virtualization platform, as the hands-on training environment. By distributing Docker images pre-configured with the necessary libraries and tools for development, the setup burden on participants can be greatly reduced. This approach ensures consistency and compatibility across different devices and streamlines the setup process. The proposed system will be developed using Docker, a virtualization platform; PDP and PEP will be developed using the Python 3.8 programming language; and web pages, which are confidential resources, will be developed using Ngix.

B. IMPLEMENTATION

This section corresponds to I (Implementation) of the ADDIE model. To verify the effectiveness of the proposed cyber security training, we conduct user training in person. Participants will be trained in the practical security human resource development course SecCap[2] and the ICSCoE core training human resource program,[3] respectively. Both SecCap and ICSCoE are educational projects to foster high-level security personnel in students and companies, and are considered appropriate participants for the training. After the training, we conduct a questionnaire survey to a total of 62 SecCap and ICSCoE participants to evaluate whether they were motivated to learn about system architecture including ZTA. We create the questionnaire based on the ARCS motivation model, which is a metrics for quantitatively measuring motivational effects, and its contents are shown in Table 4. The participants for the SecCap and ICSCoE sessions consisted of 22 and 40 students and professionals, respectively. Introductory lectures and hands-on training were conducted with all participants, and only discussion-based training was conducted with 12 groups of 4 to 5 participants each.

V. EVALUATION

In this section, we conduct a survey on the learning motivation through ARCS scheet, and verify correlation/Causal relationship. The survey aims to evaluate the correlation and causal relationship between the participants' motivation levels and the effectiveness of the training program.

A. ARCS QUESTIONAIRE

After the training, we conduct a survey to assess the participants' motivation using the ARCS questionnaire. The ARCS questionnaire is designed based on the ARCS motivational model and aims to quantitatively evaluate the level of motivation experienced by the participants during the training program. The questionnaire consists of items that correspond to the components of the ARCS model, namely Attention, Relevance, Confidence, and Satisfaction. Participants will be asked to rate each item on a 5-point scale using a Likert scale, where 1 represents "Strongly Disagree" and 5 represents "Strongly Agree." The questionnaire will include items related to the attention and engagement level during the training, perceived relevance of the content, confidence in applying the learned knowledge and skills, and satisfaction with the overall training experience.

Table 4 outlines the specific items included in the questionnaire. Participants will provide their ratings for each item, allowing for a quantitative assessment of their motivation levels. The responses from the questionnaire will be collected and analyzed to evaluate the effectiveness of the training program in terms of motivating the participants. The analysis of the questionnaire responses can provide valuable insights into the participants' perceptions of the training's impact on their motivation. It will help determine whether the training program successfully captured their attention, demonstrated the relevance of the content, enhanced their confidence in applying the knowledge, and resulted in overall satisfaction.

Table 6 presents the means and standard deviations of the ARCS questionnaire responses, while Figure 9 and Figure 10 illustrates the overall distribution of the ratings. The analysis of the results reveals interesting insights about the participants' motivation levels in the SecCap and ICSCoE training sessions, as well as the differences between beginner and expert participants. In the SecCap training session,

[2] SecCap is the program to educate security technology and knowledge at several universities to increase IT human resources with practical security skills.

[3] ICSCoE is the training project for people learning OT/IT technology, management, and business fields conducted by the IPA to strengthen cyber security measures for social infrastructure and industrial infrastructures.

TABLE 4. ARCS questionnaire survey results for the proposed training.

Dimension	No.	Question
Profile	P1	Are you student or do you work?
	P2	Security Learning Periods (Total Month)
Attenssion	A1	Was this training interesting?
	A2	Was this training sleepy?
	A3	Was this training intriguing?
	A4	Was this training in variety?
Relevance	R1	Was this training challenging?
	R2	Was this training related to yourself?
	R3	Was this training what you wanted to master?
	R4	Was this training fun during the process?
Confidence	C1	Did you gain confidence in this training?
	C2	Was the target clear in this training?
	C3	Was it steadily progressing learning with this training?
	C4	Were you able to proceed while developing this training on your own?
Satisfaction	S1	Was it good to play this training?
	S2	Do you think that this training can be used immediately?
	S3	Were you acknowledged if you could do with this training?
	S4	Was the evaluation of this training consistent?

TABLE 5. Mean and standard deviation on arcs questionaire.

No.	G_{SecCap}		G_{ICSCoE}	
	Mean	SD	Mean	SD
P1	1.00	0.00	0.00	0.00
P2	14.45	13.81	24.38	39.51
A1	4.59	0.67	3.95	0.93
A2	4.23	0.87	3.80	1.14
A3	4.50	0.86	3.85	0.95
A4	3.73	0.98	3.27	0.82
R1	4.36	0.73	3.65	1.03
R2	3.55	1.26	3.65	1.03
R3	4.45	0.80	3.88	1.02
R4	4.14	1.04	3.40	1.08
C1	3.73	0.77	3.10	1.01
C2	3.95	0.72	3.33	1.07
C3	4.00	0.93	3.83	0.75
C4	4.14	0.71	3.52	0.85
S1	4.73	0.55	4.05	0.90
S2	3.14	1.08	2.85	0.92
S3	4.14	0.64	3.33	0.53
S4	4.23	0.81	3.75	0.78

TABLE 6. Mean and standard deviation on ARCS Questionaire.

