CRICE: Cyber Range Infrastructure for Cybersecurity Education

Sajal Bhatia
Sacred Heart University
Fairfield, USA
bhatias@sacredheart.edu

Irfan Ahmed
Virginia Commonwealth University
Richmond, USA
iahmed3@vcu.edu

Nitin Talreja
Optum Services Inc. (United Health Group)
Hartford, USA
nitin_talreja@uhc.com

2025 5th Intelligent Cybersecurity Conference (ICSC) | 979-8-3503-9292-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICSC65596.2025.11140374

***Abstract*—Professionals in the cybersecurity field are in high demand in industry and government. Community colleges have a significant student population that has the potential to enable a new stream of cybersecurity professionals and meet the demand. However, community colleges often lack sufficient computing infrastructure to actively support hands-on learning of cybersecurity concepts, tools, and techniques. To assist community colleges without an extensive computing infrastructure, this paper proposes CRICE, a Cyber Range Infrastructure for Cybersecurity Education using NSFCloud, an open-access and free cloud service, funded by the National Science Foundation (NSF) and designed for academic education, research, and training purposes. CRICE aims to bring community college students into the high-rewarding cybersecurity field to secure and support the United States' cyber infrastructure.**

***Index Terms*—Cybersecurity, Education, Cyber Range, NSF, Cloud, Community College**

I. Introduction

Due to the high demand for cybersecurity professionals in industry and government, academia faces challenges in producing diverse and high-quality professionals. Unfortunately, demand exceeds the supply of students [1]. Community colleges can play a crucial role in meeting the demand for cybersecurity professionals. They have a significant student population of low-income, diverse, first-generation college students, which has the potential to enable a new stream of cybersecurity professionals. Unfortunately, community colleges face several challenges in introducing effective cybersecurity programs for cyberinfrastructure, including a lack of an effective curriculum compatible with the student population, insufficient computing infrastructure to support hands-on exercises and assignments, and limited credit hours to accommodate cybersecurity courses.

Recent statistics from the American Association of Community Colleges (AACC) indicate that 10.2 million undergraduates are enrolled in more than 1,100 two-year colleges [2]. The demographics of the students are diverse, including 28% Hispanic, 12% Black, 43% white, and 6% Asian. Interestingly, 32% of students are first-generation college students, and 13% are single parents. Provisional data from the National Center for Education Statistics (NCES)[3] indicate that a significant percentage of low-income students attend community colleges.

The overarching goal of this research is to target the next generation of cyber-infrastructure professionals (CIP) by proposing to integrate core literacy and advanced cybersecurity skills into the undergraduate curriculum of community colleges [4]. To achieve this goal, this paper proposes CRICE, a cyber range infrastructure for cybersecurity education using NSFCloud. CRICE is a free, scalable, hands-on learning environment for community college students, preparing them for a high-rewarding cybersecurity career and, in turn, helping to address the national shortage of technical staff in cybersecurity.

The remainder of the paper is organized as follows: Section II describes the cyber range concept and infrastructure. It also presents a detailed description of state-of-the-art cyber ranges. Section III provides an overview of the NSFCloud platforms and their usage in computing education and research. Section IV presents the proposed CRICE infrastructure, including the basic workflow, architecture, and resource management. Section V summarizes the work and provides directions for future research.

II. Cyber Range Concept and Infrastructure

In general terms, a cyber range is a virtual environment for cybersecurity training and development. The concept originated within the U.S. military's National Cyber Range (NCR) initiative. A cyber range can be considered similar to a kinetic range, in that it facilitates training in operations or tactics. Thus, cybersecurity professionals can use the cyber range as a safe environment for developing and testing new tools and methodologies for counterattacking and responding to security attacks and threats. Initially developed by cybersecurity industry leaders, such as Raytheon Technologies and Palo Alto Networks, cyber ranges have recently been implemented at the state level. Examples of publicly funded cyber ranges that are operated by states include systems in Maryland [5], Michigan [6], and Virginia [7]. Note that these latter examples make resources available within their state to educational institutions but are inaccessible to other states.

Cyber ranges can be mainly categorized as hardware-based cyber ranges (HCR) or virtual cyber ranges (VCR). HCRs rely on underlying IT security infrastructures and data center environments that provide trainees a real hands-on experience. VCRs rely on cloud-based resources and contain ready-made, virtual cyber infrastructures and other cybersecurity mechanisms to help students understand core cybersecurity concepts.

