My Research on Applying Mathematical Logic and Mathematics to Cyber Security and Data Science (1980 – 2020)

Bhavani Thuraisingham

October 17, 2020

After my education in the United Kingdom, I have had a 40 year career in the United States including in the commercial industry (Honeywell), the MITRE Corporation (a federal research lab), the National Science Foundation (US Government) and in academia. My educational background is in Mathematics and Physics (B.Sc), Mathematical Logic (M.Sc.) and the Theory of Computation (Ph.D) and I have applied my Mathematical Logic and Mathematics expertise in areas such as cyber security and data science.

My early work between 1980 and 1985 was on the study of decision problems in Recursion Theory and Complexity Theory. My research also included work in Algorithmic Information Theory. This research was published in top tier journals such as the Journal of Computer and Systems Sciences, Notre Dame Journal of Formal Logic and the Mathematical Logic Quarterly (as a sole author). Subsequently, in 1985, I started working in cyber security and data science (what used to be called computer security and data management). Throughout the mid to late 1980s I conducted research on applying mathematical logic for database security including developing formal models. Subsequently together with the team (**Patricia Dwyer, Paul Stachour et al**) we pioneered techniques for the design of one of the early secure database systems based on formal models and type enforcement. This work was published in top tier journals and conferences including the IEEE Transactions on Knowledge and Data Engineering and Computes and Security. Subsequently our team (**Wei-Tek Tsai et al**) was the first to introduce security for object systems and this work was published in ACM OOPSLA and Computers and Security Journal. In addition, our team (**Wei-Tek Tsai et al**) also developed a formal execution model for dependable distributed systems and this work was published IEEE Transactions on Software Engineering.

My major breakthrough was in 1990 when I proved that the inference problem was unsolvable and presented the results at the IEEE Computer Security Foundations Workshop as well as at Rome Air Development Center's New Directions in Database Security Workshop. This work was quoted by NSA (National Security Agency) as a significant development in database security in 1990 (Proceedings of the1990 National Computer Security Conference https://personal.utdallas.edu/~bhavani.thuraisingham/1990_%20A_Year_of_Progress.pdf) by Dr. John Campbell. Then in 1991 I developed a logic called NTML, Non Monotonic Typed Multi-level Logic for secure data and knowledge base systems. This was the first effort on developing a theory for secure database systems and this work was also published in the Proceedings of the IEEE Computer Security Foundations Workshop in 1991 and 1992. I continued to apply mathematical logic to multiple secure database systems including models for object databases and distributed systems. I also applied deductive reasoning for the inference problem and subsequently designed and developed logic programming based systems for inference controllers. The research mentioned above in the early 1990s was carried out by me without any collaborators.

During the 1990s, together with the team (**Sang Son, John Maurer et al**), we were the first to integrate secure data management with real-time data management and this work was published in top tier venues including IEEE Transactions on Parallel and Distributed Systems and the IEEE Transactions on Knowledge and Data Engineering. At the same time our team (**Harvey**

Rubinovitz, William Ford, Marie Collins et al) also pioneered techniques based on fundamental principles for designing secure distributed distributed database systems and Database Inference Controllers and this work appeared in the Journal of Systems and Software, Data and Knowledge Engineering, and IEEE Transactions on Knowledge and Data Engineering. At the same time I was the first to introduce the notion of applying Artificial Intelligence models (e.g., semantic nets and conceptual graphs) to represent and reason about secure database applications and this work was published in the IFIP Database Security Conference.

From 2000 until around 2010, my research proceeded in three directions. One was to develop novel machine learning techniques based on statistical reasoning for solving challenging problems in cyber security, the second was to develop foundations and logic for a secure semantic web and the third was to explore the foundations of data privacy. With respect to machine learning, together with the team (**Latifur Khan, Jiawei Han et al**), we designed and developed machine learning algorithms based on statistical reasoning for detecting novel classes. This work has had a significant impact towards understanding the zero day attacks in cyber security and published in IEEE Transactions on Knowledge and Data Engineering.

