An analysis framework of portable and measurable higher education for future cybersecurity workforce development

Feihong Liu [1], Manghui Tu [2]
[1]School of Information Technology, Ivy Tech Community College, USA
[2] Department of Computer Information Technology, Purdue University Northwest, USA

Article Info

Article history:

Received Feb 12, 2020
Revised May 10, 2020
Accepted Jul 24, 2020

Keywords:

Competency level
Curriculum alignment
Cybersecurity
Program evaluation
Workforce development

ABSTRACT

An educated workforce is essential to government and industry, hence the need to provide a high-quality workforce has been crucial in higher education academic program development. In the cybersecurity field, the situation is not quite satisfactory, the reason comes down to the fact that this new industry is lacking a portable and measurable framework to evaluate the efficacy of the academic programs, thus, to provide the industry with the unified high-quality workforce. In this paper, we aim to come up with a design of an analytical framework for portable and measurable academic programs for future workforce development. The ultimate purpose for our research is to develop cybersecurity workforce through the increase of the number of cybersecurity professionals with a 4-year degree, in this project we will develop a seamless pathway for students transferring from 2-year programs such as Ivy Tech Community College of Indiana(Ivy Tech) Cybersecurity AAS program to a 4-year program such as Purdue University Northwest(PNW) CIT program.

Corresponding Author:

Feihong Liu,
School of Information Technology
Ivy Tech Community College,
3485 Broadway, Gary, IN 46409, USA.
Email: fliu9@ivytech.edu

1. INTRODUCTION

The evolving of emerging technologies provides the world with great potential to fuel economic transformation and has achieved more than expected [1]. Cloud computing technology provides economic scale and achieved cost savings for small and medium-sized businesses and has been one of the most profitable departments for large-sized businesses such as Amazon and Microsoft. Big data technology provides business with more information in a shorter period to optimize business processes and produce new products or services to a better-targeted market [2, 3]. The technological advancement of the Internet of Things, cloud computing, and big data has driven the industry to the Industry 4.0 Era and already has a huge social and economic impact on human society. For example, the smart manufacturing driven by the industrial internet is projected to increase productivity and resource efficiency by 18% in the next few years and reduce cost by 2.6% annually [4]. While these emerging technologies brought the world the economic prosperity, they also raise severe cybersecurity challenges to public organizations and private businesses [5-11], and we have seen ever-increasing threats from cyberspace, including eavesdropping, retransmission, tampering, and denial of service attacks, and lead to network behavior denial, spoofing, unauthorized access, and virus transmission. Ginni Rometty, IBM’s Chairman, President, and CEO once said that” Cybercrime is the greatest threat to every company and individual in the world”. Thus, the advance of cyber technology should be the primary concern in this thrive.

According to Forbes, cybersecurity workforce development is the key to assuring that the nation has adequate capacity to protect information and information systems and yet, more than 30% of companies are short of security expertise in 2017. But it has been estimated by some research that there will be a 3.5 million shortage in the cybersecurity workforce [12]. The increasing demand for cybersecurity professionals from both government and private sectors makes it a critical mission for the education system to develop the next generation of cybersecurity workforce and citizenry that are capable of advancing national economic prosperity and security. But the fact is that we are short of the cybersecurity workforce, so preparing cybersecurity students to be career-ready is crucial in this case. Studies have shown that while 46% of undergraduates in the US are enrolled in community colleges, only 25% of them will transfer to a four-year institution within five years, but 70% of the cybersecurity jobs require a bachelor degree or higher, so how to better prepare for students to transfer from a 2-Y institution to a 4-Y became the key to this issue. In this paper, we are going to discuss how to develop higher education programs that can educate the high-quality future workforce in the field of cybersecurity.

2. VISION ON LONG TERM CYBERSECURITY HIGHER EDUCATION

Higher education served as the pipeline to a smooth transition to the workforce. There are some key points for the vision of long-term higher education.

2.1. K12 cybersecurity education

According to our research to investigate, 67 out of the 14832 school districts from 50 states defined cybersecurity courses to offer to K12 students. It aims to increase student interest in cybersecurity careers, which may, in turn, increase the pipeline of the future cybersecurity workforce. The National Center of Academic Excellence (CAE) program, a joint effort between National Security Agency (NSA) and the higher education community, has accredited less than 250 US higher education institutions as the NSA/DHS designated National Center of Academic Excellence in Cyber Defense and certified their cybersecurity programs including 2 year, 4-year, and graduate programs, with a rigorous curriculum that is well mapped to a set of core and optional Cybersecurity Knowledge Units. Private sectors have also actively involved in the cybersecurity education program development and numerous training and certification programs have been launched [13, 14]. However, these efforts still fall in short to address the huge national workforce shortage, and more quality academic programs need to be developed.

