Title: Identifying Potential Cyber Security Risks with Next Generation Sequencing Technology

Organizers

Dr Pushan Kumar Dutta, Assistant Professor, Department of ECE, School of Engineering and Technology, Amity University Kolkata, India

Dr Bharat Bhushan, Assistant Professor, Department of CSE, School of Engineering and Technology, Sharda University, Noida, India.

Dr Subrata Chowdhury, Associate Professor, Computer Science Engineering, Sreenivasa Institute of Technology and Management Studies: Chittoor, Andhra Pradesh, IN

Dr Denesh Sooriamoorthy, Lecturer, School of Engineering, Taylor University, Malaysia

Dr Pronaya Bhattacharya, Associate Professor, Department of CSE, School of Engineering and Technology, Amity University Kolkata, India

Introduction

Next-generation sequencing (NGS) technology has revolutionized various fields such as genomics, personalized medicine, and microbiology. However, the rapid development of this technology has also introduced new cyber security risks that could jeopardize the privacy and integrity of sensitive data. This special session aims to highlight these vulnerabilities and discuss the technical aspects related to the context, research scope, and tracks for addressing cyber security risks associated with NGS technology.

Research Scope:

The research scope of this special session includes, but is not limited to, the following topics:

1. Identifying and assessing cyber security vulnerabilities in NGS technology and related software tools.

2. Developing robust security measures and protocols for sample preparation, sequencing, and bioinformatics analysis.

3. Investigating the risks associated with the integration of NGS technology into home-based diagnostics and field applications.

4. Evaluating the impact of cyber attacks on NGS data integrity and potential implications on public health and personalized medicine.

5. Analyzing the role of synthetic DNA storage systems in mitigating cyber security risks associated with NGS technology.

Tracks:

Track 1: Cyber Security Vulnerabilities in NGS Technology

- Identification of vulnerabilities and attack vectors in NGS workflows.

- Assessment of potential threats and their impact on data privacy and integrity.

- Review of current security measures and recommendations for improvements.

Track 2 Security Measures for NGS Workflows

- Design and implementation of security protocols for sample preparation, sequencing, and bioinformatics analysis.

- Integration of security measures into NGS hardware and software tools.

- Strategies for securing NGS data storage, sharing, and archival.

Track 3: NGS Technology in Home-based and Field Applications

- Exploration of risks associated with NGS technology integration into non-laboratory settings.

- Development of security guidelines for home-based and field applications of NGS technology.

- Assessment of potential consequences of cyber attacks on NGS data in these settings.

Track 4: Impact of Cyber Attacks on N Data Integrity and Public Health

- Evaluation of the potential consequences of data breaches on public health and personalized medicine.

- Strategies for mitigating the impact of cyber attacks on NGS data integrity.

- Case studies of successful and unsuccessful cyber attacks on NGS technology.

Track 5: Synthetic DNA Storage Systems and Cyber Security

- Analysis of the role of synthetic DNA storage systems in mitigating cyber security risks associated with NGS technology.

- Techniques for encoding digital data in synthetic DNA strands with enhanced security features.

- Comparison of synthetic DNA storage systems with traditional data storage methods in terms of security and vulnerability.

By participating in this special session, researchers, practitioners, and stakeholders in the field of NGS technology and cyber security will have the opportunity to share their insights, knowledge, and experiences in addressing the potential cyber security risks associated with this rapidly advancing technology. The goal is to develop a comprehensive understanding of these risks and to propose effective strategies for mitigating them, thus ensuring the safe and secure application of NGS technology for the benefit of society.