Paper ID	Paper Title	Authors
	Regular Papers	
627	SecureFixAgent: A Hybrid LLM Agent for Automated Python Static Vulnerability Repair	Jugal Gajjar (The George Washington University)*; Kamalasankari Subramaniakuppusamy (The George Washington University); Relsy Puthal (The George Washington University); Kaustik Ranaware (The George Washington University)
646	LLM2+: Contextual Prompt Whitelist Principles for Agentic LLMs	Tom Pawelek (Mississippi State University)*; Raj Patel (The University of Alabama); Charlotte Crowell (The University of Alabama); Noorbakhsh Amiri Golilarz (The University of Alabama); Sudip Mittal (The University of Alabama); Shahram Rahimi (The University of Alabama)
649	Detection of LLM Hallucinations Usine Late Internal Reoresentations	Sakhawat Hossan (University of North Carolina Greensboro)*; Jixe Dena (University of North Carolina Greensboro)
650	Breaking and Securing Vision-Language Models: An Adversarial Robustness Study	Md Zarif Hossain (Florida Atlantic University); Abdur R. Shahid (Southern Illinois University Carbondale); Ahmed Imteaj (Florida Atlantic University)*
675	Improving Robustness of Large Language Models Used in Healthcare Through Prompt Engineering	Jonathan O'Berry (University of North Florida)*; Indika Kahanda (University of North Florida); Upulee Kanewala (University of North Florida)
687	Jailbreaking Large Vision Language Models in Intelligent Transportation Systems	Badhan Chandra Das (Florida International University)*; Md Tasnim Jawad (Florida International University); Md Jueal Mia (Florida International University); M. Hadi Amini (Florida International University); Yanzhao Wu (Florida International University)