2.2. Pathway for community college

Research indicates that the key to developing more graduates in the cybersecurity field is establishing a meaningful pathway in the educational process. Studies have shown that while 46% of undergraduates in the US are enrolled in community colleges, only 25% of them will transfer to a four-year institution within five years; however, 62% of those transferred will complete a bachelor’s degree within six years [15]. These statistics indicate that one of the keys to developing more graduates with a bachelor’s degree is to assure more community college students make the transfer. Recent studies have shown that motivation and a well-developed pathway are keys to transferring from a community college to a four-year institution. The course curriculum of cybersecurity programs at different colleges may have varying specializations, and cybersecurity programs at community colleges are usually designed with certification as an endpoint. Hence, gaps exist between 2-year and 4-year cybersecurity programs. One-on-one course mapping between a 2-year program and a 4-year cybersecurity program is not always practical. Currently, program-level articulation agreements between 4-year and 2-year cybersecurity programs are either missing or have become outdated due to the dramatic changes in the course curriculum and plans of study within cybersecurity programs. Hence, there is a critical need to develop a seamless pathway that can motivate students and successfully transition them to a 4-year degree program.

Since the early 2000s, Corby Hovis, NSF program director, has led ATE efforts to grow cybersecurity education opportunities at community colleges. Since then, the growth of the cybersecurity program has been exploding in the United States. Bragg from the US Department of Education also states that coherent workforce development should be underway to cover both academic and training [16].

Community College Cyber Summit (3CS) as the only national academic conference, stating that the role of community colleges in preparing students for cybersecurity jobs is changing. We must focus anew on workforce development and the NICE Job Roles [17]. Community Colleges are now considered new gateways to hot cybersecurity jobs. For an effective, affordable, and flexible educational pathway into a cybersecurity job, students of all ages and backgrounds are increasingly enrolling in community college degrees and certificate cybersecurity programs across the country. Many of these programs got their start through the developmental support offered through five security technology centers and projects sponsored by the National Science Foundation's (NSF) Advanced Technology Education (ATE) initiative.

2.3. Higher education

According to a report by McAfee Burling Glass Technologies, "obtaining a Bachelor's degree is the minimum qualification for entry-level positions in cybersecurity, with nearly half of companies making it a minimum requirement" [18]. This is especially true in the US that 70% of US companies require a BS degree as a minimum requirement. With a large number of prestigious colleges and universities that offer computer science and IT degrees, "cybersecurity programs are still less common than traditional computer science degree programs", according to the study from Cybersecurity Ventures, the "limited degree of specialized cybersecurity education program in information technology and computer science around the world is a major factor in the shortage".

2.4. Cybersecurity workforce development

Based upon the giant deficiency of the cybersecurity talent pool and the severe cyberspace threats, cybersecurity workforce development became the key to assuring that one nation has adequate security measures to protect and defend information and information systems, and yet, more than 30% of companies are short of security expertise [19]. In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings unfilled, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. A new survey from **Cybersecurity Ventures** also projected that there will be 3.5 million unfilled cybersecurity jobs by 2021. Another survey of the hiring manager project, the Global Information Security Workforce Study 2017 pointed out that the increase of annual workforce demand in cybersecurity in North America is 21%. Among the various reasons why the cybersecurity labor shortage continues to increase, the issue of finding enough qualified workers topped the list, at 49%. More than half of respondents in North America cite a lack of qualified workers as the main reason for their shortage of staff.