No.	G_{Beginner}		G_{Expert}	
	Mean	SD	Mean	SD
P1	0.43	0.50	0.29	0.46
P2	5.04	1.91	33.88	40.23
A1	4.29	1.01	4.09	0.79
A2	3.96	1.17	3.94	0.98
A3	4.00	1.05	4.15	0.89
A4	3.36	0.95	3.50	0.86
R1	3.96	1.00	3.85	0.99
R2	3.46	1.26	3.74	0.96
R3	4.00	1.09	4.15	0.89
R4	3.64	1.13	3.68	1.12
C1	3.29	1.01	3.35	0.95
C2	3.46	1.17	3.62	0.85
C3	3.93	0.81	3.85	0.82
C4	3.79	0.74	3.71	0.94
S1	4.29	0.98	4.29	0.76
S2	2.86	1.15	3.03	0.83
S3	3.75	0.70	3.50	0.66
S4	4.04	1.00	3.82	0.63

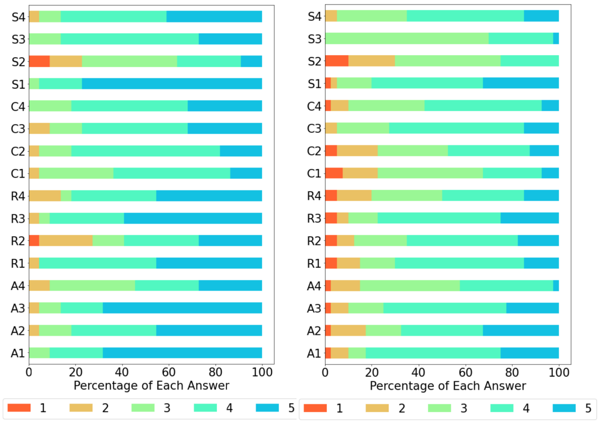

FIGURE 9. Stacked bar of ARCS question (SecCap v.s. ICSCoE).

participants consistently reported mean scores of 3.0 or higher across all questions, indicating a relatively high level of motivation. Conversely, in the ICSCoE session, participants scored lower on average, with question S2 receiving a mean score of 2.85. When comparing the responses between beginners and experts, it was observed that beginners scored lower on question S2 (Relevance) with a mean of 2.86. However, their mean scores for the other questions were above 3.0. On the other hand, the expert group achieved mean scores above 3.0 on all questions.

Analyzing the responses question by question, it was found that both SecCap and ICSCoE participants performed better than beginners in all questions except for R2 (Relevance). Furthermore, both beginner and expert participants tended to excel in the ARCS Attention and Relevance questions, as well as in the Confidence and Satisfaction questions. The beginner group had higher scores in the Confidence and Satisfaction questions compared to the expert group. These results suggest that beginners may have perceived the training content as less directly relevant to their current skill level, leading to lower scores in Attention and Relevance. However, the higher scores in Confidence and Satisfaction indicate that the proposed training still had a positive learning effect on beginners. It is important to note that both beginner and expert groups generally performed well in terms of Attention and Relevance, highlighting the training's ability to engage participants and make the content relevant to their needs.

Overall, the findings indicate that the proposed training program successfully motivated participants, particularly in the SecCap session. The differences observed between beginners and experts shed light on the specific areas where motivation levels may vary. These insights can guide future improvements and customization of the training program to better address the needs of different participant groups.

In the Stacked Bar chart shown in Figure 9 and Figure 10, the distribution of responses to each question item is

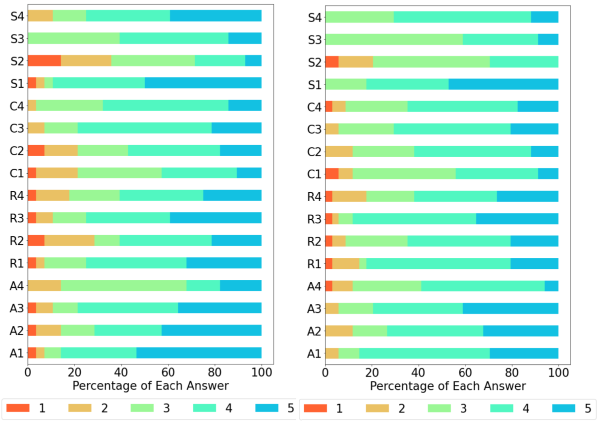

FIGURE 10. Stacked bar of ARCS question (Beginner v.s. Expert).

visualized using colors, with red indicating lower scores and blue indicating higher scores. The chart provides an overview of the participants' responses, highlighting any differences between the SecCap and ICSCoE sessions, as well as between beginner and expert participants. Based on the chart (See Figure 9), it can be observed that participants from SecCap generally responded with higher scores, indicated by shades of blue (4 and 5) for most question items. In contrast, participants from ICSCoE tended to respond with lower scores, with shades of red (1 and 2) being more prevalent. Specifically, many ICSCoE participants provided responses of 1 for each item, indicating a relatively low level of motivation.

