January 2021

Welcome Message from Editor and Team!

Happy New Year!

We welcome you to January issue of IEEE Newsletter, Toronto section.

In this issue, you will read an article "A Non-Intrusive Technique for Asserting User Identity in Internet of Things." **(Page 5)**

Meet Sahar Rahmani; in our IEEE friends and supporters section. Enjoy reading her inspirational journey from an immigrant to senior director, Global Cyber Security, RBC. **(Page 2)**

First ever virtual IEEE AGM meeting was held in November, and you can see event pictures here.

You can find newsletter's previous issues here. You can explore our Library to access links to various newsletters, resources, and chapter activities.

By launching this newsletter, we intend to cover IEEE achievements and success stories specific to the Toronto area.

If you have any questions, suggestions, or concerns, please address them to the editor; Fatima Hussain at fatima.hussain@ryerson.ca. We hope to hear from you, and we welcome your feedback!

Editor's Note

Although this year has been hard on all of us, we can appreciate we made through it safe and sound. At the same time, our heart goes out for the ones who lost their loved ones during the pandemic. While we are still not done yet, we would like to wish a Happy New Year. We are

sending this message hoping that the next year is better than 2020, and our lives get back to normalcy.

May the celebrations of the new year fill in your hearts with high spirits. With unshaken determination, we are all set to embrace the new year with courage, hope, dreams, and faith. Stay safe, and take care of yourself and your loved ones.

Happy 2021 !

Meet Our Distinguished IEEE Supporters

Sahar Rahmani, Senior Director JSOC Analytics, Global Cyber Security, RBC

I am Sahar Rahmani, a PhD in science, an immigrant, a wife and a parent. Currently, I am the Director of a Data Science team at the Global Cyber Security (GCS) group at RBC. My role involves leading a team of data scientists and machine learning engineers to provide AI solutions for detecting the ever-changing landscape of cyber/digital crime. We collaborate with various teams both within RBC and with RBC's partners to implement scalable real-time machine learning solutions for their security related issues. We also bring insight and analytics to the big data aspect of cybersecurity to help executives make data-driven strategic decisions to keep our customers' information safe. I always encourage and emphasize innovations in the application of AI/ML in digital risk. This mindset has not only resulted in solving business problems in more effective ways, but has also resulted in creating multiple patents, publishing peer-reviewed research papers, and presenting conference talks. Besides the work-related activities, I teach in data science workshops and mentor students and junior data scientists to help them start or grow their career in the field of data science.

My graduate and post-graduate journey involved attending schools in three different continents: I earned my bachelor's degree in physics from the Sharif University in Iran, after which I moved to England to continue my studies in Astrophysics, where I got my master's degree from the University of Sussex. After spending a year in England, I moved to Canada to start my PhD at the university of the Western Ontario on August of 2012. During my PhD, I had the privilege to work with one of the most forward-thinking Astrophysics in Canada, Prof. Pauline Barmby. She encouraged me and taught me to look at problems from various angles and find novel solutions for them by studying and understandings techniques that are used in other fields of science. As a result of this exercise, I started to learn about data mining, machine learning, and numerous statistical models which built the foundation for my transition from academia to a role as a data scientist in industry. To be able to improve in my role and be best at what I do, I had to develop a few strategies in my life. The strategy that helped me most in facing new changes and challenges in my path is to put on my scientist hat when facing a challenge and try to come up with a novel and innovative way to find a resolution.

An important part of my life that has shaped me into the person I am today, is being an immigrant. People who don't live in their hometown know very well that leaving your city and country is not easy. There are always cultural shocks and family, friends and loved ones are missed. In a similar way, moving from academic life to an industry one is not an easy transition, neither. As an academic, I was accustomed to a research-based mindset. However, I have to learn that data scientists who works in the industry have to learn to maintain a balance between doing research for products as well as delivering the products in a fast-paced environment. As a woman who studied physics I was always in a minority group in both my academic and my industry life. But, if I learned one thing from living in different countries, it is how to adapt, navigate through challenges, and try to work towards improving myself and my environment. That's one of the reasons that I always encourage women to study in STEM fields and try to help women who are at the start of their career to have the confidence and the courage to speak up for themselves.

How can I navigate through all these activities, work, being a mom and have a life? Well, the answer is obvious: I get help. There is only 24 hours in a day and one cannot do all the work

alone. During my journey, I've always had support systems to help me through. My husband helps me in all aspect of taking care of my son and household chores. He always supports and encourages my decisions. My parents and sisters, although living thousands of kilometers away, always have a great role on pushing me forward and giving me the courage that I need to take on new challenges. My manger always supports me greatly, both in pushing me out of my comfort zone, and understanding and accommodating my family situation. My friends, my classmates, my team, and my colleagues are all essential factors in my successes. There are always challenges, roadblocks, and ups and downs on the way. I cannot emphasis enough the importance of my support groups during the hard days. I would not be in this stage of my life and career without them and I cannot thank them enough.