3. RESEARCH METHOD

As pointed out by EC-Council [18], a leading cybersecurity training vendor, while certificate training provides learners the state-of-the-art knowledge and hands-on skill practices, training experiences may expire soon with the advancement of technology. On the other hand, "degree programs tend to teach students how to think and work through problems and that kind of knowledge doesn't expire". Cybersecurity is an evolving field with the rapid-changing set of knowledge and skills, cybersecurity professionals must stay with the latest knowledge and skills. Thus, it would be ideal for the 4-year and graduate cybersecurity programs to provide learners with a good mix of certification training experience and problem-solving ability learning process, to help college graduates to have a strong start at work. Challenges exposed to the cybersecurity education community are to determine what future workforce a (bachelor or master) degree program can educate, evaluate how much gain on knowledge, skills, and abilities a degree program can achieve, and how to effectively and efficiently educate learners with diverse backgrounds. Essentially, the following three questions should be answered to develop a cybersecurity education program.

a. (What workforce developed in terms of KSA?) What cybersecurity knowledge, skills, and abilities (KSAs), as well as work roles, can be developed for learners that complete the target education program.
b. (How many differences in KSA attained?) Comparing to a certificate training program, an associate degree program, another peer bachelor degree program, what knowledge, skills, and abilities (KSAs) will be attained for learners to complete the target education program.

To address the above questions, there is a critical need to develop a suite of mechanisms as a comprehensive framework to evaluate an educational program by correlating course curriculum with workforce requirements, assess the program differences based on the knowledge, skills, and ability gains, and develop pedagogy to provide the right content for diverse learners.

3.1. Quantitative solution I (content competency)

With a basic knowledge of the course material, the team found that it is not enough just by identify the knowledge gap by locating the knowledge in the documents and course requirements, it is also very important to identify the competency level. Only in this way can we find the actual knowledge gap. In this case, we wouldn’t make mistakes like they cover the same topic and then identify them as the same, but one is the entry-level class, and another is an advanced class.

To address the proficiency issue of knowledge units/topics, a competency proficiency level concept will be introduced, as shown in Table 1, to give another dimension of evaluation criterion to KUs and especially major topics.

Table 1. Competency level list

Score	Competence Proficiency Levels	Example
1	Fundamental Awareness (basic knowledge)	Introduce concepts of penetration testing, tools, method.
2	Novice (limited experience)	Individual ethical hacking labs (scan, break-in, etc)
3	Intermediate (practical application)	Applying the penetration testing process to a virtual environment
4	Advanced (applied theory)	Developing exploitations for unknown/known vulnerabilities

To have an unbiased comparison of two programs required more than just qualitative knowledge cover difference, we also need to quantitate analyze the learning outcome. We will achieve this goal by proposing a correlation solution of a combination of several approaches.

First, we analyze the content that may correlate the competency levels of KU topics to KSAs. Here we are going to demonstrate this with two examples, one positive and one negative to show that with only coverage, we cannot differentiate two programs with apparently different levels.

As you can see from the table above, a class might have covered a topic, but only as an introduction, and there is no lab or in-class activity associated with the topic, in the learning time has been set to 1 hour and the competency level as well. Now, let’s see the novice example, the same topic could be an important topic that has been discussed throughout the whole class, but still lacking enough lab and project activity, so the learning hour is 3 and the competency level is also 1. Same situation with the intro course.

Now, let’s examine the intermediate level class. In these classes, the topic is lectured and practiced both in class and on labs, but there is only one or two lab associate with the topic, so we set the learning time to 6 and the competency level to 2.

Lastly, the advanced level class does not only covered lectures on the topic, but it also has labs and a final project implementing it, so the competency level here has been set to 4.

This competency level comparison serves as an example of even if two classes covered the same topic, similar content, we still need a quantitative approach to examine exactly how much time students spend on such topics, to come to an unbiased conclusion on the comparison of two academic programs.

After the examination on competency level, we also need to work on the relationship between KSAs and Work Roles. Below is the table on NCWF Work Roles, the table header is as follows: describes each of the Work Roles described by the NCWF. Each Work Role is identified by the Category and Specialty Area, followed by a sequential number (e.g., SP-RM-001 is the first Work Role in the SP Category, RM Specialty Area). Some of the Work Role Descriptions originate with external documents (e.g., Committee on National Security Systems Instruction [CNSSI] 4009) and include that information in the description column.

3.2. Quantitative solution II (learning effort)

We propose to use the term Learning Effort by several hours as our second Quantitative Solution, which is assessed and combined by Instructional/discussion time, Lab/practices time, Self-reading/research time, and Project time.

For learning effort, we calculate the learning effort by assessing how many hours’ student spend on one topic, we get the information on how many chapters cover that topic and how many labs cover that topic.

For a class that meets once a week for lecture and once for the lab, if this topic contains a lab, we normally count this as 3 hours of leaning effort, for those topics that have been developed as a project, we counted it as 9 hours. For the topic that has not been extended as a lab or project, depend on if that specific topic is a major topic in that chapter, the learning time can range from 0.5 to 2 hours. We will use this criterion to categorize all topics in all the classes.

