Cyberbiosecurity Vulnerability Assessment and Resilience

Jappreet S. Gill and Dr. Sandeep Singhal

Department of Biomedical Engineering, School of Electrical Engineering and Computer Science,
Department of Pathology, School of Medicine and Health Sciences, University of North Dakota

Introduction

- A genome is an organism's complete set of DNA. A human genome is uniquely arranged to provide fundamental anatomy and individual characteristics.
- Genomic data science is rapidly moving towards digitization. Scientists utilize software tools and apps to sequence, synthesize, analyze, publish, and store genetic data in shared datastores.

- Although, such software tools and applications are often built to advance scientific understanding, cybersecurity is mostly neglected. However, given the increasing commercialization of genomic technologies and the sensitivity of data, there is a need to implement and maintain security around biomedical data.

- Cyberbiosecurity identifies and reduces security risks to life sciences, information sciences, and agriculture.
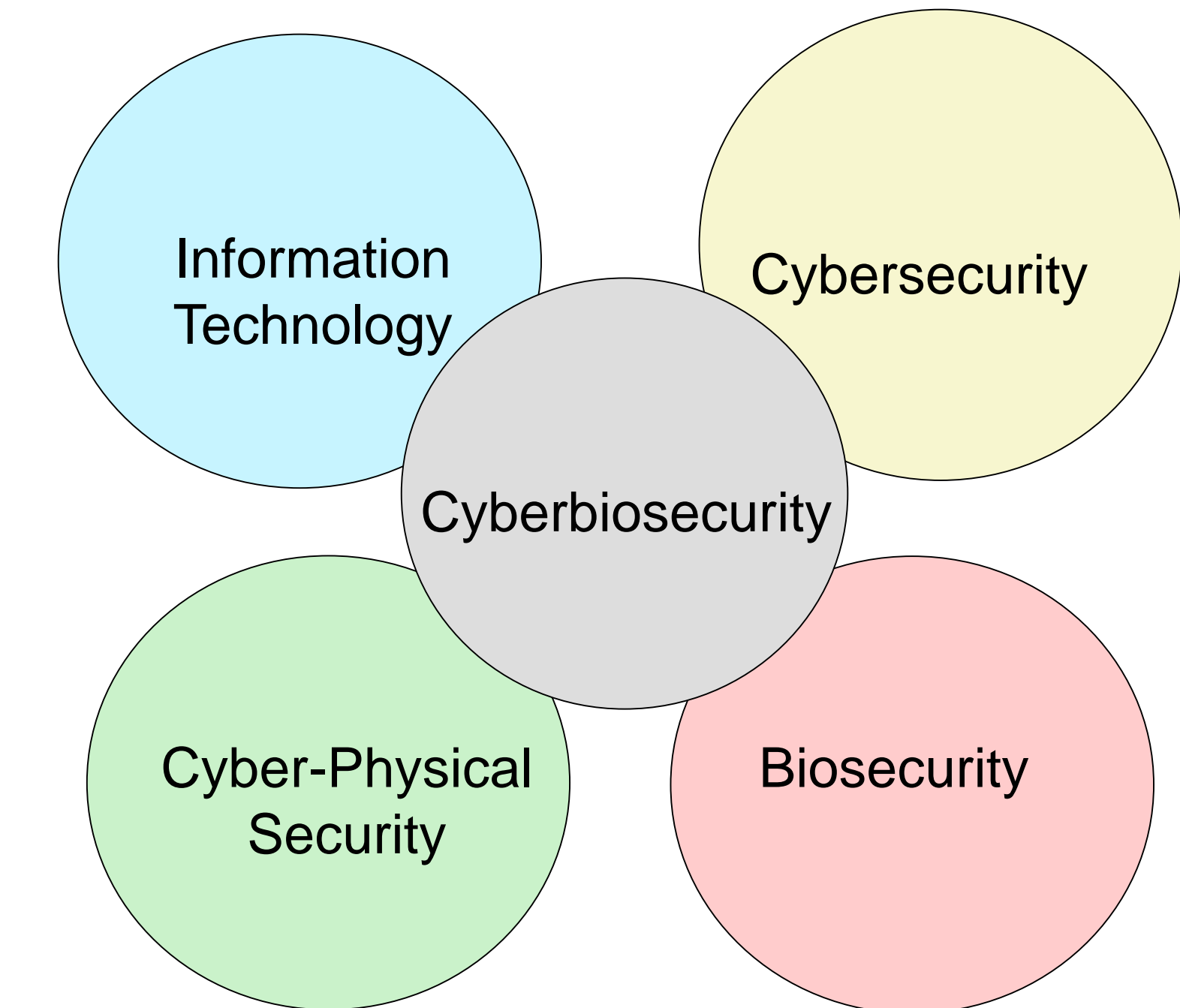
- Determining the cyberbiosecurity vulnerabilities and resilience can help forge a flexible and defensive approach to mitigate risks both economically and effectively. We will explore the common vulnerabilities present in the field of genomic data science and map these vulnerabilities to potential security risks which would aid to develop an assessment framework to mitigate cyber-attacks.
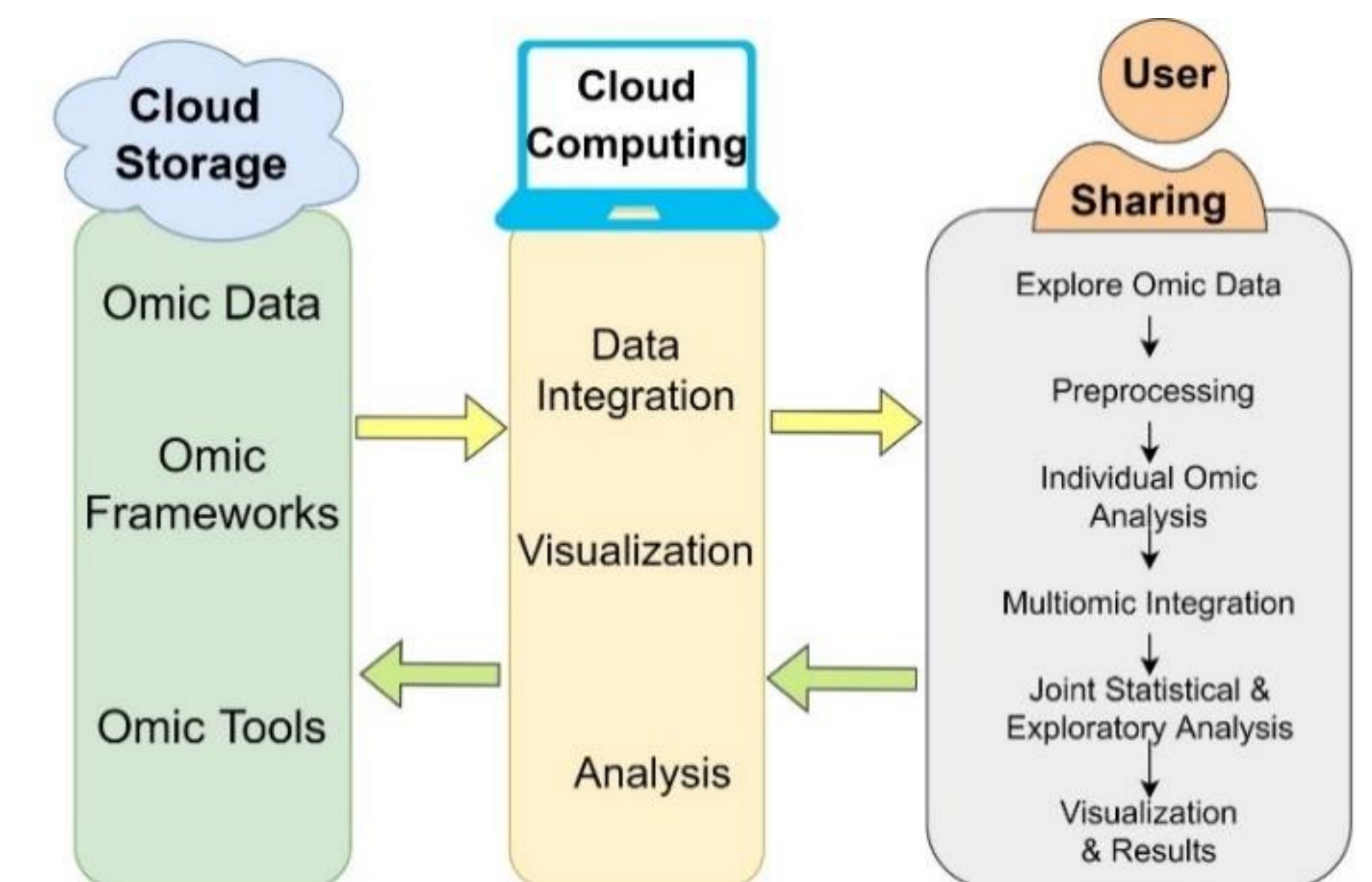
Need for Cyberbiosecurity

