CyberMaster: An Expert System to Guide the Development of Cybersecurity Curricula

https://doi.org/10.3991/ijoe.v15i03.9890

Rania Hodhod(✉), Shamim Khan, Shuangbao Wang,
Columbus State University, Columbus, Georgia
hodhod_rania@columbusstate.edu

Abstract—The growing number of reported cyber-attacks pose a difficult challenge to individuals, governments and organizations. Adequate protection of information systems urgently requires a cybersecurity-educated workforce trained using a curriculum that covers the essential skills required for different cybersecurity work roles. The goal of the CyberMaster expert system is to assist inexperienced instructors with cybersecurity course design. It is an intelligent system that uses visual feedback to guide the user through the design process. Initial test executions show the promise of such a system in addressing the enormous shortage of cybersecurity experts currently available for designing courses and training programs.

Keywords—Cybersecurity, expert systems, NICE Framework

1 Introduction

Cybersecurity has become one of the most important challenges around the world. According to a compilation published by the USA-based Identity Theft Resource Center (ITRC), the unauthorized access to confidential information and data breach that affected US organizations and customers have reached 1579 notifications with almost 179 million records exposed. This amounts to an alarming increase especially when considering ITRC reported 1,039 breaches in 2016 and just over 36.6 million records exposed. Among the types of breaches are those resulting from hacking, unauthorized access, data on the move, insider theft, accidental exposure, human error/negligence and physical theft [1]. Recent research revealed that nearly 70% of critical infrastructure companies have reported at least one security breach during 2015 that led to the disruption of operations or the loss of confidential information. Hacking remains the leading type of cyber-attack with techniques used ranging from low-tech exploits, such as phishing and social engineering, to more advanced techniques such as malware/ransomware, backdoors, exploitations, or zero-day attacks [2, 3].

Cybersecurity National Action Plan (CNAP) is a comprehensive plan that was developed in the USA but can be applied worldwide to address the cybersecurity threat by taking action to expand the cybersecurity workforce, to enhance cybersecurity education and training, and to improve cybersecurity curriculum. However, several difficulties exist that hinder the spread of cybersecurity education and training including:

lack of cybersecurity skills, lack of resources in rural areas and the shortage of high quality cybersecurity courses.

- **Poor cybersecurity skills**: Despite the existence of cybersecurity training and personnel development programs, they are not enough as they are limited in focus and lack unity of effort [2]. There are not enough cybersecurity experts within the US federal Government or private sector. Although the above statement is specific to the situation existing currently in the USA, it is likely to be applicable to many other countries. In order to maintain technical advantage over perpetrators of cybercrime to secure information systems and communication networks, it is essential to develop skilled, cyber-savvy workforce and an effective pipeline of future employees [4]. This requires that cybersecurity education reaches all students in the country, especially, high school and college students.
- **Rural districts:** Major obstacles exist to expanding the efforts to deliver high-caliber education in rural areas [5]. Rural districts in the USA make up more than half (57 percent) of all public districts in the country, while educating approximately one-quarter (11 million) of all students nationwide, which make scaling and innovating across the country a big challenge [6]. Rural schools often face geographical isolation, shortages in specialized staff, poor physical working conditions and resources [7] making access to educational programs inadequate [5]. Better technology and telecommunication can lower those barriers [5] and maximize the natural advantages of rural schools and alleviate the disadvantages [8].
- **Course quality assurance:** Well-designed courses are those designed in a way that ensures good course design and appropriate content while fulfilling student study requirements [9]. Evaluations of the developed courses can be difficult to quantify and may involve more than just surveys to collect meaningful data [9]. In addition, courses undergo constant revisions [10, 11]. Usually, participant evaluations and/or assessment tools are often used to solicit feedback and collect data to evaluate the quality of design and course material [12]. A number of resources are required to apply these evaluation instruments including human resources and time, which are two restricting factors especially when it comes to rural districts. Automated evaluation of the quality of a course design can be the way to address this challenge.

In an effort to inspire solutions and innovations in cybersecurity curriculum development, the US National Institute of Standards and Technology (NIST) published the National Initiative for Cybersecurity Education (NICE). It is a partnership between government, academia and the private sector focused on cybersecurity education, training, and workforce development [13]. The NICE framework consists of seven categories, 31 specialty areas, 369 Knowledge, Skills and Abilities (KSAs), and 65 competencies. In addition, it has 444 tasks under the various specialty areas.