4. SUMMARY ANALYSIS OF EXISTING PROGRAM CRITERIA

4.1. Center of academic excellence knowledge units

According to NICE, “A Knowledge Unit (KU) is a coherent defined block of knowledge related to cybersecurity” [20]. In the learning process of KU, the author found that KUs has changed several times in the time frame. There are four types of KU in the 2020 version, Foundational KUs, Technical Core KUs, Non-Technical Core KUs, and Optional KUs. The structure of a KU should include a title, description, outcomes, topics, and vocabulary. There are three Foundational KUs, five Technical Core KUs, five Non-Technical Core KUs, and 51 Optional KUs according to the latest update for 2020.

KUs contains several topics in them, each represents a unique topic in its area. Those KUs serves as a curricular guideline for course materials. Mapping each course to the KUs can give the reader an understanding of the academic program performance if each course contains essential knowledge topics regarding cybersecurity standards. Especially for information assurance and network security related courses, programs can adjust its course based on the KUs. In that way, the course will have a comprehensive cybersecurity-related knowledge topic, also the program can keep up with the current cybersecurity trend by following the KUs.

4.2. Criteria based method

In this section, we will study the mainstream criteria solution to see how they can represent the different approaches to evaluating the academic programs. For criteria solution, they focused more on the quality aspect of a program, which has been serving the academic society very well, but with the fact of the criteria solution lacking the quantitative aspect, sometimes it cannot fully represent the difference and the level of difference between programs.

4.2.1. Accreditation Board for Engineering and Technology (ABET) criteria

According to the official ABET website, ABET is s a non-governmental organization that accredits post-secondary education programs in applied and natural science, computing, engineering, and engineering technology [21]. There is an increasing demand for continuing education, lifelong learning as it is often called, especially among technical workers. This demand is bolstered by both employers and employees themselves, each understanding the need to stay as up-to-date as possible in these rapidly changing technological times. ABET is leading the curriculum development by promoting the idea and for providing quality assurance in technical higher education, it is not unreasonable to think that it may, too, have a hand in quality assurance of lifelong learning in the not-so-distant future. Scholars have appealed for ABET to come up a specific cybersecurity standard for years, Greenlaw et al talked about this issue in the paper “Is it time for ABET cybersecurity criteria?”, they state that cybersecurity is becoming increasingly important in society at large and ABET should establish cybersecurity as a formal academic discipline [22].

Having a unified guideline across the country not only benefits the academic institutions to educate their students with shared expectations of core knowledge, abilities, and skills but also helps the employees to hire graduates. Although other curricular guidelines already described different aspects of cybersecurity education, they do not define what constitutes an undergraduate cybersecurity program. So, a clearer and more comprehensive curricular guideline has to come in order. According to John Schnase, senior computer scientist at NASA Goddard Space Flight Center and CAC Chair, “By creating these program-specific criteria, CAC and ABET are helping to establish cybersecurity as an academic discipline, and helping to address the critical skills gap we’re seeing in this area”. If the program has already been accredited by the CAC standard, it will be reviewed under the new program criteria for cybersecurity and similarly named computing programs.

The advantages of the ABET curriculum is clear, with a unified guideline across the country, the academic institutions can educate their students with shared expectations key learning skills and the employees can hire graduates knowing they were educated with the same standard. Meanwhile, the disadvantage is also obvious, ABET standard lacks measurable and quantifiable part to distinguish the difference and gap between academic programs, CAE KU is a better content guide in technical areas comparing to ABET.

4.2.2. IEEE/ACM curriculum guide

IEEE is the acronym for Institute of Electrical and Electronics Engineers which defines the standards for Electronics & communication, while Association for Computing Machinery (ACM) is entirely made for Computer Science Majors, Electrical Engineering and Computer Science (EECS) majors for providing them the resources they need such as books, journals, conferences to improve themselves. Curriculum guidelines for baccalaureate degree programs in information technology served as a guideline for academic programs following the IEEE standard.

Practices are a critical consideration in cybersecurity education. The CSEC thought model links the academic curriculum to professional practice through the use of application areas. The application areas provide an organizing structure to combine curricular content, professional development and training opportunities, and professional certifications.