When comparing the percentages of beginner and expert participants, there were no significant differences in the distribution of responses (See Figure 10). The chart suggests that the distribution of scores is similar for both groups, with shades of blue (4 and 5) being more prevalent across the questions. Overall, the Stacked Bar chart provides a visual representation of the participants' responses, highlighting the differences in motivation levels between the SecCap and ICSCoE sessions. The predominance of higher scores among SecCap participants suggests a stronger motivation to learn, while the larger proportion of lower scores among ICSCoE participants indicates a need for further improvement in motivation levels. The similarity in the distribution of scores between beginner and expert participants suggests that the proposed training program effectively engages learners across different skill levels.

B. STATISTICAL SIGNIFICANT TEST

In the analysis of the ARCS questionnaire, two hypotheses were formulated for further investigation. The first hypothesis states that there is a significant difference in the response results of the ARCS evaluation sheet between the SecCap and ICSCoE participant groups. The second hypothesis suggests that there is a significant difference in the response results between the participant groups with different years of study (Beginner and Expert). To test these hypotheses, two sections are dedicated to analyzing the data. In Sect V-B1, the focus is on comparing the responses of SecCap and ICSCoE participants to determine if there is a significant difference in their motivation levels. This analysis will help evaluate the effectiveness of the proposed training program for each group. In Sect V-B2, the analysis is centered around comparing the responses of Beginner and Expert participants. The aim is to determine if there is a significant difference in motivation levels between participants with different levels of experience and expertise. This analysis will shed light on the impact of the training program on participants at different skill levels. By conducting these statistical analyses, it will be possible to determine if there are indeed significant differences in motivation levels between the SecCap and ICSCoE participant groups, as well as between the Beginner and Expert participant groups.

1) SECCAP VS. ICSCOE

At this stage, it is crucial to select an appropriate method for testing the significant differences, considering that Likert scale data, such as the ARCS questionnaire, cannot be treated as interval scale quantities. Therefore, the t-test is not applicable in this case. Instead, we will employ nonparametric tests, which do not rely on assumptions about the underlying distribution. Given the difference in sample size between the ICSCoE and SecCap groups, it is preferable to choose a test method that has sufficient power even with a small sample. In this experiment, we will use the Wilcoxon-Mann-Whitney (WMW) test, which is a nonparametric test that meets these requirements. The WMW test for two-sample differences has been extensively studied in the literature. To obtain the test statistic in the WMW test, the observations from groups G_A and G_B are combined to create an independent and identically distributed (i.i.d.) combined sample, denoted as $G_Z = z_1, z_2, \ldots, z_{m+n}$. The observations in G_Z are then ordered:

$$z_{(1)} \leq z_{(2)} \leq \ldots \leq z_{(m+n)} \tag{1}$$

According to the ordered list, R_{i1} is defined as the rank of x_i in G_Z and $R_1 = \sum_{i=1}^{m} R_{i1}$. And we can obtain $U_1 = R_1 - \frac{m(m+1)}{2}$. If the null hypothesis H_0 is true, then

$$Z = \frac{U_1 - E\left(U_1 \mid H_0\right)}{\sqrt{\operatorname{Var}\left(U_1 \mid H_0\right)}} \sim N(0, 1), \tag{2}$$

where

$$E\left(U_1 \mid H_0\right) = \frac{mn}{2}, \operatorname{Var}\left(U_1 \mid H_0\right) = \frac{mn(m+n+1)}{12} \tag{3}$$

Based on the above normal approximation, we can calculate the p-value to test H_0 against H_1 $(F_X(t) < F_Y(t))$ for some t. We set the null hypothesis H_0 and the alternative hypothesis H_1 to test the significance of the WMW test; H_0: G_{SecCap} and G_{ICSCoE} follow the same distribution. H_1: G_{SecCap} and G_{ICSCoE} do not follow the same distribution. Table 1 left shows the results of WMW test. The results of the WMW test showed that 12 of the 16 questions were significantly

TABLE 7. Result of WMW test.