This paper presents an interactive course design system for the rapid development of cybersecurity curriculum and training by novice instructors. It utilizes a highly visual interface and artificial intelligence techniques like rule-based inferencing to guide the design process. The system is based on a cloud-computing platform, which offers ad-

vantages such as simplified software installation and maintenance, in addition to centralized control over versioning. Moreover, end-users can access the service anytime, anywhere, share data and collaborate more easily.

The paper starts with a brief discussion of related work, especially the application of expert systems. Section 3 explains how knowledge gathering takes place in the expert system presented in this paper and how knowledge is represented using concepts maps. Section 4 describes the role of user model in providing tailored feedback for user guidance. Section 5 discusses how evaluation of designed courses takes place. The paper ends with concluding remarks in Section 6.

2 Related Work

The education of the cybersecurity workforce must include considerations of the security and privacy of urban and rural areas, curriculum development and rapid development of training programs. At the same time, teachers, students, engineers, military personnel and government employees must be trained in cybersecurity in light of the latest developments in computer networks and data communication. For example, incorporating the Internet of Things (IoT) architecture and security into the current curricula will empower students to gain the knowledge of how IoT can be used in a smart cities setting, while also allowing them to master the skills necessary to design secure IoT systems [14]. With the cybersecurity area evolving fast and the level of relevant expertise lagging behind, systems based on artificial intelligence techniques can play an important role to help improve the situation.

Intelligent systems, a.k.a. smart systems, is everywhere around us, starting from smart thermostats to smart cars. Adding intelligent features/capabilities to any system can reduce the workload on the human user and complement the user's efforts to achieve the desired tasks. Expert decision making systems are a widely used intelligent technique to support decision making in a specific domain. They have been used successfully in the medical domain to diagnose heart diseases [15, 16, 17], anemia [18], and diabetes [19]. Expert systems have been used in engineering for fault diagnosis [20, 21], and also in other domains including career guidance [22]. Expert systems are usually used to address the lack of human and/or time resources. One example is an expert system for career guidance used in African high schools to address the shortage of human and time resources that the process of quality career guidance demands [22]. Other expert systems were developed for providing academic advice to students to address the shortage of capable human advisors [23], assist novice users in using new software [24], and help make decisions on appropriate public transport alternatives to the car in certain cities [25].

Although there are expert systems developed to help with designing courses in different areas, none of these systems targeted cybersecurity. As yet, there is no intelligent system that can make use of cybersecurity experts' knowledge and the NICE Framework to guide novice instructors and trainers with the development of cybersecurity courses and study programs.

3 CyberMaster: An expert system to assist with Cybersecurity Course Development

An expert system is a computer system that emulates the decision-making ability of a human expert. Expert systems can assist people in the decision making in several domains as mentioned earlier. CyberMaster is an expert system developed to guide the development process of cyber security courses using the power of knowledge stored in its knowledge base. The different components of CyberMaster are the knowledge base, user model, inference engine and user interface. The following subsections present the details of each component.

3.1 Knowledge base

Expert systems use mainly if-then rules to reason about and solve complex problems [26]. The bottleneck in developing any expert system is knowledge gathering [27]. CyberMaster used information extracted the NICE Framework (see Fig. 1) to build the knowledge base.

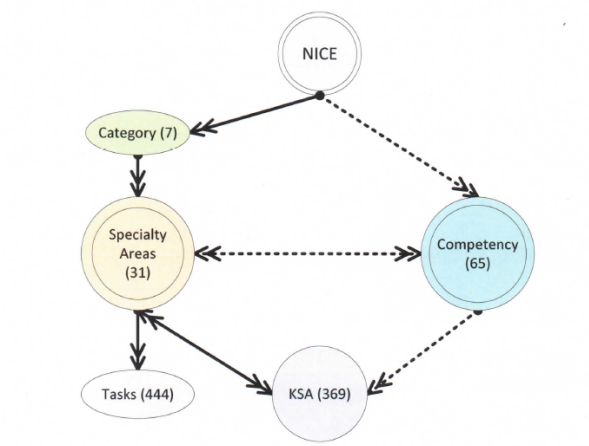

Fig. 1. An overview of the NICE Framework

The first step to building the knowledge base was to identify knowledge units and map them to corresponding work roles and KSAs, and then represent them in a way that is accessible by the expert system. The main issue for most cybersecurity educators attempting to use the NICE framework to design their courses is that all the framework data are spread over a master Excel spreadsheet file, which is hard to navigate and use. Our study shows that there are three types of mappings in the framework: one-to-one, one-to-many, and many-to-many. Excel may be fine for one-to-one and one-to-many relationships; however, for many-to-many relationships, Excel produces a large number

