Presenter Name: Venkata Nedunoori

Talk Title: Advancements in Homomorphic Encryption for Secure Data Processing

Presenter Short Bio: I am Venkata Nedunoori, a seasoned technology leader with expertise in cloud security. I am currently working as an Associate Director at Dentsu International. I lead the design and implementation of advanced cloud-based solutions. My expertise lies in architecting and delivering scalable, secure, and cost-efficient platforms that empower organizations to thrive in today's fast-paced digital era. As the technology landscape continues to evolve, I am passionate about the intersection of cloud security and artificial intelligence and am eager to explore new opportunities to fortify digital landscapes. As a Cybersecurity enthusiast, I possess deep knowledge across multiple domains of Cloud Security, including Application Security, Information Security, Network Security, Risk Assessment and Management, and Compliance with Regulatory Standards. I hold a Master's degree in Information Technology Management from The University of Texas at Dallas, where I developed a strong foundation in both technical skills and strategic thinking. As an engaged Senior Member of IEEE, I am dedicated to keeping pace with the latest advancements in software engineering and cybersecurity. Additionally, as a member of OWASP, I focus on both contributing to and staying informed about the forefront of web security innovations.

Short Talk Abstract: Homomorphic encryption (HE) is a transformative cryptographic technology that enables computations on the encrypted form of data thereby ensuring privacy and security. This presentation explores the latest advancements in HE that have significantly enhanced its efficiency, security, and applicability. Recent algorithmic optimizations and hardware accelerations have reduced computational overhead, making HE more practical for real-world applications. Security improvements offer robust protection against emerging threats, including quantum attacks. The development of application-specific HE schemes has opened new avenues for secure data processing in cloud computing, healthcare, and machine learning. For instance, HE allows privacy-preserving data analysis in the cloud, secure patient data handling in healthcare, and the training of machine learning models on encrypted datasets. Despite these advancements, there are a few challenges with HE such as performance bottlenecks, integration complexities, and standardization that need further research to make HE more effective. This talk will provide a comprehensive overview of HE and its developments, illustrating how HE can revolutionize secure data processing by ensuring data privacy without compromising functionality. This presentation also shares insights into the future directions of HE research and its potential to address critical privacy concerns in various sectors.