Application areas serve as an organizing framework to identify competency levels for each practice. The application areas help to define the depth of coverage needed for each core idea. Also, application areas provide a bridge between the thought model and a specific workforce framework.

Practices are a critical consideration in cybersecurity education. The CSEC thought model links the academic curriculum to professional practice through the use of application areas. The application areas provide an organizing structure to combine curricular content, professional development and training opportunities, and professional certifications.

Application areas serve as an organizing framework to identify competency levels for each practice. The application areas help to define the depth of coverage needed for each core idea. Also, application areas provide a bridge between the thought model and a specific workforce framework.

By comparing the ABET, IEEE, and the details of examining KU, it is clear the ABET and IEEE are lacking the quantitative solution to quantify the difference between two programs. Also, KU cannot work alone to determine the coverage and gap between programs, we have to take into consideration that the competency level is the quantitative solution that needed to use in conjunction with the qualitative solution to unbiasedly represent and compare two programs.

4.2.3. Certificate LO

Associate, bachelor’s, master’s, and doctoral degree programs are the most commonly earned marks of completion in higher education. Another common, but lesser-known, the mark of completion are certificates earned from certificate programs.

Certificate programs are like associate programs because they both take a short amount of time to complete, although associate degrees are generally better-rounded in terms of topics and courses. Certificate programs are generally completed during your education before earning your actual degree and are generally suited to the field of study you’ve chosen, whether it’s business, technology, science, or anything else.

The benefit of certificate programs can include it stands out on a resume, it can facilitate a last-minute career change, it takes a short amount of time to complete, etc. But the problems are also evidential: it lacks diversity in the knowledge area, and for these certificates must be completed before a student can earn a degree in their area of study, it can be hard for some students that struggle to pass the certificate.

2018 has been an eventful year of a cyber breach. Starting with the 2018 reform of EU data protection rules [23], following with Facebook leaking millions of data, cybersecurity has yet again become a center of attention. Those security breaches equate not only with bigger losses and more media coverage but also with more jobs and opportunities for IT and programming professionals.

Scholars also expressed their onions on this issue, whether to use professional certifications as facilitation in designing higher education curricula. Knapp and Plachkinova think that just as cybersecurity professionals must hone they also need to evolve to ensure they continue to produce knowledgeable graduates [24]. So, they shared their valued experience that to maintain a cybersecurity curriculum, the program must consider professional certifications as valuable guidance. Other scholars also promoted universities to hire cybersecurity faculty and cybersecurity professionals to teach security and encouraging professional development, thus for those that are currently offering, or planning on offering, degree programs in cybersecurity, or cybersecurity-related degrees could benefit from this pedagogical perspective [25].

4.3. Summary analysis of all criteria

Here we are providing this an analysis summary table for the program criteria (CAE KU, CAE KU with quantitative metrics, ABET, IEEE/ACM Guideline, Certificate LO), shown in Table 2.

Table 2. Analysis summary table for all program criteria

	CAE KU	ABET	IEEE/ACM Guideline	Certificate LO
Advantage	extensive topics with the specification of cybersecurity	work as a unified guideline across the country, have general criteria and program criteria	Education competency level and scope are used	Stands out on a resume, facilitate a career change, takes a shorter time to complete
Problem	not a deep dive into specifics lack quantitative measurement	The curriculum requirements specify topics but do not prescribe specific courses	lack quantitative measurement	lacks diversity in the knowledge area, too concentrate on the specific area

As we can see from the table above, CAE KU with quantitative metrics not only has the coverage of topics but also provided a quantitative measurement to the program analysis.

5. SYSTEM IMPLEMENTATIONS

As an implementation tool for the pathway from 2-Y to 4-Y cybersecurity program, we developed a database system to automate the process of course mapping. This system is developed on the Windows system; it is also available on Linux or Mac OS environment. To make this deigned system function well, it requires users to pre-installed Java JDK, at least 1.8 version, application server Tomcat, version 8.0 and above, MySQL on the device that runs it.

After the user logged into the system, all the architecture and description of the function tab will be shown in the following Table 3.

