Join us for a session on

AI Cybersecurity

January 19, 2026, 7 am PST

Live Stream Seattle Washington USA

A Quantum Computational Framework for Satellite Video Image Encryption: Design, Analysis, State-of-Art Comparison & Benchmarking

Quantum computing is a revolutionary field of computing that leverages the principles of quantum mechanics to process information in fundamentally different ways compared to classical computing. For encryption processes quantum computing enhances the security and efficiency of cryptographic protocols. One prominent technique is Quantum Key Distribution (QKD), which uses the quantum properties of particles, such as superposition and entanglement, to securely distribute cryptographic keys between parties. In today's world, where drones play a major role in military warfare and domestic surveillance a third

Register at: https://www.mytechconference.com/event-details/cybersecurity-in-the-ai-era-challenges-threats-and-trust

Mike Brisbois, PE | 708.668.5488 | mike.brisbois@ieee.org

party activities, there is a need for transmission of secured video images without any intrusion by Any intrusion by an adversary should easily be detected in real-time and the compromised information should be virtually impossible to decipher. Our work proposed a new method of encryption of video images using quantum key distribution and visual cryptographic technique. The key agreement process was done using quantum key distribution and the generated key was be used by the proposed encryption algorithm. The Performance measurement parameters for our models are Peak Signal-to-Noise Ratio (PSNR), measures the quality of the decrypted image by comparing it with the original image. Higher PSNR indicates better quality. Structural Similarity Index (SSIM) evaluates the similarity between the original and decrypted images in terms of luminance, contrast, and structure. SSIM values range from - 1 to 1, with 1 indicating perfect similarity, Mean Squared Error (MSE) measures the average squared difference between the original and decrypted images. Lower MSE indicates higher quality.

Dr. Sabyasachi Bhattacharyya

Dr. Sabyasachi Bhattacharyya is an Assistant Professor in the Department of Electronics and Telecommunication Engineering, Barak Valley Engineering College, Sribhumi, Govt. of Assam, India and he is presently deputed to serve at the Department of Electronics and Telecommunication Engineering, Residential Girls' Polytechnic, Golaghat, Govt. Of Assam. Dr. Bhattacharyya obtained his B.Tech degree (with University Gold Medal) in Electronics and Communication Engineering from School of Technology, Assam Don Bosco Univeristy, Guwahati, Assam in 2013, his MTech degree (with First Class, First Position) in Signal Processing and Communication from Gauhati University, Guwahati, Assam in 2016 and his Ph.D degree in Electronics and Communication Engineering (with specialization in Wireless Communications) from Indian Institute of Information Technology Guwahati (IIITG) in 2023. Dr. Bhattacharyya is also presently pursuing his Post Doctoral Research in Physical Layer Cybersecurity for Satellite/Space Networks as a part of his collaboration with two senior professors from University of South Florida, USA and Gauhati University, India. His research areas and interests include Digital Phased Locked Loops, DPLL based Wireless Communications, 5G Millimeter wave communication systems and channel models, 5G/ Next Generation channel modeling and transceiver design, security and computational techniques for 6G/future networks. Dr. Bhattacharyya has a number of publications in different reputed SCI/Scopus indexed journals and in various IEEE and other esteemed conferences. He is actively associated with various reputed journals (as reviewer and other similar positions) which include the IEEE Systems Journal, IEEE Letters on Wireless Communications, IEEE Transactions on Broadcasting etc. Also, Dr. Bhattacharyya is associated as TPC/Organizing Committee Member of various IEEE and other reputed international conferences including the IEEE ComSoc Annual Wireless Telecommunications Symposium (WTS) organized by the California Polytechnic State University (Cal Poly), Pomona, USA. He delivered as an Invited Speaker at the esteemed IEEE Smart Cities Session, Washington DC organized by IEEE CN

Seattle Section and co-sponsored by the IEEE Power and Energy Society during November 2024. Moreover, he has also served as a Keynote Speaker at the IEEE Silchar Sub-section sponsored One Week National Level Webinar on Science and Technology Awareness (S&T-2021) organized by NIT, Silchar during November 2021. He has also served as Invited Speaker/Session Chair for various esteemed conferences and events including the IEEE CAS sponsored 13th International Conference on Computing, Communication and Sensor Network (CCSN), Kolkata, India held during September 2024 and ASIACOMNET 2024 organized by IEEE Thailand Section and IEEE Computer Society Thailand Section.