With respect to secure semantic web research, I was the first to introduce security for semantic web at the NSF/EU workshop in Sophia Antipolis in 2001. Subsequently, together with the team (**Elisa Bertino et al**), we developed access control models for XML. This work was published in ACM Transactions on Privacy and Security and IEEE Transactions on Knowledge and Data Engineering. Later, together with the team (**Tim Finin, Anupam Joshi et al**), we also applied mathematical logic to develop formal models for a secure semantic web. Subsequently, together with the team (**Elena Ferrari et al**), we applied formal models for semantic web-based secure social networks. Our work was published in top tier venues such as the ACM Symposium on Access Control Models, Applications and Technologies (SACMAT), IEEE Conference on Data Mining and the Data and Knowledge Engineering Journal. In addition, our papers published at SACMAT in 2008 and 2009 received the ACM SACMAT 10 Year Test of Time Award in 2018 and 2019. Around the same time, together with the team (**I-Ling Yen et al**), we also developed formal models for securing web services and this research was published in IEEE Transactions on Services Computing.

In the area of data privacy, I was the first to point out the privacy violations that could occur due to data mining as early as 1996 and subsequently in 2002 I published a landmark paper while at the National Science Foundation in SIGKDD on Data Mining, Counter-Terrorism, Privacy and Civil Liberties which has been widely cited. Later, in mid 2000s, our team (**Murat Kantarcioglu et al**) was among the early researchers to design algorithms for privacy aware data mining that combines data mining with data privacy. This work was published in top tier venues such as the Data and Knowledge Engineering Journal. In 2010, I received the earned higher doctorate (D. ENG) at the University of Bristol for my research and published work in Secure Dependable Data Management between 1985 and 2010.

In the 2010s, while continuing with my research in data security, data mining, data privacy and semantic web, together with the team (**Murat Kantarcioglu et al**), our work also focused on adversarial machine learning that involved designing algorithms to handle attacks on the machine learning techniques. In this work, we applied game theoretical techniques to model the games between the defender and the attacker. This work was published in ACM Knowledge Discovery in Databases conference. In addition, together with the team, we also developed a theory for

assured information sharing as well as secure query processing and adapted the designs we subsequently developed to operate in the cloud. I worked with researchers at Kings College, London and at the University of Insubria, Italy (**Steve Barker, Barbara Carminati et al**) to design the first of its kind cloud-based assured information sharing system based on the theories we had developed. This effort was commended by the US Air Force https://www.wpafb.af.mil/News/Article-Display/Article/400150/afosr-funded-initiative-creates-more-secure-environment-for-cloud-computing/. Our team (**Latifur Khan et al**) also continued to develop novel data science techniques based on statistical reasoning and apply them to problems such as Insider Threat Detection. This work has been published in several top tier conferences and journals including the IEEE Conference on Data Mining and ACM Transactions on Management Information Systems. Around the same time (late 2000s, early 2010s), together with the team (**DZ Du, Weili Wu et al**), we also conducted research on applying graph theory for problems in network routing and rumor blocking in social networks. This research was published in journals such as Discrete Mathematics, Algorithms and Applications as well as the Journal of Combinatorial Optimization, My most recent work (late 2010s, early 2020s) together with researchers at Kings College, London (**Maribel Fernandez et al**) has focused on applying Mathematical Logic (e.g. rewriting systems) for formalizing the Internet of Things system. Our team was the first to carry out such research and this work has been published in top tier venues such as ACM CODASPY (Data and Applications Security and Privacy) and ACM SACMAT.

My work from theory to practice in cyber security and data science has resulted in me receiving many prestigious awards including the IEEE Computer Society's 1997 Technical Achievement Award, the ACM SIGSAC 2010 Outstanding Contributions Award, .ACM CODASPY 2017 Lasting Research Award, IEEE Services Computing 2017 Research Innovation Award and the IEEE Communications society's 2019 Technical Recognition Award. My research has also resulted in highly cited papers including over 130 journal articles, over 300 conference publications and several technology inventions and patents. I have also given over 170 keynote and featured addresses on my research at highly prestigious venues and have written 15 books in data management, data mining and data security. Finally, my work over the past 40 years ranging from Computing, Engineering, Science, Technology Innovation, and Mathematics has been recognized by a variety of prestigious organizations by being elected a Fellow of the ACM (2018), IEEE (2003), AAAS (2003), NAI (2018) and the British-based IMA (2020).