979-8-3503-9292-0/25/$31.00 ©2025 IEEE

One primary benefit of the VCR approach is that it provides a flexible laboratory environment that is accessible by remote users without geographic constraints.

A. *State-of-the-Art in Cyber Range Infrastructure*

Early simulation-based cybersecurity training frameworks provided relevant educational content. Unfortunately, they were not well received by the cybersecurity community, due to a lack of realistic scenarios as well as steep learning curves. Recently, several educational cyber range environments have been proposed and implemented to provide realistic scenarios on a cloud-computing infrastructure [8–11]. Note that they are based on fee-based subscription models, which may not be affordable for community colleges with their limited budgets. Also, their educational content is mainly designed for a university-level curriculum and is not as suitable for community colleges.

As one of the first well-known examples of a network-based cybersecurity experimental laboratory, Peterson and Reiher created a collection of computers and routers that can be configured dynamically and accessed over the network, called the DETERlab (cyber-DEfense Technology Experimental Research laboratory) [11]. Using custom Linux images and open-source cybersecurity tools, realistic security exercises were provided on a 300-node medium-scale testbed. Although virtualization was also an initial consideration as a core enabling mechanism for running cybersecurity tests, at the time, it was too early to utilize virtual resources due to: (i) inherent overhead in managing the storage footprint of virtual machine (VM) images, (ii) the requirement for most tests for multiple hosts, and (iii) the overhead of keeping up with the changes in VM images. The current implementation of DETERlab is based on Emulab software, and it is jointly run by the University of Southern California Information Sciences Institute and the University of California, Berkeley. As with other Emulab-based research testbeds, DETERlab has a steep learning curve for setting up content-specific experiments; in particular, it requires hands-on knowledge of UNIX command-line utilities.

Weiss et al.'s EDURange [8] is a collection of cloud-based resources for hosting flexible, interactive cybersecurity scenarios using an Amazon Web Services (AWS) platform. Using Chef as a cloud orchestration and management tool, along with the YAML descriptive language for customized scenarios, multiple cloud instances can be deployed for a set of cybersecurity exercises. Although it is still in its early stages, EDURange has provided invaluable insights into using cloud-based resources for cybersecurity training. A number of exercises were developed under EDURange; each exercise is designed to address particular information assurance and security (IAS) goals in ACM/IEEE CS2013 Curricula [12]. These exercises were designed to cover the core cybersecurity topics of network diagramming and monitoring, access control policies, reconnaissance, malware and infection analysis, and network diagramming and monitoring. Similar to DETERlab, EDURange also has a steep initial learning curve due to its requirements for terminal-based UNIX command line tools and other manual cloud deployment methodologies on AWS, as well as the need to learn YAML to describe cybersecurity scenarios for deployment. In addition, each instructor must set up an AWS account and manually configure nodes on AWS.

SCREDENT is a cloud-based cybersecurity tool [9] that extends mobile malware detection to include cloud-based analysis methodologies using open-source tools. Based on a security malware database and a malware analysis tool, it employs behavior-triggering Markovian models to detect suspicious behavior. Its cloud-based library allows SCREDENT to scale its analysis using Docker container technology as the testbed platform.

ThoTh Lab (formerly V-Lab) is a true cloud-based virtual laboratory platform for hands-on networking courses [10]. It uses a Xen-based hypervisor and virtual local area network (VLAN) technology to deploy scalable cloud infrastructures. This allows students to create, configure, and monitor common network elements, as well as build network security exercises in the cloud. ThoTh Lab has a web-based graphical user interface that is used to allow novice users to experiment with core security concepts, eliminating the need to introduce command-line UNIX tools into the curriculum. ThoTh Lab's curriculum approach focuses on the following learning factors: motivation, knowledge, creativity, collaboration, demonstration, and feedback. Initially developed for proprietary hypervisors, the recent version of ThoTh Lab can also run with Linux-based KVM hypervisors; thus, it can take advantage of OpenStack-based research clouds. ThoTh Lab would be an implementation that is very close to our proposed system; however, it is designed to be proprietary, and it requires a fee-based subscription.

RAVE Lab (formerly ASSERT Lab) is another project for sharing virtual machines with academic institutions across the country. RAVE is based on vSphere, a proprietary cloud provisioning tool by VMware. vSphere allows custom scenarios to be automated. RAVE scenarios, which include an enhanced set of various security concepts such as cryptography, public key infrastructure, authentication, intrusion detection systems, and secure software development, can be deployed on isolated networks. Unlike CRICE, which is based on an open-access model, NSFCloud and RAVE Lab use a closed cluster supported by several higher education institutions across the country.