	SecCap vs. ICSCoE		Beginner vs. Expert	
	p-value	Test Statistic U	p-value	Test Statistic U
A1	0.003**	628.5	0.135	573.5
A2	0.170	529.0	0.704	502.0
A3	0.003**	631.0	0.672	447.5
A4	0.099	546.0	0.270	402.0
R1	0.003**	627.0	0.675	503.5
R2	0.889	430.5	0.528	433.0
R3	0.011*	601.0	0.737	453.5
R4	0.008**	615.0	0.912	468.0
C1	0.013*	599.5	0.742	453.5
C2	0.018*	592.5	0.764	455.5
C3	0.295	505.5	0.659	505.0
C4	0.007**	608.5	0.884	486.0
S1	0.001**	644.5	0.728	499.0
S2	0.301	507.0	0.477	428.0
S3	0.000***	714.5	0.137	571.5
S4	0.018*	590.0	0.145	572.0

* is $p < 0.05$, ** is $p < 0.01$, and *** is $p < 0.001$

different between the SecCap and ICSCoE groups, indicating a possible difference in the results of the ARCS questionnaire.

2) BEGINNER VS. EXPERT

Next, we investigate whether there is a significant difference in the results of the ARCS evaluation sheet based on the participants' security background. We define the security background as "Beginner" for those with less than one year of security-related learning experience, and "Expert" for those with one year or more of experience. In this division, we have a sample size of 28 beginners and 34 experts. Similar to the WMW test conducted in Section V-B1, we will use the WMW test to compare the distributions of the beginner and expert groups. We define the null hypothesis (H_0) and the alternative hypothesis (H_1) to verify the significant difference between the beginner group and the expert group: H_0: G_{Beginner} and G_{Expert} follow the same distribution. H_1: G_{Beginner} and G_{Expert} do not follow the same distribution. The test results are shown in the right section of Table 7. The results of the WMW test indicate that there are no significant differences in any of the 16 questions. This suggests that there is no difference between the beginner and expert groups in their responses to the ARCS questionnaire. This result proves that our training does not require a learning history in security area, and we achieve research objective 1 (See Section I).

Based on the results in Tables 6 and 7, we discuss why these significant differences occurred. First, as Tables 6 and 7 show, A1, A4, R1, R4, C1, C4, S1, S3, and S4 were all significantly higher in the SecCap group, that is, students. On the other hand, there were no significant differences in A2, A4, R2, C3, and S2, suggesting that the training progress itself (training time, number of participants, and training content) was not the cause of the significant differences. In other words, it was not the content of the training that was the cause, but the participants. Students, regardless of their security backgrounds, were highly interested in the training, eager to take on challenges, and proactive about self-development, while working professionals tended to focus more on practicality and realistic possibilities. This may be due to the fact that the proposed training was designed to acquire the skill set necessary to become a system architect, and made working professionals feel that system architecting was not really directly related or relevant to their own careers.

C. CORRELATION ANALYSIS

The WMW test identified significant differences between the responses of the SecCap and ICSCoE groups to the ARCS questionnaire. However, the WMW test does not provide information about the correlation between individual items in the questionnaire. To analyze the correlation between the questions, we use Spearman's rank correlation coefficient. Spearman's rank correlation coefficient is a nonparametric measure of the strength and direction of the monotonic relationship between two variables. It assesses how well the relationship between two variables can be described using a monotonic function. By analyzing the correlation between the questions, we can gain insights into the relationships among the motivational factors represented by the ARCS model. This analysis help us understand which factors are more strongly correlated and potentially identify underlying patterns in the participants' responses to the questionnaire.

Tables 8 and 9 display the results of the correlation analysis in the ARCS questionnaire. Correlations of 0.6 or higher are highlighted in bold as particularly strong correlations. In Table 8, which presents the correlation results for the SecCap group, 10 items exhibit particularly strong correlations. Among them, 6 items demonstrate strong correlations with items within the same dimension of the ARCS model (e.g., A1-A3, A2-A3, A3-A4, R2-R3, and C2-C3). Additionally, 4 items exhibit strong correlations with items from different dimensions of the ARCS model (e.g., A2-R3, A2-R4, A3-R3, and A4-R4). Table 9 showcases the correlation results from the ICSCoE group. Out of the 18 correlations examined, 4 items show correlations within the appropriate dimension of the ARCS model, while 14 items display correlations with items from different dimensions.

D. FACTOR ANALYSIS

In the previous section, we conducted a correlation analysis for each group: SecCap and ICSCoE. The results of the analysis indicate that participants in the ICSCoE group did not accurately correlate the dimensional items of the ARCS questionnaire. This suggests the presence of motivational factors among ICSCoE participants that are different from the dimensions outlined in the ARCS model. In order to identify the factors that motivate SecCap (students) and ICSCoE (working professionals) to learn differently, as indicated by the questionnaire results presented in Section V-A, we conduct a factor analysis from the responses to each question item in the ARCS questionnaire.

Factor analysis is a statistical technique used to uncover the underlying structure or common factors that explain the relationships among a set of observed variables. It allows

TABLE 8. Results of correlation analysis of ARCS questionnaire results (SecCap).