of duplicates. Accordingly, for many-to-many mappings, we used two-dimensional visual mapping techniques that map specialty areas to competencies and KSAs (see Fig. 2). This was followed by the creation of a visual mapping of the curriculum.

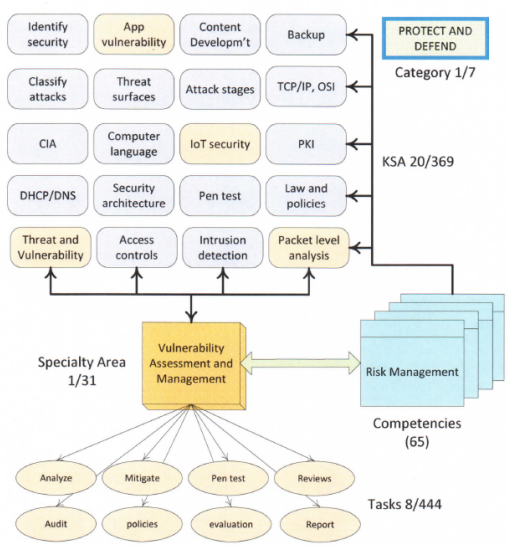

Fig. 2. Mapping of Specialty areas to KSAs

Curriculum visual mapping: The curriculum visual mapping connects knowledge units to skills and abilities based on the cross-reference of NICE framework and CAE framework. The NICE framework lists knowledge, skills, and abilities needed to successfully complete cybersecurity tasks for students or cyber professionals. Fig. 3 shows the representation of the NICE Framework as database schema.

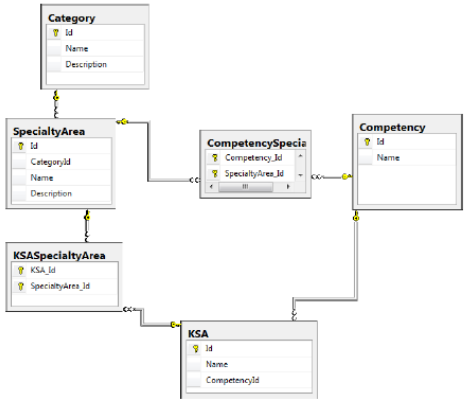

Fig. 3. NICE Database Schema

In this work, competencies in NICE framework are considered as assessments. Mapping specialty areas to competencies allows checking that the content discussed in a course is assessed appropriately. This many-to-many mapping is linked with KSAs keeping the completeness in course content. Fig. 4 is the visual representation of the mapping of specialty areas with corresponding competencies.

