

Emad Saad Alsuwat, Ph.D.
Assistant Professor

| | | |
|--------------------------------|--|----------------|
| 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: https://emadalsuwat.github.io/index.html Phone: (+966) 555537280 | |
| LANGUAGES | Arabic (native) English (very fluent) | |
| PROFESSIONAL EXPERIENCE | <i>Professional Consultant</i> Professional Development and Career Support Unit Deanship of Students Affairs Taif University | 2020 - present |
| | <i>Assistant Professor</i> Department of Computer Science College of Computers and Information Technology Taif University | 2019 - present |
| | <i>Research Assistant</i> Probabilistic Graphical Models Laboratory Department of Computer Science and Engineering College of Engineering and Computing University of South Carolina, Columbia, SC, USA | 2016 – 2019 |
| | <i>Research Assistant</i> 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 | 2012 – 2019 |
| | <i>Teaching Assistant</i> Department of Computer Science and Engineering College of Engineering and Computing University of South Carolina, Columbia, SC, USA | 2012 – 2014 |
| | <i>Teaching Assistant</i> Department of Computer Science College of Computers and Information Technology Taif University | 2009 – 2011 |

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 4011Evaluated 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 poisoning 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] Sara Almotrafi, Bdour Alkhudadi, Hatim Alsuwat, & Emad Alsuwat, (2021). "Cloud of Things (CoTs): Security, Threats, and Attacks", International Journal of Computer Science & Network Security, 21(8), 229 - 237. (**Web of Science** indexed journal)
- [2] Ghada Aljumaie, Ghada Alzeer, Reham Alghamdi, Hatim Alsuwat, & Emad Alsuwat, (2021). "Modern Study on Internet of Medical Things (IOMT) Security", International Journal of Computer Science & Network Security, 21(8), 254 - 266. (**Web of Science** indexed journal)

- [3] Asma Mohammed, Jamilah Alkhathami, Hatim Alsuwat, & Emad Alsuwat, (2021). "Security of Web Applications: Threats, Vulnerabilities, and Protection Methods", *International Journal of Computer Science & Network Security*, 21(8), 176 - 176. (**Web of Science** indexed journal)
- [4] Emad Alsuwat, Sabah Alzahrani & Hatim Alsuwat, (2021). "Detecting COVID-19 Utilizing Probabilistic Graphical Models", *International Journal of Advanced Computer Science and Applications(IJACSA)*, 12(6), 786-793. (**Web of Science** indexed journal)
- [5] Amjaad Altalhi, Maram AL-Saedi, Hatim Alsuwat, & Emad Alsuwat, (2021). "Privacy-Preserving in the Context of Data Mining and Deep Learning", *International Journal of Computer Science & Network Security*, 21(6), 137-142. (**Web of Science** indexed journal)
- [6] Leena Alotaibi, Azhar Alsalmi, Hatim Alsuwat, & Emad Alsuwat, (2021). "Bitcoin and the Monetary System Revolution Changes", *International Journal of Computer Science & Network Security*, 21(6), 156-160. (**Web of Science** indexed journal)
- [7] Bayan Al-Amri, Hatim Alsuwat, & Emad Alsuwat, (2021). "Human Factor & Artificial Intelligence: For future software security to be invincible, a confronting comprehensive survey", *International Journal of Computer Science & Network Security*, 21(6), 245-251. (**Web of Science** indexed journal)
- [8] Asalah Altwairqi, Hatim Alsuwat & Emad Alsuwat, (2020). "The Role of Dark Web on Cyberspace", *International Journal of Current Research*, 12(12), 15337-15341, DOI: 10.24941/ijcr.40274.12.2020.
- [9] Noha M. Altalhi, Emad Alsuwat, (2020). "Enhance Software Security Utilizing Code Obfuscation", *International Journal of Current Research*, 12(11), 14966-14969, DOI: 10.24941/ijcr.40257.11.2020.
- [10] Lama Alhathally and Emad Alsuwat, (2020). "Ransomware Attack Detection and Prevention", *International Journal of Current Research*, 12(11), 14917-14922, DOI: 10.24941/ijcr.40253.11.2020.
- [11] Reem Alqurashi and Emad Alsuwat, (2020). "Cyber Insurance: A Case Study of United Arab of Emirates, European Union's and Poland". *International Journal of Advances in Multidisciplinary Research*. 7(12), 6478 - 6482.
- [12] May Alotaibi and Emad Alsuwat, (2020). "Tracing Distributed Denial of Service Attacks from Practical Perspectives". *International Journal of Advances in Multidisciplinary Research*. 7(10), 6349-6354.
- [13] Abeer Alotaibi and Emad Alsuwat, (2020). "A Study on Social Engineering Attacks: Phishing Attack". *International Journal of Advances in Multidisciplinary Research*. 7(11), 6374-6379.
- [14] Hind Alshamari and Emad Alsuwat, (2020). "False Data Injection Attack in Healthcare". *International Journal of Advances in Multidisciplinary Research*. 7(11), 6397-6400.
- [15] Samah Alhusayn and Emad Alsuwat, (2020). The Buffer Overflow Attack and How to Solve Buffer Overflow in Recent Research. *Academic Journal of Research and Scientific Publishing*. 2(19), 1-13.
- [16] Asma Alsufyani and Emad Alsuwat, (2020). Smart Contract Survey. *Academic Journal of Research and Scientific Publishing*. 2(20), 12-20.
- [17] Ohoud Al-Harthi, Emad Alsuwat, (2020). "Comprehensive Study of Current Reverse Engineering Tools and Techniques", *International Journal of Science and Research (IJSR)*. 9(12), 924 - 927.