In summary, CRICE is unique in that it supports free, hands-on learning for community college students without requiring a substantial investment in computing infrastructure.

III. NSFCloud Platforms

In 2014, the National Science Foundation (NSF) awarded $20 million through its CISE Research Infrastructure program to develop test environments supporting applied computing research [13]. As described by Mambretti et al., the NSF Cloud Initiative led to the creation of two large-scale distributed testbeds – Chameleon [14] and CloudLab [15], which enable cloud experimentation and integration with software-defined networking (SDN) [16]. Both testbeds provide interfaces similar to commercial cloud platforms (e.g., Amazon Web Services, Google Cloud) and offer researchers bare-metal access and control. The Chameleon Cloud, spanning over 550 nodes across two sites, is highly reconfigurable and available to the U.S. computer science research community. CloudLab, on the other hand, comprises 15,000 cores at three physical sites, focusing on storage, networking, high-memory, and energy-efficient computing [17]. Both platforms received renewed funding in 2017 and continue to serve the scientific community.

A. NSFCloud Testbeds for Research and Experiments

Since their inception, the two NSF testbeds have been widely utilized for applied computing research. Research summarized in this section highlights how NSFCloud environments have supported diverse experimental work [18]. For example, Chameleon Cloud, built on OpenStack, enables the deployment of large numbers of parallel, programmable virtual networks on a single infrastructure. Researchers use Chameleon Cloud in three primary ways: as a component within broader experiments, for exploring novel cloud architectures, and for investigating foundational infrastructure layers. The platform supports four core network services – Layer 3 (L3) networking, Layer 2 (L2) networking, SDN, and hybrid SDN/non-SDN networks. Its architecture separates the control and data planes, and ongoing developments aim to enhance network isolation for bare-metal nodes that are developed for the testbed.

Lama et al. [19] demonstrate how the Chameleon Cloud testbed enables performance testing of cloud storage systems. Researchers implemented 'DLR'—a dynamic load redistribution system designed to optimize throughput and latency in heterogeneous hardware environments—using Ceph, Chameleon's distributed object storage platform. By simulating low I/O bandwidth conditions on half of the testbed nodes, they validated DLR's ability to mitigate hardware variability and performance interference. Noel et al. [20] details a machine learning system deployed on Chameleon Cloud using Ceph's distributed object storage architecture. Their implementation enables autonomous load balancing and self-management capabilities for cloud storage systems. The experiment utilized an 8-node Ceph cluster configured with two storage containers, featuring nodes equipped with 2.3 GHz Intel Xeon E5-2650 v3 processors, 80GB storage, and 16GB memory running Ubuntu Linux. Beck et al. [21] discuss how NSF-funded cloud testbeds like CloudLab and GENI can address infrastructure gaps in underserved regions by providing advanced network and storage resources. Data Logistics Networks (DLN) could leverage these platforms to expand Data Logistics Toolkit (DLT) services, enabling communities with limited local storage to access distributed 'big data' storage solutions across nearby locations.

Mandal et al. [22] discuss how NSFCloud testbeds enable realistic simulations for training machine learning models. Their work highlights ML applications in analyzing data from distributed scientific workflows across national-scale cyberinfrastructure, detecting unintentional data anomalies and integrity errors, and diagnosing their sources to ensure validity and reliability of results. Purohit et al. [23] demonstrate how the NSFCloud platform can be utilized to develop and test new security solutions. Specifically, it details the creation and evaluation of a defense system called "DefenseChain" on the NSFCloud testbed using Hyperledger Composer, a toolset for building blockchain networks. DefenseChain leverages blockchain architecture to detect and mitigate cyberattacks. The study includes visual representations of the NSFCloud testbed configuration used to assess DefenseChain's performance and its software-defined networking (SDN) capabilities.

IV. Proposed CRICE Platform

The authors present a freely accessible, cloud-based cyber range infrastructure for cybersecurity education (CRICE). The proposed infrastructure utilizes NSFCloud (an open-access cloud infrastructure funded by the NSF), and supports student-centric learning by providing a computing infrastructure platform for hands-on activities. The primary purpose of CRICE is to reduce the burden on community colleges of maintaining their expensive computing infrastructure, allowing them to utilize the proposed training modules effectively. CRICE has two objectives: first, hosting virtual machines (VMs) to support hands-on learning; second, allowing novice users of a cloud deployment to utilize computing infrastructure efficiently and easily. The authors have used open-source cloud provisioning and orchestration tools to provide solutions that novice cybersecurity learners can easily interact with, easing the learning curve for cloud deployment.

