Cyber Infrastructure for emerging computing technologies: A new global perspective

Gurdeep S Hura

Professor

Department of Mathematics and Computer Science,

University of Maryland Eastern Shore, Princess Anne, MD, USA

410 651 6426

gshura@umes.edu

 Cyber Infrastructure is one of the most challenging topics the world Internet community is facing as more and more applications are being introduced over the Internet for global communications. The knowledge of various topics dealing with Cyber infrastructure needs the formation of an Information Assurance Curriculum and needed research that can be considered by the students of multi-disciplinary majors. The lack of information assurance system faculty, curriculum and facilities has left students behind as the world moves to produce a workforce capable of addressing these emerging needs.

 The Internet grew rapidly as a general-purpose enabling infrastructure, upon which controls had to be superimposed in an ad hoc manner.  Advanced knowledge infrastructure, by contrast, is human-centered and optimized for particular resources and communities.  *Cyber infrastructure* offers a vision of advanced knowledge infrastructure for research and education that integrates diverse resources across barriers of geography and time – and across the subtle and complex barriers of discipline, community, sector, and jurisdiction.  Because it aspires to provide human-centered access to diversely controlled resources, cyber infrastructure must be open and sensitive to institutional, legal, and cultural context, especially mechanisms and procedures for collaborative research and innovation.  This is critical not only for optimizing the productivity of particular research communities and initiatives but in developing public policy for advancing knowledge and innovation in an IT-enabled world.

 Cybercrime is a global phenomenon and educational and research efforts needs to be carried out collaboratively with a number of countries. This issue has also impacted the new integrated technologies of cloud computing, big data and social networking. We will briefly introduce these technologies, their benefits, applications, problems, and how each of these technologies will be affected by cyber infrastructure. The goals of this presentation is to present various aspects needed to be aware of the establishing the cyber infrastructure such as cyber-attacks, incident response methodology, cyber-ethics, and other related cyber entities. Hands-on experience will be demonstrated for some of the network forensics tools.