Communications in Computer and Information Science 1549

More information about this series at https://link.springer.com/bookseries/7899

Ram Krishnan · H. Raghav Rao ·
Sanjay K. Sahay · Sagar Samtani ·
Ziming Zhao (Eds.)

Secure Knowledge Management In The Artificial Intelligence Era

9th International Conference, SKM 2021
San Antonio, TX, USA, October 8–9, 2021
Proceedings

Springer

Editors
Ram Krishnan
The University of Texas at San Antonio
San Antonio, TX, USA

H. Raghav Rao
The University of Texas at San Antonio
San Antonio, TX, USA

Sanjay K. Sahay
Birla Institute of Technology and Science
Pilani, Rajasthan, India

Sagar Samtani
Indiana University
Bloomington, IN, USA

Ziming Zhao
SUNY Buffalo
Buffalo, NY, USA

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-3-030-97531-9 ISBN 978-3-030-97532-6 (eBook)
https://doi.org/10.1007/978-3-030-97532-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

With the advent of revolutionary technologies such as artificial intelligence (AI), machine learning, cloud computing, big data, and IoT, secure knowledge management (SKM) continues to be an important research area that deals with methodologies for systematically gathering, organizing, and disseminating information in a secure manner. The recent development of AI in the security arena shows a promising future, and there is no doubt that AI can provide new ideas and tools for SKM. This conference on SKM brings together researchers and practitioners from academia, industry, and government on a global scale. The aim of the SKM conference is to present and discuss the most recent innovations, trends, and concerns including practical challenges encountered and solutions adopted with a special emphasis on AI. SKM 2019 was held at the BITS Pilani Goa Campus, India, and past iterations of SKM were held at SUNY at Buffalo, SUNY Albany, NYU, SUNY Stony Brook, UT Dallas, Rutgers University, BITS Dubai, and the University of South Florida. Following the biennial tradition of the Secure Knowledge Management Workshop that began in 2004, SKM 2021 was hosted by the University of Texas at San Antonio, USA, during October 8–9, 2021. The conference took place virtually due to the COVID-19 pandemic.

SKM 2021 received many high-quality submissions, with authors coming from countries such as the USA, India, Austria, Norway, and Ireland. A total of 30 research papers were received by the Technical Program Committee (TPC). The TPC of SKM 2021 comprised researchers and industry practitioners from all corners of the world. Most of the submitted papers received three reviews, and each paper received at least two reviews. The review process was double-blind, and after the careful review process, the top 11 papers were selected for publication in this proceedings volume, with an acceptance rate of 36.6%.

The conference was organized over two days with a very compact schedule. Beyond the technical program of the research papers, the conference was enriched by many other items. The conference program featured three keynotes: James Joshi (University of Pittsburgh) spoke on the privacy challenges we face in the emerging world in his talk titled “Privacy – Challenges and Directions”, Stephanie Hazlewood (IBM) spoke on the challenges in using AI for securing organizations in light of attackers armed with AI technology as well (“Cybersecurity: AI vs AI”), and Hsinchun Chen (University of Arizona) spoke on the decade-long effort and journey in building the University of Arizona Eller/MIS AZSecure Cybersecurity Program (“Building the UA/Eller/MIS AZSecure Cybersecurity Analytics Program: My Journey”).

The conference also featured a panel on “Women in Cybersecurity”, which was chaired by Bhavani Thuraisingham (University of Texas at Dallas) with the support of PhD student volunteer, Alexis Votto. The panel members were Sharmistha Bagchi-Sen (Arizona State University), Nicole Lang Beebe (University of Texas at San Antonio), Elisa Bertino (Purdue University), Heng Xu (American University), and Danfeng (Daphne) Yao (Virginia Tech).

We are very much thankful to the speakers, panelists, and authors for their active participation in SKM 2021. We are also thankful to Springer for providing continuous guidance and support. We extend our heartfelt gratitude to the TPC members and external reviewers for their efforts in the review process. We are indeed thankful to everyone who was directly or indirectly associated with the organizing team of the conference leading to a successful event. We also gratefully acknowledge US National Science Foundation grant 2133980 for partially funding the conference. We hope the proceedings will inspire more research in secure knowledge management, digital payments, and the application of artificial intelligence.