Unlocking the Black Box: Building Transparent and Ethical AI with Explainability

This presentation will explore explainable artificial intelligence (XAI), addressing critical ethical challenges such as algorithmic bias and discrimination, illustrated with real-world examples from healthcare and defense. It will clarify the distinction between interpretability and explainability and discuss ante-hoc and post-hoc techniques for transforming "black-box" systems into transparent, regulation-compliant AI aligned with frameworks like the GDPR. By promoting human-centered AI, the talk highlights strategies for building more inclusive, trustworthy, and responsible technologies for the future.

Dr. Imen Jdey

Dr. Imen Jdey is an Associate Professor of Computer Science at the Faculty of Economics and Management of Sfax (FSEGS), University of Sfax. Her research focuses on artificial intelligence, including deep learning, computer vision, and decision support systems, with a particular emphasis on model explainability and medical applications. She has contributed to international projects such as "RAQMYAT" and "REMEDIA" and has held academic and administrative roles, including department head and research center director, fostering interdisciplinary AI research and innovation.

Cybersecurity in the AI Era: Challenges, Threats, and Trust

Cybersecurity in the AI Era: Challenges, Threats, and Trust examine the security implications of deploying artificial intelligence in modern digital infrastructures. The talk focuses on the dual role of AI as both a defensive tool and an attack vector, highlighting AI-driven threat detection, automated incident response, and the increasing use of generative and adversarial techniques by attackers. It addresses security vulnerabilities in machine learning systems, including adversarial examples, data poisoning, model extraction, and prompt injection, and discusses defense strategies such as robust training, explainable AI, and secure ML pipelines. The session also explores Zero Trust architecture as a foundational security model for cloud-native, distributed, and AI-enabled environments, emphasizing continuous authentication, least-privilege access, and behavior-based risk assessment to establish trust in intelligent systems.

Dr. Jonti Deuri

Dr. Jonti Deuri holds a Ph.D. in Computer Science and Engineering and currently serves as Head of the Department and Assistant Professor at the Faculty of Engineering and Technology, Sharda University, Uzbekistan. Her research interests include Artificial Intelligence, Cybersecurity, Secure Machine Learning, Soft Computing, and Network Security, with a strong focus on bio-inspired optimization and AI-driven security systems. She has authored and co-authored numerous research papers in Scopus- and IEEE-indexed journals and conferences, including IEEE international conferences, and has contributed book chapters published by Springer, Wiley, CRC Press (Taylor & Francis), IGI Global, and Cambridge Scholars Publishing. Dr. Deuri is a UGC-NET-qualified researcher, recipient of the Rajiv Gandhi National Fellowship, and holds international patents in AI-enabled systems. She actively contributes to interdisciplinary research and regularly serves as an invited speaker and resource person on advanced topics in AI, cybersecurity, and emerging technologies.

The AI Arms Race: The New Era of Social Engineering and Defense

Tanusree Chatterjee

As artificial intelligence evolves, the greatest security threat is no longer just malicious code, but the perfect manipulation of human trust. The talk explores how hackers are now using "Generative AI" to clone voices and faces with terrifying accuracy, turning a simple 30-second video into a tool for multi-million-dollar fraud. We will dive into the "Forger vs. Detective" battle happening inside these AI systems, uncover why traditional passwords and voice IDs are becoming obsolete, and demonstrate how we can use "Defensive AI" as a digital immune system to spot these deceptions before they strike.

Dr. Tanusree Chatterjee is an Associate Professor in the department of Computer Science & Engineering, Future Institute of Technology, under Future Education Group, Kolkata, West Bengal, India. She completed her master's in computer science & engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India and accomplished her Ph.D. in the field of Wireless Sensor Network, Information Centric Networking from Indian Institute of Engineering Science & Technology, Shibpur, West Bengal, India. She has more than 16 years of teaching experience in reputed engineering colleges of West Bengal, India and 12 years of research experience. She has published more than 20 research papers in international journals, referred conference proceedings, and book chapters. She edited multiple book chapters with renowned publishers and has multiple patents and copyrights to her credit. Her current research interests include Information Centric Networking, Internet of Things, Machine Learning, Artificial Intelligence and Prompt Engineering.

Register at: https://www.mytechconference.com/event-details/cybersecurity-in-the-ai-era-challenges-threats-and-trust