What's next then? Honestly who knows! Right now, I am working on improving my knowledge of cybersecurity and management. Working in the cross section of the cybersecurity and AI for the past few years has given me the belief that the combination of these two fields is one of the most important career paths in the future. You might have heard that in this era data is more valuable than oil and it must be protected. Our detection and protection systems improve by the hour, but in the same time threat actors are improving their techniques and the threat landscape changes rapidly and that is what make the hybrid of cyber security and AI so interesting and challenging. As we've seen in the past few months, life, and even the World, changes in a blink of an eye. A year ago, none of us would have thought that our lives would be so different as they are today. Who knows what will happen in the future and what it's effect will be on our lives. The best thing we can do is to embrace the challenge, always learn and improve ourselves and put our knowledge to best use.

A Non-Intrusive Technique for Asserting User Identity in Internet of Things

Ameera Al-Karkhi

Internet of Things environments are an exciting new computing scene due to the recent advances in wireless communications and digital electronics. These environments are small smart worlds that have many advantages, such as continuous and distributed interaction with people using a variety of wireless devices, which are ubiquitous and sharable, to provide useful services. In addition, each user has wide interaction with a huge number of entities. It would be impractical to require people to authenticate themselves every time they cross various network boundaries, as the frequent authentication process would disrupt the users' normal activities. The use of frequent authentication contradicts the objectives of Internet of Things in creating seamless environments and delivering distributed services. Due to the characteristics of these environments there is a challenge in dealing with asserting user identity. As a result, the need for a system to apply a non-intrusive authentication technique to assert user identity across the environment, and for every interaction within these environments, becomes one of the main challenges in these environments. My research aims to develop a technique for verifying user identity when interacting with such environments. User identity information is used by the system in Internet of Things environments to retrieve a variety of contextual information, which is necessary for providing the required services. In doing so, a new approach for asserting user identity that is non-intrusive and adaptable is developed. The approach, called Non-Intrusive Identity Assertion System (NIAS), would be aware of the intentions of the user and authenticate her/him continuously throughout the day to maintain confidence in user identity. It is assumed that users in smart environments carry identification devices which are used by NIAS to detect when users attempt to access resources. Although these devices provide a basic mechanism for identifying users, they are not sufficient to assert users' identity, for they could easily be picked up by other people. Therefore, NIAS attempts to assert users' identity by monitoring a minimum amount of their activities instead of extensive tracking. The system then uses these activities to infer user events. User events inference is achieved using an unsupervised

clustering technique, which gathers a group of user activities and creates an event. Then each user event has to be converted to a numeric value and passed to the system to assert user identity. The system should be able to cope with various situations, such as users losing their smart tags or people impersonating other people and raise an alarm to block an intruder from being asserted as a legitimate user. NIAS provides an alternative to the intrusive periodic user authentication process and, at the same time, minimize the risk of false identity in Internet of Things environments.

About the Author

Dr. Ameera Al-Karkhi is a professor at Sheridan college, she developed and conducted new courses on Internet of Things (IoT) such as cybersecurity and data analysis. She has worked as post doctorate fellow in Electrical and Computer Engineering department at Ryerson University, in the area of context aware systems and the Internet of Things (IoT) to design predictive systems and apply machine learning algorithms for various fields such as health centers in Ontario, to provide security and data analysis. She has various academic publications in various conferences and journals in computer engineering, control systems, machine learning and IoT domains. She contributed as a co-author to an introductory text on the Internet of Things technology published by Springer which covers the introduction to the entire IoT domain. Her recent publication is a chapter book on Mobile Edge cloud computing in Springer.

Get Involved with Us!

IEEE Toronto section is looking forward to hearing from you. your contributions are welcome to this monthly newsletter. We invite our members to share and submit:

- Short Story (about IEEE members, WIE members)
- News items and Affinity group reports
- Technical Articles/Blogs (Brief discussions of cutting edge research, new technological tools, topics of your choice)

Submission

Articles should be submitted in Word format. Word count for News items, Affinity group reports is 50 to 200 words and for blogs/ articles is 500 to 800 words.

Editor: Fatima Hussain

Contact: fatima.hussain@ieee.org

Coordinator: Ameera Karkhi

Contact: ameera.karkhi@gmail.com

Webmaster: Melanie Soliven

Contact: msoliven@ieee.org