Table 3. System function architecture

Main Module	Two Level module	Three Level module	Functions
System Administration	User Management	User Profiles	Search, add, delete, update data
		Password Update	Update password
	Data Management	User-Defined	Allow user to self-define import data and shown on the website
		Course	Search, add, delete, update data Show all the courses on the selected institution
		Question and Answer	Students can post their questions and make it public. Anyone can publish answer of the uploaded questions
		Data Download	Users can upload, download and delete attachments
Program Analysis	Analysis Criteria	KSAS	Search, add, delete, update all data about KSAs.
		Work Role	Search, add, delete, update all data about Work Role
		Knowledge Units	Search, add, delete, update all data about Knowledge Units
		Competency Level	Search, add, delete, update all data about Competency Level.
	Analysis Tool	Course Mapping	Any of two or more courses can be chosen to show their specific difference
		KU Mapping	Any of the different Knowledge Units under the dropdown list can be chosen to have a comparison.
		Summary	Polymerization display non-duplicate topics with the highest proficiency level or One by one polymerization displays non-duplicate topics with the highest proficiency level

Model layer: The data model, which defines how data is connected and how data is processed and stored within the system. It provides the data which to be displayed, mainly supports different kinds of data processing, which is the foundation of the Database Management System (DBMS).

View layer: It takes responsibility for the user's interface.

Controller layer: It takes charge of receiving the user's request, delegating to the model for processing, then returning the processed good data to the view [26]. As has been described above, the view layer will show this data.

6. CONCLUSION

The revolution is needed in classroom pedagogy, taking us beyond the traditional model of one teacher at the front of the classroom with twenty more or less similar students listening. We need to develop pedagogical approaches that move beyond on-the-same-page, standardized content paradigms, replacing them with approaches that continuously diagnose differentiated learning needs and promote the design of customized learning programs. We need to move away from traditional one-size-fits-all instruction, developing and testing strategies for customization of learning to meet individual learner needs more effectively.

A broader aspect of curriculum customization will entail research and development of new programs to meet the needs of special groups. Teachers need to be supported as designers of learning that suit learner needs, instead of just following standardized tests. The Productive Diversity Curriculum needs to be developed through collaborations with learners, their communities, and education experts. It would also require ongoing professional learning opportunities and investment in leadership training to support pedagogical improvements and effective use of resources.

By doing the mapping process in this project, it should be clear that the seamless 2Y-4Y cybersecurity program pathway development for community college students will achieve the following objectives; (1) ensure transfer students are sufficiently prepared to be successful in pursuing their higher education in the CAE 4Y program and will be able to graduate on time, (2) ensure all CAE knowledge units and their associated major topics are covered for transfer students when they graduate from the CAE 4Y cybersecurity program, (3) Determine knowledge/skill/ability gains that could motivate students' transfer to a CAE 4Y program. The pathway development will be achieved through the following approach. A systematic study of the course curriculum for the 2Y and 4Y cybersecurity programs CAE 2Y-4Y program articulation development and knowledge gap identification. Knowledge gap remediation through curricular and extra-curricular activity collaboration. The way to achieve the seamless 2Y-4Y cybersecurity program pathway development for community college students is by incorporating competency levels into the curricular design, along with the KU and the certificate LO. This is the analytical framework we proposed for portable and measurable academic programs for future workforce development: as competency level as a major part of the quantitative measure, KU as the center for the qualitative solution, working together with certificate LO as the evaluation and preparation for the future workforce.

REFERENCE

[1] B. Swanson, "The economic impact of mobile and cloud computing is greater than previously thought," 2018. [Online] Available: https://www.aei.org/economics/the-economic-impact-of-mobile-and-cloud-computing-is-greater-than-previously-thought/

[2] M. Armbrust *et al.*, "A view of cloud computing," *Communications of The ACM*, vol. 53, no. 4, pp. 50-58, 2010.

[3] Joseph Kennedy, "Big Data's Economic Impact," Committee for Economic Development of The Conference Board, 2020. [Online] Available: https://www.ced.org/blog/entry/big-datas-economic-impact.

[4] N Granato, *Smart manufacturing: technologies and global markets*. BCC Publishing, IFT126A, 2018.

[5] F. Alaba, M. Othman, I. Hashem and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017. Available: 10.1016/j.jnca.2017.04.002.

[6] S. Biggs and S. Vidalis, "Cloud Computing Storms," *International Journal of Intelligent Computing Research*, vol. 1, no. 2, pp. 47-54, 2010.

[7] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, 2017.

[8] M. Pogliani, D. Quarta, M. Polino, M. Vittone, F. Maggi, and S. Zanero, "Security of controlled manufacturing systems in the connected factory: the case of industrial robots," *Journal of Computer Virology and Hacking Techniques*, vol. 15, no. 3, pp. 161-175, 2019.

