Emad Saad Alsuwat

CONTACT INFORMATION

Department of Computer Science
College of Computers & Information Technology
Taif University
P.O. Box 888
Al-Hawiya, Taif, 21974 Kingdom of Saudi Arabia
E-mail: Alsuwat@tu.edu.sa or Alsuwat@live.com

PERSONAL INFORMATION

Born in Taif, Saudi Arabia
Saudi citizen
Website:
Phone: (+966) 555537280

LANGUAGES

Arabic (native)
English (very fluent)

PROFESSIONAL EXPERIENCE

Assistant Professor 2019 - present
Department of Computer Science
College of Computers and Information Technology
Taif University

Research Assistant 2016 – 2019
Probabilistic Graphical Models Laboratory
Department of Computer Science and Engineering
College of Engineering and Computing
University of South Carolina, Columbia, SC, USA

Research Assistant 2012 – 2019
Center for Information Assurance Engineering (a leading academic institute in the United States for Cybersecurity Education and Research)
Department of Computer Science and Engineering
College of Engineering and Computing
University of South Carolina, Columbia, SC, USA

Teaching Assistant 2012 – 2014
Department of Computer Science and Engineering
College of Engineering and Computing
University of South Carolina, Columbia, SC, USA

Teaching Assistant 2009 – 2011
Department of Computer Science
College of Computers and Information Technology
Taif University

EDUCATION

***Doctor of Philosophy (Ph.D.)*, Computer Science and Engineering**
University of South Carolina, Columbia, SC, December 2019
Concentration: Cybersecurity and Machine Learning
Dissertation Title: "Challenges in Large-scale Machine Learning Systems: Security and Correctness"

Major Advisors: Prof. Csilla Farkas and Prof. Marco Valtorta
Overall GPA: 3.767 / 4

***Graduate Certificate*, Graduate Certificate in Cybersecurity Studies**
University of South Carolina, Columbia, SC, May 2018
Concentration: Cybersecurity

***Master of Science*, Computer Science and Engineering**
University of South Carolina, Columbia, SC, December 2014
Concentration: Cybersecurity
Thesis Title: "Practical Concurrency Support for Web Service Transactions"
Major Advisor: Prof. Csilla Farkas

***Degree of Information Assurance Specialization*, National Training Standard for Information Systems Security (INFOSEC) Professionals, CNSS 4011**
Evaluated under the *IA Courseware Evaluation Program of the National Security Agency (NSA) and the Committee on National Security Systems (CNSS)*
University of South Carolina, Columbia, SC, May 2014
Concentration: Cybersecurity

***Bachelor of Science*, Computer Science**
Taif University, Taif, Saudi Arabia, May 2008
Concentration: Computer Science

Ph.D. QUALIFYING EXAM

No.	Field	Time	Result
[1]	Information Security Principles	Fall 2016	Passed from the first time
[2]	Analysis of Algorithms	Fall 2016	Passed from the first time
[3]	Compiler Construction	Fall 2016	Passed from the first time

RESEARCH INTERESTS

Cybersecurity: Information security; Data integrity; Secure machine learning; Adversarial machine learning; Data poising attacks; Evasion attacks; Resilience analysis of probabilistic graphical models against cyber attacks; Secure database systems; Concurrency control in database systems; Concurrency support for web service transactions; Security of cryptographic shuffling algorithms against cyber attacks; Concept drift detection; distinguishing between cyber attacks and natural concept drift

Uncertainty in Artificial Intelligence: Probabilistic Graphical Models (especially Bayesian Networks); Applications of Bayesian networks; Link strength measures in Bayesian networks; Structure learning of Bayesian network models from data; Performance improvement of current Bayesian network structure learning algorithms

BRIEF BIOGRAPHY

Emad Alsuwat (Ph.D., University of South Carolina, 2019) is an assistant professor of Computer Science in the College of Computers and Information Technology at Taif University. He received a bachelor degree with first class honors in computer science from Taif University in 2008 and a master of science degree with first class honors in computer science and engineering from the department of computer science and engineering at the University of South Carolina in 2014. Emad Alsuwat is a certified cybersecurity trainer since May 2014 as he joined the National Training Standard for Information Systems Security (INFOSEC) Professionals, CNSS 4011 during his graduate work at the University of South Carolina. He Also received a graduate certificate in cybersecurity studies from the department of computer science and engineering at the University of South Carolina in 2018. In January 2020 he joined the faculty at the

college of computers and information technology at Taif University. Emad's research interests are in the fields of cybersecurity, machine learning and adversarial machine learning. His research interests are in cybersecurity and machine learning, namely probabilistic graphical models. His first research result, which is known as "Alsuwat's link strength measure," is a novel mathematical technique that is useful to not only quantify the strength of links of causal models but also analyze the security of such causal models. Indeed, the proposed link strength measure plays a crucial role in identifying vulnerable network structures and the ease of corrupting the Bayesian models, and thus it is useful for increasing the robustness of probabilistic graphical models. Most of his later research has been in the area of secure machine learning, a.k.a adversarial machine learning. His theoretical and methodological contributions include results on measuring the uncertainty of links of causal models, an algorithm for learning the structure of Bayesian networks from data, theoretical frameworks to classify cyber attacks, namely data poisoning attacks, against Bayesian networks, a theoretical framework to classify long duration cyber attacks on causal models, algorithms for measuring the resilience of Bayesian network structure learning algorithms against traditional and long duration cyber attacks, algorithms for detecting adversarial attacks in the context of Bayesian networks, novel algorithms for data dependencies preserving shuffle, and a probabilistic graphical model framework to explicitly detect the presence of concept drift using latent variables.