January 2022

Ram Krishnan
H. Raghav Rao
Sanjay K. Sahay
Sagar Samtani
Ziming Zhao

Organization

Steering Committee

Kwiat, Kevin	Air Force Research Laboratory, USA
Memon, Nasir	New York University, USA
Rao, H. Raghav	University of Texas at San Antonio, USA
Thuraisingham, Bhavani	University of Texas at Dallas, USA
Upadhyaya, Shambhu	University at Buffalo, USA

General Chairs

Krishnan, Ram	University of Texas at San Antonio, USA
Rao, H. Raghav	University of Texas at San Antonio, USA

Technical Program Committee Chairs

Samtani, Sagar	Indiana University, USA
Zhao, Ziming	University at Buffalo, USA

Publicity Chairs

Bou-Harb, Elias	University of Texas at San Antonio, USA
Shah, Ankit	University of South Florida, USA

Scientific Chair

Sahay, Sanjay K.	BITS Pilani, Goa Campus, India

Technical Program Committee

Abdelsalam, Mahmoud	Manhattan College, USA
Al-Alaj, Abdullah	Virginia Wesleyan University, USA
Benjamin, Victor	Arizona State University, USA
Bertino, Elisa	Purdue University, USA
Bhatt, Smirti	Texas A&M University, USA
Bose, Indranil	NEOMA Business School, France
Chen, Rui	Iowa State University, USA
Cheng, Yuan	California State University, USA
Chowdhury, Dipanwita Roy	IIT Kharagpur, India

Goel, Sanjay	University of Albany, USA
Gupta, Maanak	Tennessee Technological University, USA
Halder, Raju	IIT Patna, India
Hu, Hongxin	University at Buffalo, USA
Hu, Peizhao	Rochester Institute of Technology, USA
Jain, Shweta	City University of New York, USA
Jaiswal, Raj K.	BITS Pilani, Goa Campus, India
Li, Weifeng	University of Georgia, USA
Liang, Yunji	Northwestern Polytechnic University, USA
Liu, Peng	Pennsylvania State University, USA
Masoumzadeh, Amirreza	University at Albany, USA
Medrano, Carlos Rubio	Texas A&M University-Corpus Christi, USA
Mehnaz, Shagufta	Dartmouth College, USA
Mi, Xianghang	University at Buffalo, USA
Mishra, Sumita	Rochester Institute of Technology, USA
Mohaisen, Aziz	University of Central Florida, USA
Nam, Kichan	American University of Sharjah, UAE
Narang, Pratik	BITS Pilani, India
Ninglekhu, Jiwan	InterDigital Communications, USA
Pal, Abhipsa	IIM Kozhikode, India
Park, Jaehong	University of Alabama in Huntsville, USA
Ratazzi, Paul	Air Force Research Laboratory, USA
Rathore, Hemant	BITS Pilani, Goa Campus, India
Ray, Indrakshi	Colorado State University, USA
Santanam, Raghu	Arizona State University, USA
Shah, Ankit	University of South Florida, USA
Shan, Jay	Miami University, USA
Sharma, Ashu	Mindtree, Hyderabad, India
Thakur, Rahul	IIT Roorkee, India
Vaish, Abhishek	IIIT Allahabad, India
Valecha, Rohit	University of Texas at San Antonio, USA
Verma, Rakesh	University of Houston, USA
Wang, Huibo	Baidu Security, USA
Wang, Jingguo	University of Texas at Arlington, USA
Wang, Weihang	University at Buffalo, USA
Xiao, Nan	University of Texas Rio Grande Valley, USA
Yang, Jay	Rochester Institute of Technology, USA
Zhang, Penghui	Arizona State University, USA
Hongyi, Zhu	University of Texas at San Antonio, USA

Abstracts of Invited Talks

Privacy - Challenges and Directions

James Joshi

School of Computing and Information, University of Pittsburgh, PA, USA
jjoshi@pitts.edu

Rapid advances in computing and information technologies are enabling a hyper-connected world. Enabled by such connectivity and the growing computational power/infrastructures at our disposal, innovative Artificial Intelligence (AI) and Machine Learning (ML) techniques are increasingly being deployed in various applications. Innovations in AI/ML is further being fueled by huge amounts of data that is continuously collected in myriad of ways, including data that has or can reveal highly privacy-sensitive information about us. While AI/ML technologies and the huge amounts of data available can be used for immense benefits for our society, privacy issues pose as a huge potential roadblock. Globally, there is also increasing number of privacy regulations being introduced to address privacy challenges related to access to and use of data by analytic engines and AI/ML-enabled applications. In this talk, he discuss the current privacy challenges that we face in emerging world that is increasingly reliant on technologies and some directions for research. He also briefly overview the National Science Foundation's Secure and Trustworthy Cyberspace program, and other programs that are aligned with the themes of this conference.