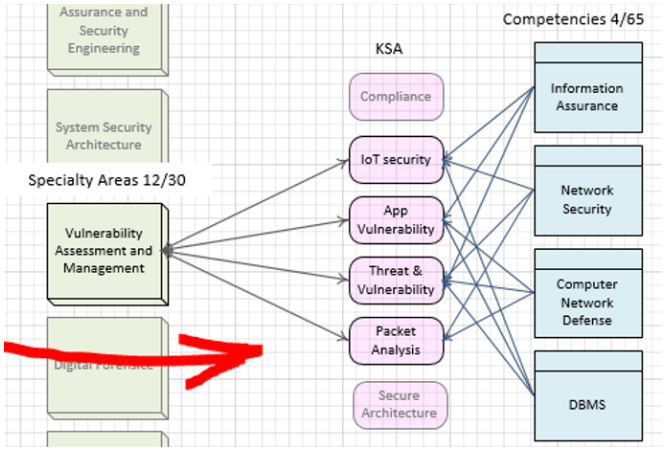

Fig. 4. Mapping of a Specialty Areas to Competencies

Concept maps for knowledge representation and extraction: Concept maps provide a way to represent organized knowledge (concepts) based on a person's understanding of a domain of knowledge [28]. They are graphs consisting of nodes (vertices) representing concepts and edges connecting these vertices. These edges may be labelled with the type of relationship between the pair of connected nodes. Concept maps were used in many disciplines as a formal or semi-formal diagramming technique [29]. Concept mapping systems used in education and knowledge management emphasize flexibility of representation to enhance learning and facilitate knowledge capture [30], in addition to being a way to represent terminology variance, informality, and organizational variation. These factors make it difficult to match elements between maps in comparison, retrieval, and merging processes [30]. Matching algorithms for the knowledge elements in educational concept maps were introduced in [30-32]. Concept maps and expert systems are soft tools used for knowledge modelling [33] where establishing a concept map was considered as the first step in curriculum development [34].

Concepts maps were used to model the NICE framework and an analysis algorithm was used to extract knowledge stored in them for use by the expert system. The relationship between concept map nodes represented the relevance or closeness of association between two components in the course being designed. This was expressed implicitly without using any labels in the visual display of the concept map; instead, the thickness of the edge was used to show the strength of a relationship. A concept map showing relationships between the different components in a course is shown in Fig. 5.

Fig. 5. A concept map showing strong association between two specialty areas RSK and ARC

Knowledge acquired from concepts maps and represented in the form of rules. Example facts extracted from the concept map shown in Fig. 5 are:

```
connect_cat_sa_sa_wt("SP", "RSK", "ARC", 0.67)
path_cat_sa_wr_ksa("SP", "ARC", "001", "K0212")
path_cat_sa_wr_ksa("SP", "RSK", "001","K059")
```

The above facts represent the connections between the different concepts (nodes) as follows: The first of the above facts is defined by the relation `'connect_cat_sa_sa_wt'`, where, the first parameter indicates the category name, the second and third parameters indicate the specialty areas of interest and the fourth parameter is the strength of the connection (1 indicates maximum possible connection strength). This information is used later by the graphical user interface for visualization purpose. `'path_cat_sa_sa_wt'` is another fact that provides a full path between a category and a skill or ability. The fact takes category name as the first parameter, specialty area, work role and KSA in the second, third and fourth parameters respectively.

3.2 User modeling

User modeling is a subarea of human computer interaction that focuses on the process of building up and modifying a conceptual understanding of the user [35] to provide customization and adaptation to the user's specific needs. The user model in CyberMaster aims to track the user's interaction with the system and to build a model for user performance. For example, if the user chooses specialty area A and specialty area B to be included in their course, the user model adds this information to the user model with an indication of the strength of the connection/association between those specialty areas. The user model then provides this information to the inference engine to reason about the user's performance and provide tailored feedback to the user.

3.3 Inference engine

The inference engine applies logical rules to the knowledge base. For example, If the connection between specialty area 1 and specialty area 2 is a weak connection and

the connection between specialty area 2 and specialty area 3 is a weak connection then it is deduced that the connection between specialty area 1 and specialty area 3 is a weak connection. It does also make use of the rules in the knowledge base and the user model to provide tailored feedback to the course designer.

3.4 User interface

The user interface allows the user to interact with CyberMaster. Using the interface, the user is able to explore and interact with the visual maps for the developed courses, see Fig. 6. The user interface also provides an editor, which the user can use to create or modify a course.

