SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures

Dr Bhavani Thuraisingham

The University of Texas at Dallas

While Artificial Intelligence was first conceived over 60 years ago, it is only recently that these AI systems are being used in practical applications in various fields such as medicine, finance, marketing, defense, transportation and manufacturing. For example, it is now possible to collect, store, manipulate, analyze and retain massive amounts of data and therefore the AI systems are now able to learn patterns from this data and make useful predictions. While AI has been evolving as a field during the past 60 years, the vast developments in computing and data management systems have resulted in serious security and privacy violations. Numerous cyber-attacks have occurred on such systems and various regulations are being proposed to handle big data so that the privacy of the individuals is not violated.

To address the security challenges of computing systems, AI and Security are being integrated. For example, machine learning techniques are being applied to solve security problems such as malware analysis and insider threat detection. However, there is also a major concern that the machine learning techniques themselves could be attacked. Therefore, the machine learning techniques are being adapted to handle adversarial attacks. This area is known as adversarial machine learning. In addition, privacy of the individuals is also being violated through these machine learning techniques as it is now possible to gather and analyze vast amounts of data.

With the advent of the web, computing systems are now being used in every aspect of our lives from mobile phones to autonomous vehicles. It is now possible to collect, store, manage, and analyze vast amounts of sensor data emanating from numerous devices and sensors including from various transportation systems. Such systems collectively are known as the Internet of Transportation, which is essentially the Internet of Things for Transportation, where multiple autonomous transportation systems are connected through the web and coordinate their activities. However, security and privacy for the Internet of Transportation and the infrastructures that support it is a challenge. Due to the large volumes of heterogenous data being collected from numerous devices, the traditional cyber security techniques such as encryption are not efficient to secure the Internet of Transportation. Some Physics-based solutions being developed are showing promise. More recently, the developments in AI/ML are also being examined for securing the Internet of Transportation and its supporting infrastructures.

To assess the developments on the integration of AI and Security over the past decade and apply them to the Internet of Transportation, the presentation will focus on three aspects. First it will examine the developments on applying AI techniques for detecting cyber security problems such as insider threat detection as well as the advances in adversarial machine learning. Some developments on privacy aware and policy-based data management frameworks will also be discussed. Second it will discuss the developments on securing the Internet of Transportation and its supporting infrastructures and examine the privacy implications. Finally, it will describe ways in which SecAI could be incorporated into the Internet of Transportation.

Biography of Dr Bhavani Thuraisingham

Dr. Bhavani Thuraisingham is the Founders Chair Professor of Computer Science and the Executive Director of the Cyber Security Research and Education Institute at the University of Texas at Dallas. She is also a visiting Senior Research Fellow at Kings College, University of London and an elected Fellow of the ACM, IEEE, the AAAS, the NAI and the BCS. Her research interests are on integrating cyber security and artificial intelligence/data science for the past 34 years (where it used to be computer security and data management/mining). She has received several awards including the IEEE CS 1997 Technical Achievement Award, ACM SIGSAC 2010 Outstanding Contributions Award, the IEEE Comsoc Communications and Information Security 2019 Technical Recognition Award, the IEEE CS Services Computing 2017 Research Innovation Award, the ACM CODASPY 2017 Lasting Research Award, the IEEE ISI 2010 Research Leadership Award, and the ACM SACMAT 10 Year Test of Time Awards for 2018 and 2019 (for papers published in 2008 and 2009). She co-chaired the Women in Cyber Security Conference (WiCyS) in 2016 and delivered the featured address at the 2018 Women in Data Science (WiDS) at Stanford University and has chaired several conferences for ACM and IEEE. Her 39-year career includes industry (Honeywell), federal research laboratory (MITRE), US government (NSF) and US Academia. Her work has resulted in 130+ journal articles, 300+ conference papers, 140+ keynote and featured addresses, six US patents, fifteen books as well as technology transfer of the research to commercial and operational systems. She received her PhD from the University of Wales, Swansea, UK, and the prestigious earned higher doctorate (D. Eng) from the University of Bristol, UK.