No.	A1	A2	A3	A4	R1	R2	R3	R4	C1	C2	C3	C4	S1	S2	S3	S4
A1	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
A2	**0.50**	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—	—
A3	**0.62**	**0.73**	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—
A4	0.26	**0.63**	**0.62**	1.00	—	—	—	—	—	—	—	—	—	—	—	—
R1	0.13	0.24	0.00	0.15	1.00	—	—	—	—	—	—	—	—	—	—	—
R2	0.05	0.19	0.18	0.09	0.24	1.00	—	—	—	—	—	—	—	—	—	—
R3	0.37	**0.60**	**0.62**	0.23	0.19	**0.64**	1.00	—	—	—	—	—	—	—	—	—
R4	0.29	**0.60**	0.51	**0.60**	**0.56**	0.16	**0.50**	1.00	—	—	—	—	—	—	—	—
C1	0.24	0.03	0.22	0.34	-0.33	-0.04	0.13	-0.01	1.00	—	—	—	—	—	—	—
C2	-0.04	0.09	0.19	0.58	0.40	-0.02	-0.13	0.45	0.06	1.00	—	—	—	—	—	—
C3	0.23	0.12	0.18	**0.52**	0.42	0.12	0.06	**0.55**	0.40	**0.64**	1.00	—	—	—	—	
C4	0.12	0.26	0.35	**0.53**	0.08	0.13	0.30	0.36	0.33	0.20	0.29	1.00	—	—	—	—
S1	**0.59**	**0.53**	**0.50**	0.30	0.14	0.22	**0.62**	**0.57**	0.15	-0.03	0.19	0.22	1.00	—	—	—
S2	0.28	0.32	0.33	0.13	-0.19	0.47	0.25	-0.10	0.16	-0.11	-0.00	-0.27	0.07	1.00	—	—
S3	0.47	0.28	**0.56**	**0.52**	-0.32	0.14	0.25	0.04	**0.56**	-0.09	0.16	0.27	0.25	0.45	1.00	—
S4	0.36	0.46	**0.58**	**0.50**	-0.23	0.01	0.27	0.19	0.10	0.10	-0.13	0.27	0.25	0.02	0.49	1.00

TABLE 9. Results of correlation analysis of ARCS questionnaire results (ICSCoE).

No.	A1	A2	A3	A4	R1	R2	R3	R4	C1	C2	C3	C4	S1	S2	S3	S4
A1	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
A2	0.45	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—	—
A3	**0.77**	**0.59**	1.00	—	—	—	—	—	—	—	—	—	—	—	—	—
A4	0.49	0.28	0.42	1.00	—	—	—	—	—	—	—	—	—	—	—	—
R1	**0.73**	0.47	**0.73**	0.49	1.00	—	—	—	—	—	—	—	—	—	—	—
R2	0.46	0.22	**0.52**	0.15	0.44	1.00	—	—	—	—	—	—	—	—	—	—
R3	0.45	0.22	0.43	0.47	**0.52**	**0.67**	1.00	—	—	—	—	—	—	—	—	—
R4	**0.66**	**0.53**	**0.53**	0.45	**0.64**	0.15	0.44	1.00	—	—	—	—	—	—	—	—
C1	**0.63**	0.42	0.47	0.31	**0.60**	0.41	0.46	**0.74**	1.00	—	—	—	—	—	—	—
C2	**0.58**	0.39	**0.58**	0.42	**0.50**	0.41	0.44	**0.62**	**0.68**	1.00	—	—	—	—	—	—
C3	0.24	0.29	0.29	0.38	0.05	0.15	0.34	0.25	0.23	0.49	1.00	—	—	—	—	—
C4	0.29	0.30	**0.52**	0.05	0.39	0.39	0.26	0.18	0.12	0.23	0.35	1.00	—	—	—	—
S1	**0.76**	0.48	**0.70**	0.40	**0.63**	0.43	0.48	**0.69**	**0.61**	**0.67**	0.39	0.27	1.00	—	—	—
S2	**0.50**	0.22	**0.53**	0.19	**0.54**	**0.68**	0.42	0.27	0.40	0.28	0.04	0.40	0.47	1.00	—	—
S3	0.19	0.24	0.36	0.03	0.26	0.17	-0.02	0.17	0.28	0.31	0.41	0.36	0.29	0.32	1.00	—
S4	0.19	0.12	0.23	0.48	0.27	0.18	0.48	0.27	0.26	**0.59**	**0.59**	0.17	0.24	-0.05	0.33	1.00

us to identify the hidden factors or latent variables that contribute to the observed phenomena. By examining the interrelationships among variables, factor analysis helps us understand the complex patterns and underlying dimensions present in the data. We also provide an explanation of the statistical model in factor analysis. Consider a scenario where we have a set of m random variables, $x_1, \ldots, x_m$. Each variable is assumed to have a population mean of $\mu_1, \ldots, \mu_m$, respectively. In factor analysis, our goal is to explain these variables using p common factors, $f_1, \ldots, f_p$, through the following linear model:

$$x_j - \mu_j = \lambda_{j1}f_1 + \lambda_{j2}f_2 + \cdots + \lambda_{jp}f_p + \varepsilon_j \quad (j = 1, \ldots, m) \tag{4}$$