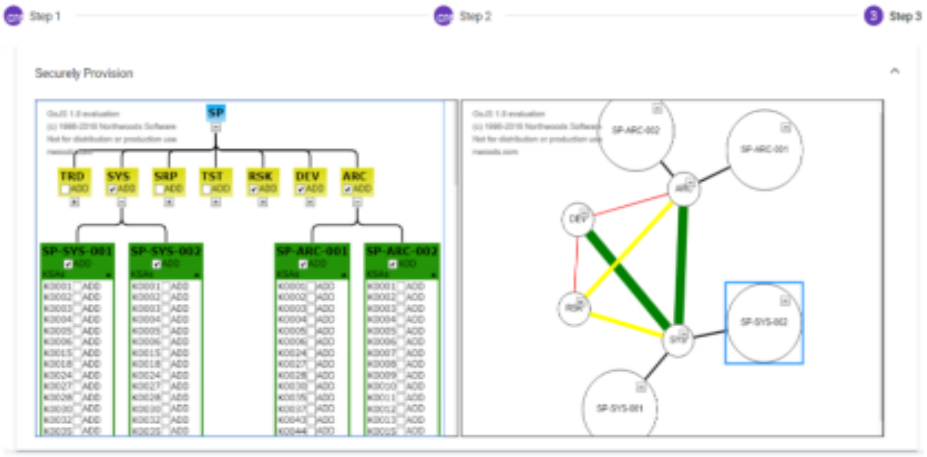

Fig. 6. Example screenshot of the graphical user interface

4 Course Evaluation

Each new course created in CyberMaster is represented as an incremental tree (See Fig. 6) which is then transformed and saved as a concept map that holds all the course components, strength of connections, and course tags. The curriculum evaluation component in CyberMaster provides an overall evaluation for the concept map in which a final score is computed based on the strength of the connections between the different components including specialty areas, work roles and KSAs. This score provides a measure of how good the curriculum design is. Moreover, CyberMaster provides recommendations on how to make the design better; for example, information is provided on specialty areas and/or KSAs that can be added or removed from the current design to enhance the curriculum design (see Figure 7). The user has the freedom to apply the recommendations or leave the course as is.

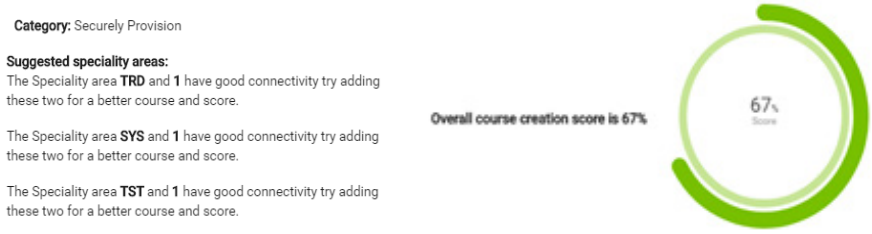

Fig. 7. An example screenshot of user feedback provided by CyberMaster

5 Conclusion

This paper presents work in progress to develop an expert system to guide instructors while developing cybersecurity courses in a rapid and reliable way. The system contributes to changing the current status of cybersecurity education by helping instructors anywhere in the world to develop cybersecurity courses. The culmination of this work is a robust, fully usable online curriculum development tool that can be used by both novice as well as experienced cybersecurity educators. The system evaluates every course design for quality in terms of its cohesiveness – how well the course components fit together – and conformity to a published framework for cybersecurity curriculum design. It provides a normalized course evaluation score to indicate the closeness of the curriculum to the framework. Initial test results show that CyberMaster can guide users to develop curricula following the NICE framework for cybersecurity education. Although, the interactive and guided design process currently ensures conformity of the course content with the NICE framework, additional cybersecurity education frameworks can be added as an option in future.

6 Acknowledgement

This work is part of a project funded by an NSA CAE Cybersecurity Grant Program Grant H98230-17-0316.

7 References

[1] Identity Theft Resource Center. (2018 July 21). *Data Breaches*. Retrieved from https://www.idtheftcenter.org/data-breaches
[2] Shuangbao Wang, Amjad Ali, and William Kelly (2015). Data security and threat modeling for smart city infrastructure. pp. 1–6.
[3] Shuangbao Wang and William Kelly (2014). invideo a novel big data analytics tool for video data analytics. pp. 1–19. https://doi.org/10.1109/ITPRO.2014.7029303
[4] Karen Evans and Franklin Reeder (2010). A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. CSIS.
[5] William A Galston and Karen J Baehler (1995). Rural Development in the United States: Connecting Theory, Practice, and Possibilities. ERIC.