- [18] 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 (**Web of Science indexed journal, Q2, Impact Factor: 1.671**)

CONFERENCE PUBLICATIONS

- [19] 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.
- [20] Emad Alsuwat, Hatim Alsuwat, John Rose, Marco Valtorta, and Csilla Farkas. “Detecting Adversarial Attacks in the Context of Bayesian Networks.” 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec’19), , pages 3 - 22. Charleston, SC, USA - July 15 - 17, 2019.
- [21] 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.
- [22] 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.
- [23] 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.
- [24] 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 Kratochvil and Jirina Vejnarova, editors.) Trebon, Czech Republic, June 6 - 9, 2018.
- [25] 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: “Detecting COVID-19 Utilizing Probabilistic Graphical Models.”
 Agency: The Deanship of Scientific Research, Taif University
 Role: PI
 Amount: **SR**50,000.
 Period: June 2020 - February 2021.

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

- **Member:** Innovation and Entrepreneurship Center, Taif University. 2021 - Present
- **Session Chair:** The National Computing Colleges Conference (NCCC 2021), Taif University.
- **PC member:** The 4th Scientific Forum for Taif University Students.
- **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

GRADUATE STUDENTS

- [1] Asalah Altwairqi. Master in Cybersecurity. The title of her research project is “Cybersecurity Challenges in the Context of Probabilistic Graphical Models.”
- [2] Shahad Alzahrani. Master in Cybersecurity. The title of her research project is “On the effectiveness of Utilizing Latent Variable to Mitigate Data Poisoning Attacks in the Context of Bayesian Networks.”
- [3] Taghreed Almalki. Master in Cybersecurity. The title of her research project is “On the effectiveness of Data Poisoning Attacks on Probabilistic Graphical Models by Using Data Conflict Analysis.”
- [4] Asma Mohammed. Master in Cybersecurity. The title of her research project is “Robustness of Probabilistic Graphical Models to Dirichlet Distributed Cyberattacks.”

**MORE ON
GRADUATE
SUPERVISION**

- [1] Member of research project committees for multiple students at the Cybersecurity Program at Taif University.
- [2] Member of research project committees for multiple students at the Artificial Intelligence Program at Umm Al-Qura University.
- [3] Member of research project committees for multiple students at the Computer Science Program at Umm Al-Qura University.

**UNDERGRAD
STUDENTS**

- [1] Salma Althormani, Roqaya Alnemary, Kholoud AlNafei, Raghad Aljuaid, Hton Alsalmi, and Fatima Alshehri. Capstone Project 1&2. The title of their project is “An Interactive and Intelligent Application to Teach Chinese.”

**COURSES
TAUGHT**

[I] 2021 Fall Semester

- (501435-3) Algorithms Analysis and Design.
- (501513-2) Cryptography.
- (501110-2) Introduction to Problem Solving.
- (502801-3) Cryptography Theory.
- (502809-3) Research Project (Graduate).

[II] 2021 Spring Semester

- (501435-3) Algorithms Analysis and Design.
- (501125-2) Scientific Computing.
- (502805-3) Internet Security (Graduate).
- (501599-3) Capstone Project.
- (502809-3) Research Project (Graduate).

[III] 2020 Fall Semester

- (501435-3) Algorithms Analysis and Design.
- (501513-3) Cryptography.
- (501110-2) Introduction to Problem Solving.
- (502212-3) Digital and Computer Forensics (Graduate).
- (501599-3) Capstone Project.
- (502809-3) Research Project (Graduate).

[IV] 2020 Summer Semester

- (501435-3) Algorithms Analysis and Design.

[V] 2020 Spring Semester

- (502804-3) Software Security (Graduate).
- (501435-3) Algorithms Analysis and Design.
- (501125-2) Scientific Computing.

Last updated on October 14, 2021