A. NSFCloud for Cybersecurity Training

CRICE uses NSFCloud infrastructure and provides a nearly ideal environment for resource-constrained community college students to master the key cybersecurity skills required in the real world. CRICE employs a multi-layered approach to isolate attacks, preserve integrity, and protect its infrastructure, especially when used by learners conducting potentially disruptive or malicious experiments. Specifically, CRICE provides the following salient feature set:

- Real-World Simulation: Cloud-based cyber ranges provide a simulated desktop environment where students can experience real-world cyber threats, such as phishing or ransomware attacks, without risking the live network. These labs will provide scenario-based training that mimics real-world cyber threats, allowing learners to practice identifying and mitigating attacks, such as phishing or ransomware, in a risk-free environment. Virtualized networks will enable students to test malware, new security strategies, or software without affecting live systems.
- Hands-On and Interactive Learning: These labs enable hands-on training for both technical and non-technical staff, fostering a cybersecurity-focused culture through direct experience. Features like Automated assessments, Real-time progress tracking, and Gamified challenges

will engage learners and reinforce key concepts through hands-on practice.
- Scalability and Accessibility: NSFCloud labs will be accessible from any device with an internet connection, enabling "on-demand learning" and supporting multiple users simultaneously without the need for physical infrastructure. NSFCloud-based labs will be highly scalable and accessible, making them ideal for large or distributed teams.
- Instructor Control and Monitoring: Instructors can track student progress, provide live coaching, and customize exercises to adjust difficulty levels, ensuring a structured and guided learning experience.
- Real-Time Cloud System Updates: With automatic security updates, NSF public cloud ensures defenses are always current against evolving threats and the system is up and running with latest software updates.
- Reduced Maintenance: NSFCloud labs eliminate the need for physical infrastructure, lowering maintenance costs and complexity to maintain VMs and expensive software licenses.
- Customizable Isolation Granularity: Users can select between bare-metal nodes for full hardware isolation or KVM-based virtualized environments for finer-grained, yet still logically separated, experiments. Bare-metal allocation provides the highest level of isolation, while KVM instances offer resource efficiency with logical separation.
- Reuse Potential: CRICE developed on Chameleon Cloud framework will have its reusable cybersecurity labs through its customizable infrastructure, automation tools, and artifact-sharing capabilities through Chameleon Trovi and federated authentication.

These benefits make CRICE a practical and effective solution for cybersecurity training and testing. CRICE prioritizes research needs over general-purpose cloud features, offering tailored tools for large-scale, reproducible experiments. Its bare-metal access provides cost effective, high-fidelity environments compared to commercial alternatives. It will help collectively create an immersive, practical, and scalable learning experience, essential for developing cybersecurity skills.

B. *Workflow, Resource Management and User Authentication*

Robust security protocols are essential for protecting sensitive data and providing a safe learning environment. The secure creation of key pairs and configuration of SSH access underscore the developed model's strong security measures. These practices ensure secure access to cloud instances, maintaining the integrity and confidentiality of educational environments in CRICE. Every time a user needs to log in to the Cloud server, they would have to use a capable SFTP client (puTTYgen) to enter their username and password and then load their SSH private key. The SFTP client will then use the private key to generate a digital signature that the server can validate and match with the user's account through the corresponding public key stored there. The cloud instance ensures a streamlined activation process, allowing users to easily initiate virtual machines with preconfigured settings. The instances are tailored to educational requirements, enabling seamless integration with existing curricula. Here, the User, after authentication, makes the request via CLI. The request for the resource (VM) allocation is enqueued at Resource provisioning. The Information is then sent to Cloud Resource Manager, which is further sent to Chameleon IaaS (Infrastructure as a Service) for allocating the VMs. From the pool of VMs, the allocation is done, and the resources are allocated based on the user demand.