[6] National Center for Education Statistics. Downloaded April 12, 2017
[7] Terri Duggan Schwartzbeck, Cynthia D Prince, Doris Redfield, Helen Morris, and P Hammer (2003). How are rural districts meeting the teacher quality requirements of no child left behind. Charleston, VA: Appalachia Educational Laboratory.
[8] Weldon Beckner and Bruce O Barker (1994). Technology in Rural Education. Fastback No. 366. ERIC.
[9] Pavla Dr´aˇzdilov´a, Gamila Obadi, Kateˇrina Slaninov´a, Shawki Al-Dubaee, Jan Martinoviˇc, and V´aclav Sn´aˇsel (2010). Computational intelligence methods for data analysis and mining of elearning activities. In Computational intelligence for technology enhanced learning, pp. 195–224. Springer. https://doi.org/10.1007/978-3-642-11224-9_9
[10] Shuangbao Wang, William Kelly, and Jiayin Zhang (2015). Using novel video indexing and data analytics tool to enhance interactions in e-learning. pp. 1919–1927.
[11] Paul Wang and William Kelly (2015). A novel threat analysis and risk mitigation approach to prevent cyber intrusions. Colloquium for Information System Security Education (CISSE), 3:157–174.
[12] Dan Shoemaker, Anne Kohnke, and Ken Sigler (2016). A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0): A Guide to the National Initiative for Cybersecurity Education (NICE) Framework (2.0), volume 3. CRC Press. https://doi.org/10.1201/b19962
[13] NIST. Downloaded April 8, 2017
[14] Kortuem, G., Bandara, A. K., Smith, N., Richards, M., & Petre, M. (2013). Educating the Internet-of-Things generation. Computer, 46(2), 53-61.https://doi.org/10.1109/MC.2012.390
[15] Abdel-Badeeh M Salem, Mohamed Roushdy, and Rania A HodHod (2005). A case based expert system for supporting diagnosis of heart diseases. AIML Journal, 5(1):33–39.
[16] Abdel-Badeeh M Salem and Rania A HodHod (2002). A hybrid expert system supporting diagnosis of heart diseases. In Proceedings of Intelligent Information Processing, pages 301–305. Springer. https://doi.org/10.1007/978-0-387-35602-0_32
[17] Ragab, A. H. M., Fakeeh, K. A., Roushdy, M. I. (2004). A Medical Multimedia Expert System for Heart Diseases Diagnosis & Training. In the Proceedings of the 2nd Saudi Science Conf., Fac. Sci., KAU, IV: 31-45.
[18] Norman I Birndorf, Jeffrey O Pentecost, James R Coakley, and Kent A Spackman (1996). An expert system to diagnose anemia and report results directly on hematology forms. Computers and biomedical research, 29(1):16–26, 1996. https://doi.org/10.1006/cbmr.1996.0002
[19] Chang-Shing Lee and Mei-Hui Wang. A fuzzy expert system for diabetes decision support application (2011). IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 41(1):139–153. https://doi.org/10.1109/TSMCB.2010.2048899
[20] F Filippetti, M Martelli, G Franceschini, and C Tassoni (1992). Development of expert system knowledge base to on-line diagnosis of rotor electrical faults of induction motors. In Industry Applications Society Annual Meeting, Conference Record of the 1992 IEEE, pages 92–99. IEEE. https://doi.org/10.1109/IAS.1992.244459
[21] Heung-Jae Lee, Deung-Yong Park, Bok-Shin Ahn, Young-Moon Park, Jong-Keun Park, and SS Venkata (2000). A fuzzy expert system for the integrated fault diagnosis. IEEE Transactions on Power Delivery, 15(2):833–838. https://doi.org/10.1109/61.853027
[22] Ojenge Winston and Muchemi Lawrence (2008). Career guidance using expert system approach. Strengthening the Role of ICT in Development, 123.
[23] Olawande Daramola, Onyeka Emebo, IT Afolabi, and CK Ayo (2014). Implementation of an intelligent course advisory expert system. IJARAI) International Journal of Advanced Research in Artificial Intelligence, 5(4). https://doi.org/10.14569/IJARAI.2014.030502