HONORS AND AWARDS

Selected for submission to a special issue of Knowledge Discovery and Information retrieval Journal November 2019.

Selected among Best Students' Papers Award in KDIR'19 August 2019.

Selected among Best Students' Papers Award in DBSec'19 July 2019.

Selected for submission to a special issue of International Journal of General Systems August 2018.

Received Epsilon Pi Epsilon, the honor society for the computing and information disciplines April 2015

Received an award from Taif University for graduating with first honor, Ranked first on the College of Computers and Information Technology graduates May 2008

Received multiple awards from the Ministry of Education in Saudi Arabia for being one of the highly scored students in middle and high school 2001-2002-2003-2004

JOURNAL PUBLICATIONS

[1] Emad Alsuwat, Hatim Alsuwat, Marco Valtorta & Csilla Farkas (2020) "Adversarial data poisoning attacks against the PC learning algorithm", International Journal of General Systems, 49:1, 3-31, DOI: 10.1080/03081079.2019.1630401

CONFERENCE PUBLICATIONS

[2] Hatim Alsuwat, Emad Alsuwat, Marco Valtorta, John Rose, and Csilla Farkas. "Modeling Concept Drift in the Context of Discrete Bayesian Networks." Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management - Volume 1: KDIR, ISBN 978-989-758-382-7, pages 214 - 224. DOI: 10.5220/0008384702140224, Vienna, Austria, September 17 - 19, 2019.

[3] Emad Alsuwat, Hatim Alsuwat, John Rose, Marco Valtorta, and Csilla Farkas. "Detecting Adversarial Attacks in the Context of Bayesian Networks." 33rd An-

nual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'19), , pages 3 - 22. Charleston, SC, USA - July 15 - 17, 2019.

[4] Hatim Alsuwat, Emad Alsuwat, Tieming Geng, Chin-Tser Huang, and Csilla Farkas. "Data Dependencies Preserving Shuffle in Relational Database", Second IEEE International Conference on Data Intelligence and Security (ICDIS), pages 180 - 187. South Padre Island, Texas, USA, June 28 - 30, 2019.

[5] Emad Alsuwat, Hatim Alsuwat, John Rose, Marco Valtorta, and Csilla Farkas. "Long Duration Data Poisoning Attacks on Bayesian Networks", Tech. report, University of South Carolina, SC, USA, 2019.

[6] Emad Alsuwat, Hatim Alsuwat, Marco Valtorta, and Csilla Farkas. "Cyber Attacks against the PC Learning Algorithm." Second International Workshop on A.I. and Security at ECML-18, pages 19 - 35. Dublin, September 10 - 14, 2018.

[7] Emad Alsuwat, Marco Valtorta, and Csilla Farkas. "How to Generate the Network You Want with the PC Learning Algorithm." Proceedings of the 11th Workshop on Uncertainty Processing (WUPES'18), pages 1 - 12. (Vaclav Kratochvıl and Jirina Vejnarova, editors.) Trebon, Czech Republic, June 6 - 9, 2018.

[8] Emad Alsuwat, Marco Valtorta, and Csilla Farkas, "Bayesian Structure Learning Attacks", Tech. report, University of South Carolina, SC, USA, 2018.

FUNDS AND FUNDED PROJECTS

Title: "Challenges in Large-scale Machine Learning Systems: Security and Correctness."
Agency: M. Bert Storey Engineering and Innovation Center, University of South Carolina.
Role: Ph.D. Student Amount: $35,000.
Period: January 2015 - December 2019.

TRAVEL GRANTS

M. Bert Storey Engineering and Innovation Center Travel Grant to attend the The ACM Conference on Computer and Communications Security (CCS) held in Dallas,Texas, USA October 30 - November 3, 2017.

M. Bert Storey Engineering and Innovation Center Travel Grant to present at the WUPES'18 Conference held in Trebon, Czech Republic June 6 - 9, 2018.

M. Bert Storey Engineering and Innovation Center Travel Grant to present at The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases held in Dublin, Ireland September 10 – 14, 2018.

M. Bert Storey Engineering and Innovation Center Travel Grant to present at the 2nd IEEE International Conference on Data Intelligence and Security (ICDIS) held in South Padre Island, Texas, USA June 24 - 26, 2019.

M. Bert Storey Engineering and Innovation Center Travel Grant to present at 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'19) held in Charleston, South Carolina, USA July 15 -17, 2019.

SERVICE AND ACTIVITIES

- **PC member**: IFIP WG 11.3 Conference on Data and Applications Security and Privacy.
- **PC member**: IEEE International Conference on Data Intelligence and Security.

- **Member**: The committee of Master of Cybersecurity Program at College of Computers and Information Technology, Taif University.
- **Volunteer:**
  - Student volunteer at Leadership and Service Center at the University of South Carolina. 2014 - 2018
  - Student volunteer in Information Technology Center of Indie Grits in Columbia, South Carolina. March 2016
  - Volunteer at Transitions Homeless Center at the state of South Carolina. 2013 - 2019

Last updated on June 5, 2020