Insufficient cyberbiosecurity risk-mitigation techniques and lack of worldwide standards.

Amount of publicly accessible sequencing data available in data repositories with minimal cyber-security protection.

Ignorance of the fact how fast genomic data science is moving towards digitization and the security risks associated with it.

Lack of awareness about potential depictions of new threats and risks to patient and public health.

Potential of attack to corrupt genetic analysis technologies and data with high camouflage potential.

Attack on biological systems and software with direct patient impact through production of drugs and discovery of biomarkers.

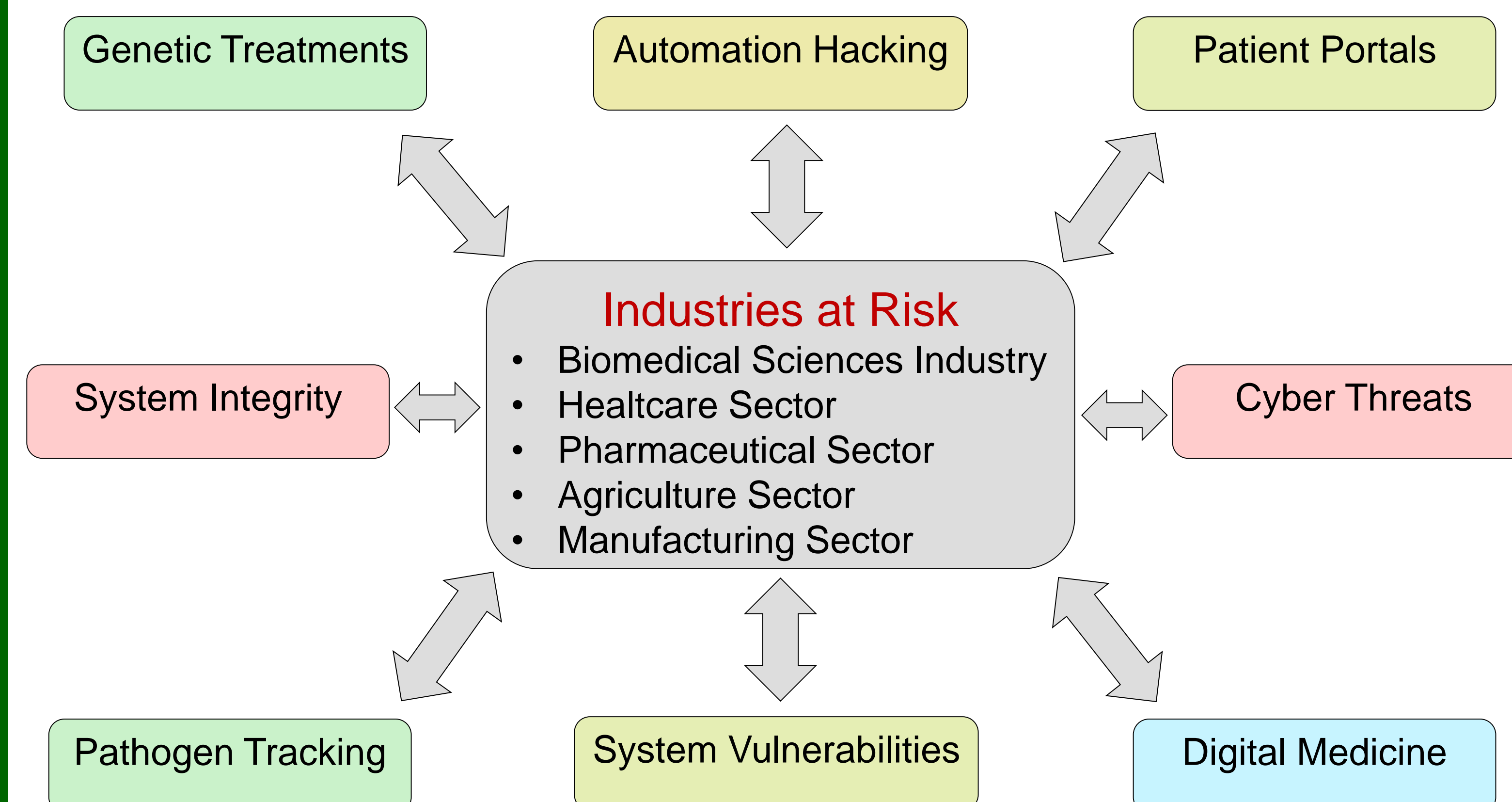## Cyberbiosecurity Vulnerabilities

Genetic Treatments · Automation Hacking · Patient Portals · System Integrity · Cyber Threats · Pathogen Tracking · System Vulnerabilities · Digital Medicine

Industries at Risk
- Biomedical Sciences Industry
- Healtcare Sector
- Pharmaceutical Sector
- Agriculture Sector
- Manufacturing Sector

Cyberbiosecurity Domains

Information Technology · Cybersecurity · Cyberbiosecurity · Cyber-Physical Security · Biosecurity

Threat to Cloud-based Genomic Technologies

Cloud Storage — Omic Data, Omic Frameworks, Omic Tools

Cloud Computing — Data Integration, Visualization, Analysis

User Sharing — Explore Omic Data → Preprocessing → Individual Omic Analysis → Multiomic Integration → Joint Statistical & Exploratory Analysis → Visualization & Results

References

- Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?. *Biosafety and health*, 3(01), 11-21.

- Srivastava, A., & Ahmad, S. (2022, June). Bio-Computing Based Algorithms for Cloud Security: A Critical Review. In *2022 IEEE World Conference on Applied Intelligence and Computing (AIC)* (pp. 894-900). IEEE.

- Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: a call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology*, 7, 99.

- https://projects.iq.harvard.edu/sciencepolicy/blog/next-generation-forensics-changing-role-dna-plays-justice-system