[24] Jeff Shrager and Timothy W Finin (1982). An expert system that volunteers advice. In AAAI, pages 339–340.
[25] Roger Mackett and Marion Edwards (1996). An expert system to advise on urban public transport technologies. Computers, environment and urban systems, 20(4):261–273. https://doi.org/10.1016/S0198-9715(96)00020-8
[26] Luconi, F. L., Malone, T. W., & Scott Morton, M. S. (1985). Expert systems and expert support systems: the next challenge for management.
[27] Cullen, J. and Bryman, A. (1988). The knowledge acquisition bottleneck: time for reassessment? Expert Systems, 5(3), pp.216-225. https://doi.org/10.1111/j.1468-0394.1988.tb00065.x
[28] Dumitru Dan Burdescu, Marian Cristian Mihaescu, and Bogdan Logofatu (2008). Building a decision support system for students by using concept maps. In ICEIS (2), pp. 130–135.
[29] Brian R Gaines and Mildred LG Shaw. Concept maps as hypermedia components (1995). International Journal of Human-Computer Studies, 43(3):323–361. https://doi.org/10.1006/ijhc.1995.1049
[30] Byron Marshall, Hsinchun Chen, and Therani Madhusudan (2006). Matching knowledge elements in concept maps using a similarity flooding algorithm. Decision Support Systems, 42(3):1290–1306. https://doi.org/10.1016/j.dss.2005.10.009
[31] Ying Feng, Robert L Goldstone, and Vladimir Menkov (2004). Absurdist ii: A graph matching algorithm and its application to conceptual system translation. In FLAIRS Conference, pp. 640–645.
[32] Fausto Giunchiglia, Mikalai Yatskevich, and Pavel Shvaiko (2007). Semantic matching: Algorithms and implementation. In Journal on data semantics IX, pp. 1–38. Springer. https://doi.org/10.1007/978-3-540-74987-5_1
[33] Zolt´an Baracskai, Hungary Viktor D¨orfler, and Jol´an Velencei (2008). Concept mapping and expert systems: exploring synergies. In 3rd International Conference on Concept Mapping.
[34] Wang-Kun Chen and Ping Wang (2012). A framework of active learning by concept mapping. Online Submission.
[35] David Benyon and Dianne Murray (1993). Applying user modeling to human-computer interaction design. Artificial Intelligence Review, 7(3):199–225. https://doi.org/10.1007/BF00849555

8 Authors

Rania Hodhod received Ph.D. in computer science at University of York, UK. From 2011-2013, Rania was a Postdoctoral Research Fellow at the Adaptive Digital Media (ADAM) Lab in the Georgia Tech School of Literature, Media and Communication. Dr. Hodhod is currently the Assistant Chair of TSYS School of Computer Science, Columbus State University (CSU). She has published over 45-refereed articles and two book chapters in these areas. Her current research work on intelligent systems is supported by the National Science Association (NSA). Dr. Hodhod is the holder of the CSU Teaching and Learning Award 2017 and was a finalist for the Faculty Research and Scholarships Award at CSU 2016. She also received the Columbus State University Outstanding Teacher of Writing Award and Recognition of Excellence: Graduate Faculty Award in 2015.

Shuangbao (Paul) Wang received Ph.D. in computer science at George Mason University at Fairfax, Virginia USA under the guidance of Dr. Robert Ledley, the inventor of body CT scanner in 2004.

Paul is a professor and TSYS endowed chair in cybersecurity. He was previous the Chief Information and Technology Officer (CIO/CTO) of the National Biomedical Research Foundation (NBRF). He has been speakers to many major cybersecurity and IoT conferences. His research areas are secure architecture, IoT/CPS, cryptography and video indexing.

Prof. Wang is the recipient of Advanced Simulation and Training Award by the Link Foundation. He was directly involved in drafting of the National Initiative of Cybersecurity Education (NICE) framework. In addition to books, referred publications, conference speakers and numeral grant activities, Paul has four patents; three of them have been licensed to the industry.

Shamim Khan earned his BS and MS in Applied Physics & Electronics from Rajshahi University in Bangladesh, and a Ph.D. in Computer Science from the University of Manchester, UK for his work on parallel image processing.

Dr. Khan taught Computer Science at the National University of Singapore and Murdoch University in Australia. He is currently a Professor and Director of Graduate Studies at the TSYS School of Computer Science, Columbus State University.

Apart from computer vision, Dr. Khan's current research interests include the application of artificial intelligence techniques for knowledge representation and decision support, computer science education and cybersecurity. He has numerous publications in refereed journals and conference proceedings in the areas of soft computing, intelligent decision support, computer vision and computer science education.

Article submitted 13 October 2018. Resubmitted 16 November 2018. Final acceptance 07 January 2019. Final version published as submitted by the authors.