Building the UA/Eller/MIS AZSecure Cybersecurity Analytics Program: My Journey

Hsinchun Chen

University of Arizona, Eller College of Management, Management Information Systems Department, Tucson, AZ 85721, USA
hchen@eller.arizona.edu

In this talk, a decade-old effort and journey in building the University of Arizona Eller/MIS AZSecure Cybersecurity Program has been discussed. Based on $15M+ funding from the National Science Foundation (NSF) SaTC (Secure and Trustworthy Cyberspace), ACI (Advanced Cyber Infrastructure), and SFS (CyberCorps Scholarship-for-Service) programs since 2012, our research team at the Eller/MIS Artificial Intelligence (AI) Lab has developed significant Cybersecurity Analytic research in: (1) Dark Web Analytic for studying international hacker community, forums, and markets; (2) Privacy and PII (Personal Identifiable Information) Analytic for identifying and alleviating privacy risks for vulnerable populations; (3) Adversarial Malware Generation and Evasion for adversarial AI in cybersecurity; and (4) Smart Vulnerability Assessment for scientific workflows and OSS (Open Source Software) vulnerability analytics and mitigation. Our research advances the development of large-scale longitudinal cybersecurity data (e.g., hacker forms, darknet markets, stolen email accounts, malware source code and binary, GitHub OSS, scientific VMs) and advanced AI and DL/ML (deep learning and machine learning) based algorithmic and representational innovations (e.g., transfer learning, attention mechanism, multi-view learning, transformer) inspired by unique cybersecurity domain-specific characteristics, practices and opportunities. As a leader in advanced cybersecurity education, University of Arizona has received the CAE-CD/R/CO cybersecurity designations from NSA/DHS and significant SFS fellowship funding from NSF.

Cybersecurity: AI vs AI

Stephanie Hazlewood

Security Automation, IBM Security, Canada
stephanie@ca.ibm.com

In the rapidly transforming business domain of today applications have become modular and containerized. Large amounts of data generated from business processes serve as shared resources for conducting advanced analytic and building robust Artificial Intelligence (AI) models. In the current state-of-the-art AI cybersecurity, there exist many complexities such as the presence of too many vendors and alerts. AI is a double-edged sword as it is used by both attackers as well as cybersecurity professionals, to mount attacks and defend against them. In essence, AI addresses three key business issues – prediction, automation and optimization.

Security threats that organizations face continue to increase exponentially. However, AI-infused security solutions bring speed and accuracy to help businesses proactively protect their assets, more accurately detect threats, and respond faster when security incidents arise. The future of cybersecurity converges with AI strengths and thus this talk focuses on how Trusted AI systems can be implemented that provide fair, explainable, and robust business insights. She also discuss how security solutions must defend against attackers that use AI to enhance the speed and accuracy of their own attacks.

Women in Cyber Security at the International Conference on Secure Knowledge Management in the Artificial Intelligence Era

Bhavani Thuraisingham[1], Alexis Votto[2], Sharmistha Bagchi-Sen[3], Nicole Beebe[4], Elisa Bertino[5], Heng Xu[6], and Daphne Yao[7]

[1] The University of Texas at Dallas, USA
bhavani.thuraisingham@utdallas.edu
[2] The University of Texas at San Antonio, USA
Alexis.Votto@utsa.edu
[3] Arizona State University, USA
Sharmistha.Bagchi-Sen@asu.edu
[4] The University of Texas at San Antonio, USA
Nicole.Beebe@utsa.edu
[5] Purdue University, USA
bertino@purdue.edu
[6] American University, USA
xu@american.edu
[7] Virginia Tech, USA
danfeng@vt.edu