In Equation (4), the coefficients $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{mp-1}, \lambda_{mp}$ are known as factor loadings, which can be considered analogous to the partial regression coefficients in multivariate regression analysis. Furthermore, ε_j represents the unique factor (also known as the specific factor) for variable x_j. It is important to note that this assumption of unique factors differs from the assumption of observation error in a typical linear regression model. To express the above model using vectors and matrices, we have:

$$\mathbf{x} - \boldsymbol{\mu} = \Lambda \mathbf{f} + \boldsymbol{\varepsilon} \tag{5}$$

In Equation (5), $\mathbf{x}$ and $\boldsymbol{\mu}$ are vectors, Λ is a matrix of factor loadings, $\mathbf{f}$ is a vector of common factors, and $\boldsymbol{\varepsilon}$ is a vector of unique factors. By examining the large observed variables in Λ from Equation (5), we can interpret the factors.

The primary purpose of conducting factor analysis in this study is to identify the common factors or motivational factors that influence participants' responses to the ARCS questionnaire. These factors may not be directly observable, but through factor analysis, we can estimate and extract them from the data. This enables us to gain a deeper understanding of the underlying motivational aspects that may be driving participants' responses. In the factor analysis, we use maximum likelihood estimation and promax rotation to maximize the factor loadings on each axis.

In the factor analysis, a criterion of an eigenvalue of 0.5 or higher was used to identify the factors. Based on the difference in eigenvalues for the cumulative contribution ratio and the number of factors, two factors were assumed for SecCap and three factors for ICSCoE. For the SecCap group,

TABLE 10. Results of the factor analysis.

	SecCap		ICSCoE		
	Factor 1	Factor 2	Factor 1	Factor 2	Factor 3
A1	0.64	0.01	0.81	0.18	-0.14
A2	0.67	0.24	0.53	0.06	0.01
A3	0.87	0.10	0.52	0.45	-0.03
A4	0.51	0.47	0.50	-0.15	0.28
R1	-0.25	0.73	0.72	0.28	-0.17
R2	0.27	0.06	-0.03	0.82	-0.02
R3	0.61	0.11	0.28	0.30	0.22
R4	0.25	0.86	1.07	-0.32	-0.04
C1	0.38	-0.09	0.79	-0.02	-0.02
C2	-0.14	0.69	0.56	-0.03	0.41
C3	0.03	0.65	-0.08	0.03	0.82
C4	0.29	0.30	-0.14	0.61	0.16
S1	0.54	0.19	0.73	0.14	0.02
S2	0.47	-0.30	0.12	0.83	-0.29
S3	0.79	-0.29	-0.05	0.29	0.30
S4	0.59	-0.09	0.01	-0.14	0.90

the first factor showed large factor loadings for all items in the Attention dimension, all items in the Satisfaction dimension except S2, and R3. Interestingly, despite R3 being a question related to the Relevance dimension, it appeared to reflect the trainees' desire to master the training, which is closely related to the attractiveness and interest in the training itself (similar to A1 and S1). Therefore, this factor was interpreted as "Training attractiveness". In the second factor for SecCap, the factor loadings for C2, C3, R1, and R4 were prominent. All these questions assessed the progression of training. The high mean values and small standard deviations indicated that the SecCap participants, as a whole, had a positive impression of the training progress. Consequently, this factor was interpreted as "Training Smoothness".

In the ICSCoE group, the factor analysis revealed three distinct factors, which we will now interpret in detail. The factor loadings of A1, R1, R4, C1, and S1 were found to be substantial in the first factor. These questions share a common theme of assessing the training experience. Thus, we interpret this factor as "Training Experience," capturing participants' perceptions and evaluations of their overall training experience. The second factor consists of S2 and R2, which are different questions within the ARCS dimensions. However, both items focus on the relevance of the training to actual security work. Considering that the ICSCoE group comprises working professionals capable of assessing the practical utility of the training in their jobs, we interpret this factor as "Training Utility." It reflects participants' perceptions of the extent to which the training is beneficial and applicable to their professional roles. The third factor exhibits substantial factor loadings for C3 and S4. These items are crucial for the training process, as inconsistent content and difficulty impede steady learning progress. Notably, unlike the SecCap group, the questions related to the Relevance dimension in the ARCS did not demonstrate high factor loadings in this factor. This suggests that the third factor primarily assesses the coherence and difficulty of the training content, rather than its direct relevance to participants' background. Therefore, we interpret this factor as"Training Difficulty," representing the challenges and complexity associated with the training materials and tasks. To summarize, the factor analysis in the ICSCoE group revealed three distinctive factors: Training Experience, Training Utility, and Training Difficulty. These factors provide valuable insights into different aspects of participants' perceptions and experiences regarding the training program within the ICSCoE context.

