secCC: Securing the Future of Cloud Computing

Special track with Cloud Computing 2021

http://www.iaria.org/conferences2021/CLOUDCOMPUTING21.html

Aspen Olmsted
Fisher College
Department of Computer Science, Boston, MA 02116
email: aolmsted@fisher.edu

***Abstract*— As cloud computing continues its evolution into one of the primary forms of application deployment, many new cybersecurity challenges are rising to visibility. These challenges include deploying legacy applications to the cloud and developing new applications for the cloud. Each model has problems ensuring the confidentiality and integrity of the data and the service level available for the applications. This special track aims to expose some of these new problems and novel approaches to solving these problems. While we want to solve issues supporting our legacy architectures and algorithms moving to the cloud, we also want to give enough energy to new and evolving architectures and algorithms to secure future applications. Both challenges with private and public cloud infrastructure are welcome**

Keywords-Business Intelligence; Cloud Computing; Heterogeneous Data

I. INTRODUCTION

Cloud Computing has evolved into the modern operating system of the early 21st century. New York University (NYU) has developed an online graduate cybersecurity program called Cyber Fellows [1]. Cyber Fellows provides a 75% scholarship towards tuition for an elite online Cybersecurity Master's Degree. Thanks to generous support, this first of its kind program is offered for the affordable price of approximately $16,000 and includes access to hands-on virtual labs, industry collaborations, and industry-reviewed curriculum, exclusive speaker events, and peer mentors.

In the Cyber Fellows program, the students are challenged to marry their life experience with the competencies they learn in the classroom to solve applied problems. The challenge not only helps to develop the next generation of cybersecurity problem solvers, it also teaches the students to differentiate between scientifically proved solutions and industry hype.

The two classes utilize a system name "peergrade" [2] to submit eight peer reviewed scaffolded submissions that lead to their final paper and presentation. TABLE I shows the scaffolded submissions along with the week they are submitted in the course. The process works by allowing the students to learn in several phases for each submission. They learn from; listening to the professors, doing the work, reviewing their peers, and reacting to the reviews.

The participants of this special track are all participants in the NYU Cyber Fellows program. The papers are the dissemination of solutions that are solved were developed and solved in the classroom. Aspen Olmsted is the professor and mentor for over one thousand students through these two classes each year. Lenna Nashif is a maters candidates in the program. The professor and the students are also industry professionals. This life experience allows real work problems to be brought to the classroom for examination.

TABLE I. Research Scaffolding

Week	*Submission*
4	*Define Problem Domain and 3 Papers*
5	*Threat Model*
6	*Hypothesis and Differences from Current Solutions*
8	*Sampel Metric and Figure*
11	*Introduction Section*
12	*Related Work Section*
13	*Epirical Evidence Section*
15	*Presentation & Paper*

The organization of the paper is as follows. Section II describes the paper presented in the special session. We conclude in Section III and discuss the students' future work and how we will attempt to get more to disseminate their work at the conference.

II. SPECIAL TRACK PAPERS

There were over one thousand cybersecurity papers submitted in the past year by students in the Cyber Fellows program. Some students had terrific solutions but did not feel comfortable extending their work and submitting to the conference at this time. The first two submissions are from students in the program, and the third is from the professor.

Lenna Nashif [3] delves into the profound impact of social media on relaying information, which is often stored and hosted in the cloud. The ability to differentiate between correct information and information that can be termed “misinformation” or “fake news” is integral for social media platforms. The spread of misinformation can lead to severe and possibly negative effects. To understand this further, this paper uses Big Data Analytics, often applicable in cloud computing, cross-referenced with reliable newspaper sources, to understand a tweet’s validity in the context of the Covid-19 pandemic. Tweepy and TextBlob are Python libraries that are used to extract, derive sentiment analysis and subjectivity, and critically analyze the data for trends and implications in tweets. This analysis then is used to locate

where the misinformation is spreading from. Through rigorous testing and verification, it becomes possible to determine and indicate in a simple and effective way which tweets are reliable and which are not. Implementing cloud storage to build this out on a larger scale opens up the exciting possibility of applying this method of locating fake news on Twitter to other trending topics, including elections, scientific discussions, and sporting events.

Olmsted [4] explores how the US and world economies need more trained technical workers. These workers' demand has driven prominent private universities to create large, reduced-cost programs for graduate students. Unfortunately, less than twenty-five percent of the population has an undergraduate degree, and most do not have the pre-requisite knowledge to enter these graduate-level programs. In this paper, we look at developing an undergraduate technology program through cloud-based automatically graded labs and assessments that can guarantee the integrity and availability required to scale these programs to meet the demand for workers with these skills. We develop techniques to increase lab participation and integrity through a concept we call non-fungible labs. We also formulate testing assessments that allow each student to have a different version of the test. We provide preliminary evidence that these assessments have, in fact, increased engagement and integrity in our online sections of courses in our undergraduate Massive Open Online Courses computer science programs.

III. Conclusions and Future Work

Based on the student research's success, we demonstrate that applied Cloud cybersecurity problems can be solved by leveraging adult learners' life experience with competencies and research tools in the classroom. We plan to continue to push students to extend their work and submit to special tracks at the conference in future years.

References

[1] New York University, "NYU Cyber Fellows," [Online]. Available: https://engineering.nyu.edu/academics/programs/cybersecurity-ms-online/nyu-cyber-fellows. [Accessed 16 October 2020].

[2] peergrade ApS, [Online]. Available: https://www.peergrade.io/getting-started/. [Accessed 16 October 2020].

[3] L. Nashif, "Detecting and Identifying Fake News on Twitter," in *Proceedings of The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization*, Porto, Portugal, 2021.

[4] A. Olmsted, "Integrity through Non-Fungible Assessments in Cloud-Based Technology Courses," in *Proceedings of The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization*, Porto, Portugal, 2021.