[9] L. Mailloux, M. McEvilley, S. Khou, and J. Pecarina, "Putting the "Systems" in Security Engineering: An Examination of NIST Special Publication 800-160," *IEEE Security & Privacy*, vol. 14, no. 4, pp. 76-80, 2016.

[10] Deinde Prima Illa, IN: Quid TU, InquiT, HUC, "Smarter Security for Manufacturing in The Industry 4.0 Era," 2020. [Online] Available: https://docs.broadcom.com/doc/industry-4.0-en.

[11] P. Bruening and B. Treacy, Cloud computing: privacy, security challenges. Bureau of National Affairs, Inc. 2009.

[12] Brian NeSmith, "Council Post: The Cybersecurity Talent Gap Is An Industry Crisis," 2019. [Online] Available: https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#23855d95a6b3

[13] David Bisson, "10 Respected Providers of IT Security Training - Security Boulevard," 2020. [Online] Available: https://securityboulevard.com/2019/09/10-respected-providers-of-it-security-training/

[14] Cybercrime Magazine, "List of Cybersecurity Education and Training Providers," 2020. [Online] Available: https://cybersecurityventures.com/cybersecurity-education/.

[15] M. Jennifer and B. Sandy, "Trends in community colleges: Enrollment, prices, student debt, and completion," *College Board Research Brief*, vol. 4, pp. 1-23, 2016.

[16] D. Bragg, "Opportunities and challenges for the new vocationalism in American community colleges," New Directions for Community Colleges, vol. 2001, no. 115, pp. 5-15, 2001.

[17] Bossier Parish Community College "2019 Community College Cyber Summit," 2019.[Online] Available: https://7bc5496d-882f-4630-911d
2824effb3b6a.filesusr.com/ugd/0ecb0b_0d335842ebd641469790e02a182dae26.pdf

[18] EC-Council University, "A Degree in Cybersecurity or a Certification Course: Which is Better for Your Future?", 2020. [Online] Available: https://blog.eccu.edu/a-degree-in-cybersecurity-or-a-certification-course-which-is-better-for-your-future/.

[19] A. Fitzpatrick, *Cybersecurity experts needed to meet growing demand*, Washington Post, 2012.

[20] CyberEdWiki, "NICE Framework," 2020. [Online] Available: https://cyberedwiki.org/index.php?title=NICE%20Framework.

[21] ABET, "ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs," 2020. [Online] Available: https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/.

[22] R. Greenlaw, A. Phillips, and A. Parrish, "Is it time for ABET cybersecurity criteria?," *ACM Inroads*, vol. 5, no. 3, pp. 44-48, 2014.

[23] European Commission, "EU data protection rules," 2020. [Online] Available: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en.

[24] K. Knapp, C. Maurer, & M. Plachkinova, "Maintaining a cybersecurity curriculum: professional certifications as valuable guidance," *Journal of Information Systems Education*, vol. 28, no. 2, pp. 101-114, 2017.

[25] J. James, C. Morsey, and J. Phillips, "Cybersecurity education: a holistic approach to teaching security," *Issues in Information Systems*, vol 17, no. 2, pp. 150-161, 2016.

[26] H. Zeynal, M. Eidiani, and D. Yazdanpanah, "Intelligent substation automation systems for robust operation of smart grids," *In Innovative Smart Grid Technologies-Asia (ISGT Asia)*, pp. 786-790, 2014.

BIOGRAPHIES OF AUTHORS

Feihong Liu is a software development faculty in the School of IT, Ivy Tech Lake County campus. She is the faculty advisor for Software Development and Computer Science in Lake County campus and also helps started Women in IT student club. She has an M.S. in Computer Information Technology and an M.S. in Regional Economics. Feihong Liu had solid experiences in program articulation development and IT program curriculum development.

Dr. Manghui Tu is a professor of Computer Information Technology, Director of the Center for Cyber Security, and the Point of Contact of the NSA/DHS Designated National Centers of Academic Excellence in Cyber Defense Education at Purdue University Northwest. Dr. Tu's areas of expertise are information assurance, digital forensics, cybersecurity education, and distributed computing. His research has been supported by the National Science Foundation and National Security Agency and published more than 45 peer-reviewed papers in journals and peer-reviewed conference proceedings. Dr. Tu has over 15 years of college teaching and research experience in cybersecurity and digital forensics.