1) QUALITATIVE ANALYSIS

Finally, we discuss the results of the discussion-based training, focusing on the policy creation process. We observed a noticeable bias in the policies developed by each group.

The student groups predominantly created policies that employed a point reduction method to calculate trust scores. These policies incorporated common monitoring features, such as hardware identifiers like MAC addresses and client certificates, as well as contextual features, including the volume of data acquired within a short time frame, the rarity of the destination mail domain, and the frequency of access. These features were considered crucial for assessing the trustworthiness of the entities involved.

In contrast, the working group also utilized similar monitoring features as the student groups, but they exhibited a preference for designing conditional policies rather than scoring policies. The choice of conditional policies stemmed from several factors. Firstly, the working group found it challenging to establish the validity of the confidence score calculation formula inherent in scoring-type policies. Secondly, accountability for the return location posed a significant challenge. Consequently, the working group opted for conditional policies, which allowed for more specific criteria to be defined in response to different conditions or events.

The contrasting policy approaches between the student and working groups highlight the differences in their perspectives and considerations. While the students focused on score-based assessments, the working group prioritized conditional policies to address the challenges of validity and accountability in their particular context. Understanding these divergent approaches provides valuable insights into the decision-making processes and considerations of different participant groups within the training program. Since the results reveal the imposition of learning motivation and its common factors and differences between the SecCap and ICSCoE groups, we achieve research objective 2 (See Section I).

VI. CONCLUSION

There are a lot of the proposal and increased attention towards cyber security training programs to gain security personnel. But the existing training programs focus on acquiring knowledge of security technologies and practicing incident response and often fail to provide the skills necessary for system architecture, such as system design and scaling.

In this study, we proposed a cyber security training program (CYTØRUS) aimed at cultivating system architects by fostering internal motivation for learning. The training was designed and implemented based on the ADDIE model, a well-established instructional design framework, with the objective of motivating participants to learn system architecture. CYTØRUS encompasses a step-by-step approach to zero-trust system design and implementation, accompanied by group discussions using a virtual company as a context. It encompasses six key skills essential for system architects, including system scalability and security. To assess the effectiveness of the training program, we conducted an analysis of the ARCS questionnaire, which is designed to measure motivation for learning. The findings revealed that the ARCS questionnaire successfully motivated both novice and experienced security professionals to engage in learning activities. Furthermore, the analysis highlighted differences in learning motivation between student participants and professionals. This results suggest that work experience is more important than academic history in the field of security, and that participants' impressions of the training vary greatly depending on their work experience. Building upon these outcomes, we believe that CYTØRUS has the potential to significantly enhance students' motivation to learn system architecture.

There are two important avenues for future work in this reserach. Firstly, it is crucial to investigate the sustainability of participants' learning motivation over time. Learning motivation can be challenging to sustain continuously and may diminish after a certain period. Therefore, it is imperative to examine whether the learning motivation generated by the training program persists beyond the training period and, if not, identify the factors contributing to its decline. Secondly, it is essential to compare CYTØRUS with other cyber security training programs that focus on non-zero-trust themes. Numerous training approaches, such as Capture The Flag (CTF), gamification, and hardening, have been proposed in the field of cyber security. A comparative analysis between these programs and system design training programs, like CYTØRUS, will enable us to identify the specific knowledge and skills that can be acquired through each approach, as well as any limitations or gaps in their respective coverage. Addressing these research directions will provide valuable insights into the long-term effectiveness of the training program and its unique contributions in the broader landscape of cyber security education and skill development.

REFERENCES

[1] K. J. Andreasson, *Cybersecurity: Public Sector Threats and Responses*. Taylor & Francis, 2011.

[2] *10 Major Threats to Information Security 2018*. Accessed: May 16, 2023. [Online]. Available: https://www.ipa.go.jp/files/000065376.pdf

[3] R. M. Gagne and L. J. Briggs, *Principles of Instructional Design*. Holt, Rinehart & Winston, 1974.

[4] P. L. Smith and T. J. Ragan, *Instructional Design*. Hoboken, NJ, USA: Wiley, 2004.

[5] J. Sweller, "Instructional design," in *Encyclopedia of Evolutionary Psychological Science*. Berlin, Germany: Springer, 2021, pp. 4159–4163.

[6] R. M. Branch, *Instructional Design: The ADDIE Approach*, vol. 722. Berlin, Germany: Springer, 2009.

[7] J. M. Keller, "Development and use of the ARCS model of instructional design," *J. Instructional Develop.*, vol. 10, no. 3, pp. 2–10, Sep. 1987.

[8] J. Kim and J. Shim, "Development of an AR-based AI education app for non-majors," *IEEE Access*, vol. 10, pp. 14149–14156, 2022.