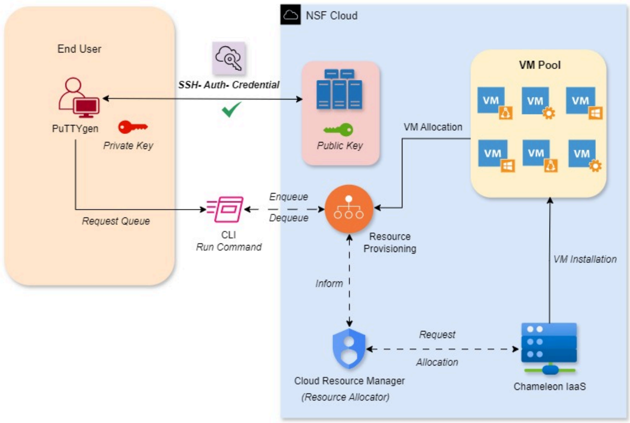

Fig. 1: CRICE Workflow, Resource Management & User Authentication

V. Conclusion and Future Work

Cybersecurity education and training play a pivotal role in addressing the gap between the demand and supply of cybersecurity professionals. Community colleges have a significant student base that is entirely capable of addressing this gap and meeting the demand. However, community colleges often lack sufficient computing infrastructure to support hands-on learning in cybersecurity, a necessity for excelling in the field. In this paper, the authors address this shortcoming by presenting a cyber range infrastructure for cybersecurity education (CRICE) that utilizes an open-access and free cloud service provided by the NSF for academic research and education. This proposed work-in-progress platform provides a controlled, scalable, accessible, and cost-efficient hands-on learning environment aiming to assist resource-limited community colleges and their students break into the rewarding field of cybersecurity, and in-turn address the national shortage of technical staff in cybersecurity. As part of future work, the authors plan to incorporate a virtual machine (VM) management mechanism and develop a user interface portal for CRICE. Both future work directions are described below.

Cloud Instance and VM Management: CRICE plans to use tools like Heat, an open-source orchestration tool for OpenStack, for cloud orchestration as shown in Figure 2. The model's ability to automate instance management provides a practical foundation for this approach, ensuring efficient

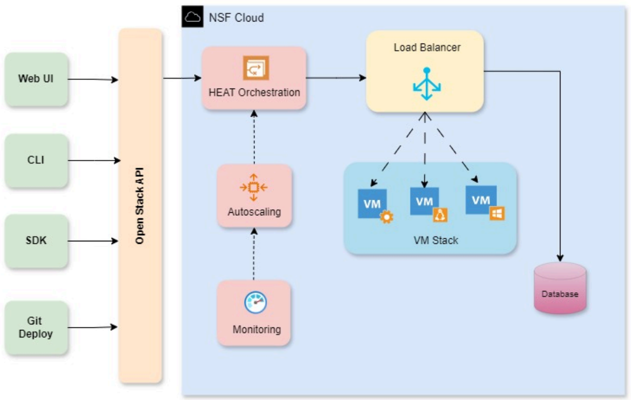

Fig. 2: CRICE Cloud Instance & VM Management

and scalable deployment of virtual learning environments. OpenStack, an open-source platform, provides advanced virtualization and software-defined networking (SDN) for efficient resource management and network optimization. It helps to orchestrate data center operations on bare metal cloud resources. Its APIs enable users to script and automate cloud environments, databases, and security configurations. Heat, OpenStack's orchestration engine, automates infrastructure deployment using templates, allowing for the creation of complex cloud applications. DevStack simplifies OpenStack deployment from Git repositories, making it easier to experiment and develop. This setup supports interactive and competency-driven learning experiences by providing a flexible and scalable infrastructure for cybersecurity initiatives, which enhances collaboration and educational outcomes in virtual environments.

CRICE Portal: While this workflow, outlined in Figure 1, is straightforward for a skilled cloud user, we envision a much simpler interface for our cybersecurity audience. Using a common portal, users will be able to choose to deploy and run a virtual learning environment for each of the developed hands-on learning modules as a part of this project. Figure 3 depicts this scenario.

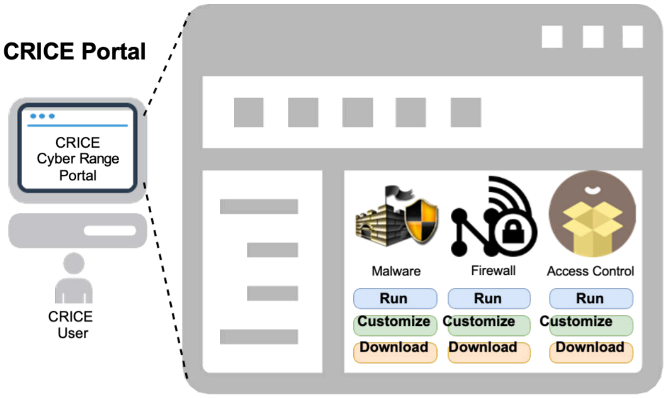

Fig. 3: CRICE Portal

Acknowledgment

This work is supported by the National Science Foundation under Grant Award Numbers 2017337 and 2017371

References

[1] NIST, "Hack the Gap Close the Cybersecurity Talent Gap with Interactive Tools and Data," https://www.cyberseek.org/, [Accessed 22-03-2025].