Secure Knowledge Management (SKM) Workshop/Conference was the first venue to host an event on Women in Cyber Security. With a grant from the National Science Foundation, Profs. Sharmistha Bagchi-Sen, Shambhu Upadhyaya, and H. Raghav Rao, all from the University of Buffalo, hosted the first Women in Cyber Security panel at SKM 2004. Since then the panel was organized at various SKM events. The most recent panel was chaired by Prof. Bhavani Thuraisingham at SKM 2021 on October 09, 2021 and coordinated by Ms. Alexis Votto. The panelists were Profs. Sharmistha Bagchi- Sen, Nicole Beebe, Elisa Bertino, Heng Xu, and Daphne Yao. Each of the panelists discussed their work in cyber security and as well as opportunities and challenges for women in cyber security. Sharmistha discussed her work on geography and security as well as the need to focus on Diversity, Equity add Inclusion (DEI). Nicole discussed her initial work for the Air Force in cyber security and her more recent research in academia in areas such as digital forensics. She also discussed opportunities for research grants in cyber security. Elisa discussed her initial work in database management and then her work in cyber security. In particular she discussed her early research in secure database systems and then how she migrated into secure wireless networks and 5G technologies. Heng discussed her research in data privacy, fairness in artificial intelligence and her most recent work in cyber security governance. She also discussed aspects of social responsibility as well as the need for change to lead the future. Finally, Daphne discussed

A panel discussion chaired by Bhavani Thuraisingham and coordinated by Alexis Votto.

her research on crypto systems, certifying data breaches as well anomaly detection. She also discussed the workshop she co-founded on Women in Cyber Security Research (Cyber-W) and about overcoming racism and sexism in one's career. She emphasized that persistence is important and never to give up. She also discussed about how some women face the impostor syndrome and the need to get help from others. After the panel positions, the audience asked several questions. For example, one of the questions asked was to discuss the challenges for women in cyber security. One panelist answered that early in her career one of the bosses essentially mentioned that women need to have a thick skin in engineering. Also, when she was a tenure track assistant professor, one colleague asked her why do you want to go for tenure? I thought you would want to be in the Mommy track. She also added that there are roadblocks for women and they have to work extremely hard to get ahead. She said that it is very important to prioritize. Another panelist mentioned that we have come a long way compared to, say, the 1980s. She ignores such comments as it is not easy to convince others to change their behavior. Another panelist mentioned that some women have left their careers not because of one or two comments, but due to the community not supporting them. For example, female faculty that take maternity leave may not have published as much during their leave. When such faculty are being criticized for this it's very important that other faculty explain the reasons and support the female faculty. One panelist mentioned that the challenges are even more for BIPOC (Black, Indigenous, and People of Color) women and there is a concrete ceiling for them. Another panelist mentioned that we need policies to support women as well as men and also focus on the inequity in research areas. For example, it's harder to publish in some areas and this has to be recognized. The panel chair mentioned that none of us would be where we are now if not for the women who came before us. She also added that she would never have been in the position she is in now fifty years ago.

Another question from the audience was how to select an area for research and get funding for the research projects. There was an interesting discussion on this topic. It depends on whether you are in, say, Computer Science (where funding and top tier conference publications are important) and Business (where journal publications are important). It was felt that one has to also pursue one's passion. Another panelist discussed the importance of interdisciplinary research and the challenges involved such as bringing in behavioral scientists into cyber security research. The panel chair also mentioned that when she did not mention her title in an email, she was referred to as a student from the University of Texas at Dallas. She felt that this is subconscious bias because her name was a foreign sounding one. For example, had her name been a very English sounding name such a mistake may not have been made. Finally, the chair asked each panelist for their ending statements with respect to her research as well as on supporting women. One panelist mentioned that we need more data for research. She added that advancing women including BIPOC women is critical. Another panelist mentioned to follow your passion. She also cautioned not to swing the pendulum too far and we must not promote a person just because she is a woman or from an underrepresented minority community. A third panelist mentioned that we need to motivate our students and carry out systematic research. A fourth panelist mentioned that we need a pipeline of women so that the representation of women continues to increase. Another panelist mentioned

that research depends on the stage you are in. For example, before tenure focus on the publications and grants, But after tenure you need it make an impact with your research. Finally, a panelist mentioned that we need an end-to-end plan for research. She also added that the concrete ceiling comment made earlier is very true. Finally, she offered that we should not be unhappy as it could destroy us. We must be positive and do the best we can. The panel chair agreed with the panelists that we cannot change others and not to be unhappy when others are mean to us. We must support each other. The panel chair has mentioned that a high income career is a must for every woman and a person from the underrepresented minority community. She emphasized that this is especially true for women. She ended the panel by saying "what better way to have an intellectually stimulating and yet a high income career than pursuing one in cyber security".

Contents