[9] P.-H. Lin, Y.-M. Huang, and C.-C. Chen, "Exploring imaginative capability and learning motivation difference through picture e-book," *IEEE Access*, vol. 6, pp. 63416–63425, 2018.

[10] N. Refat, M. A. Rahman, A. T. Asyhari, I. F. Kurniawan, M. Z. A. Bhuiyan, and H. Kassim, "Interactive learning experience-driven smart communications networks for cognitive load management in grammar learning context," *IEEE Access*, vol. 7, pp. 64545–64557, 2019.

[11] S. F. Noorani, M. H. Manshaei, M. A. Montazeri, and Q. Zhu, "Game-theoretic approach to group learning enhancement through peer-to-peer explanation and competition," *IEEE Access*, vol. 6, pp. 53684–53697, 2018.

[12] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing zero trust cloud networks with transport access control and first packet authentication," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2016, pp. 5–10.

[13] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021.

[14] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic access control and authorization system based on zero-trust architecture," in *Proc. Int. Conf. Control, Robot. Intell. Syst.*, Oct. 2020, pp. 123–127.

[15] S. Mandal, D. A. Khan, and S. Jain, "Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic," *New Gener. Comput.*, vol. 39, nos. 3–4, pp. 599–622, Nov. 2021.

[16] T. Sasada, Y. Masuda, Y. Taenaka, Y. Kadobayashi, and D. Fall, "Zero-trust access control focusing on imbalanced distribution in browser clickstreams," in *Proc. 8th Int. Conf. Softw. Defined Syst. (SDS)*, Dec. 2021, pp. 1–8.

[17] *Homeland Security Exercise and Evaluation Program*. Accessed: May 16, 2023. [Online]. Available: https://preptoolkit.fema.gov/documents/1269813/1269861/HSEEPRevisionApr13Final.pdf

[18] *CYDER: CYber Defense Exercise With Recurrence*. Accessed: May 16, 2023. [Online]. Available: https://cyder.nict.go.jp/

[19] (2017). *CIIREX: Critical Infrastructure Incident Response EXercise*. Accessed: May 16, 2023.. [Online]. Available: https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf

[20] R. Beuran, D. Tang, C. Pham, K.-I. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE," *Comput. Secur.*, vol. 78, pp. 43–59, Sep. 2018.

[21] T. Omiya and Y. Kadobayashi, "Secu-one: A proposal of cyber security exercise tool for improving security management skill," in *Proc. 7th Int. Conf. Inf. Educ. Technol.*, Mar. 2019, pp. 259–268.

[22] J. Downey, "Systems architect and systems analyst: Are these comparable roles?" in *Proc. ACM SIGMIS CPR Conf. Comput. Personnel Res., 44th Years Comput. Personnel Res., Achievements, Challenges Future*, Apr. 2006, pp. 213–220.

TAISHO SASADA (Student Member, IEEE) received the B.S. degree in culture and information science from Doshisha University, in 2020, and the M.Sc. degree in engineering from the Nara Institute of Science and Technology (NAIST), in 2021, where he is currently pursuing the Ph.D. degree. He is a Research Fellow (DC1) with the Japan Society for the Promotion of Science (JSPS) and a Research Assistant with NAIST. His research interests include privacy enhancing technologies, access control, data resampling, and machine/deep learning security.

MASATAKA KAWAI received the B.S. degree from the Muroran Institute of Technology, Hokkaido, Japan, and the M.S. degree from the Nara Institute of Science and Technology, Nara, Japan. He holds an OSCP Certificate. He is currently with the DX Security Consulting Business Division, NRI Secure Technologies Ltd., Tokyo, where he was involved in the research and development of vulnerability assessment and penetration testing. In addition to vulnerability assessment, he has launched a new service related to breach and attack simulation (BAS) tools, while working to further enhance penetration testing services.

YUTO MASUDA received the B.S. degree from the University of Hyogo, Japan, and the M.S. degree from the Nara Institute of Science and Technology, Japan. He holds an OSCP Certificate. He is currently with the DX Security Consulting Business Division, NRI Secure Technologies Ltd., Tokyo, where he has actively contributed to research and development in vulnerability assessment and penetration testing.

YUZO TAENAKA (Member, IEEE) received the D.E. degree in information science from the Nara Institute of Science and Technology (NAIST), Japan, in 2010. He was an Assistant Professor with The University of Tokyo, Japan. Since April 2018, he has been an Associate Professor with the Laboratory for Cyber Resilience, NAIST. His research interests include information networks, cybersecurity, distributed systems, and software defined technology.

YOUKI KADOBAYASHI (Member, IEEE) received the Ph.D. degree in computer science from Osaka University, Japan, in 1997. Since 2013, he has been a Rapporteur of ITU-T Q.4/17 for cybersecurity standardization. He is currently a Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Japan. His research interests include cybersecurity, web security, and distributed systems. He is a member of the IEEE Communications Society.