[2] AACC, "Association of Community Colleges (AACC)," https://www.aacc.nche.edu/research-trends/fast-facts/, [Accessed 22-03-2025].

[3] NCES, "National Center for Education Statistics (NCES)," https://nces.ed.gov/, [Accessed 22-03-2025].

[4] S. Bhatia, S. Elhadad, and I. Ahmed, "PATCH: Problem-Based Learning Approach for Teaching Cybersecurity and Ethical Hacking in Community Colleges," in *2024 17th International Conference on Security of Information and Networks (SIN)*. IEEE, 2024, pp. 1–9.

[5] BCR, "Baltimore Cyber Range," https://bcrcyber.com/, [Accessed 12-09-2024].

[6] MCR, "Michigan cyber range," https://www.merit.edu/, [Accessed 12-09-2024].

[7] VCR, "Virginia cyber range," https://www.virginiacyberrange.org/, [Accessed 12-09-2024].

[8] R. S. Weiss, S. Boesen, J. F. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen, "Teaching Cybersecurity Analysis Skills in the Cloud," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, 2015, pp. 332–337.

[9] L. Xu, D. Huang, and W.-T. Tsai, "Cloud-based Virtual Laboratory for Network Security Education," *IEEE Transactions on Education*, vol. 57, no. 3, pp. 145–150, 2013.

[10] Xu, Le and Huang, Dijiang and Tsai, Wei-Tek, "V-lab: a Cloud-based Virtual Laboratory Platform for Hands-on Networking Courses," in *Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education*, 2012, pp. 256–261.

[11] P. A. Peterson and P. L. Reiher, "Security Exercises for the Online Classroom with {DETER}," in *3rd Workshop on Cyber Security Experimentation and Test (CSET 10)*, 2010.

[12] J. T. F. on Computing Curricula, *Computer Science Curricula 2013*. ACM/Association for Computing Machinery, 2013.

[13] "CISE Research Infrastructure: Mid-Scale Infrastructure - NSFCloud (CRI: NSFCloud) — nsf.gov," https://www.nsf.gov/funding/opportunities/cri-nsfcloud-cise-research-infrastructure-mid-scale-infrastructure/504951/nsf13-602/solicitation, [Accessed 22-03-2025].

[14] "Chameleon – chameleoncloud.org," https://www.chameleoncloud.org, [Accessed 22-03-2025].

[15] "CloudLab – cloudlab.us," https://cloudlab.us, [Accessed 22-03-2025].

[16] J. Mambretti, J. Chen, and F. Yeh, "Next Generation Clouds, the Chameleon Cloud Testbed, and Software Defined Networking (SDN)," in *2015 international conference on cloud computing research and innovation (ICCCRI)*. IEEE, 2015, pp. 73–79.

[17] D. C. Erdil, "Using NSFCloud Testbeds for Research: Conference Tutorial," 2019.

[18] J. Mambretti, J. Chen, and F. Yeh, "Next Generation Virtual Network Architecture for Multi-tenant Distributed Clouds: Challenges and Emerging Techniques," in *Proceedings of the 4th Workshop on Distributed Cloud Computing*, 2016, pp. 1–6.

[19] R. R. Noel and P. Lama, "Taming Performance Hotspots in Cloud Storage with Dynamic Load Redistribution," in *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*. IEEE, 2017, pp. 42–49.

[20] R. R. Noel, R. Mehra, and P. Lama, "Towards Self-managing Cloud Storage with Reinforcement Learning," in *2019 IEEE International Conference on Cloud Engineering (IC2E)*. IEEE, 2019, pp. 34–44.

[21] M. Beck, T. Moore, N. H. French, E. Kissel, and M. Swany, "Data Logistics: Toolkit and Applications," in *Proceedings of the 5th EAI International Conference on Smart Objects and Technologies for Social Good*, 2019, pp. 61–66.

[22] A. Mandal and E. Deelman, "The Role of Machine Learning in Scientific Workflow Management on Distributed Cyberinfrastructure," 2020.

[23] S. Purohit, P. Calyam, S. Wang, R. Yempalla, and J. Varghese, "Defensechain: Consortium Blockchain for Cyber Threat Intelligence Sharing and Defense," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2020, pp. 112–119.