Call for Papers

Special Issue on Security and Privacy for IoT-assisted Technology Frameworks

The Internet of Things (IoT)-based applications are changing our surroundings very rapidly. These applications nearly impact every aspect of our modern life. The number of IoT-based smart gadgets is supposed to exceed dozens of billions till 2025. However, the insecure and open channel in IoT-based environment leads to critical security and privacy problems. An adversary could take advantage of these exposed network vulnerabilities. In this scenario, vigorous authentication protocols must be developed to fix the security problems. The bulk data production of the IoT-based system requires sophisticated solutions beyond cloud computing. The new technologies such as edge computing (EC) and fog computing largely shared the burden of cloud computing. Yet, the EC nodes suffered from security problems due to limited computational resources. Meanwhile many blockchain and Artificial Intelligence based security solutions were also presented to promote reliability and detection of malicious intrusions in the system. In this scenario more focus is needed on securing edge and fog computing models, as well as AI and blockchain-based solutions to enhance the viability of IoT environment.

The topics of interest for this special issue include, but are not limited to:

1. Artificial intelligence- based security and privacy enhancement for IoT-based systems
2. Blockchain based security enhancement IoT networks
3. Edge and fog computing-based security protocols for IoT systems
4. Trust assurance protocols for self-sustainable IoT and wireless systems
5. Security provisioning for industrial IoT (IIoT) systems
6. Security and privacy issues in Internet of medical things (IoMT)
7. Security issues for IoT assisted Unmanned Aerial Vehicle (UAVs)
8. Security enhancement for IoT led transport and vehicular systems

Submission Procedure: Papers should be formatted according to the Researchpedia Journal of Computing guidelines for authors and manuscripts. Submission should be submitted electronically through the email with Special issue name in the title.

Important Dates:
30 March 2022: Submission deadline
31 May 2022: Notification of first round of reviews
30 June 2022: Revised submissions due
31 July 2022: Final notice of acceptance/rejection
30 August 2022: Publishing date

Guest Editors:

- Dr. Shehzad Ashraf Chaudhry

Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey
sashraf@gelisim.edu.tr
https://scholar.google.com/citations?user=rtwXvjkAAAAJ&hl=en

- Dr. Azeem Irshad
  Faculty of computer Science, Asghar Mall College Rawalpindi, HED, Punjab, Pakistan
  azeemirshad@gpgcam.edu.pk
  https://scholar.google.com/citations?user=17pm_0EAAAAJ&hl=en

- Dr. Anwar Ghani
  Department of computer science and software engineering, International Islamic University Islamabad, Pakistan
  anwar.ghani@iiu.edu.pk
  https://scholar.google.com/citations?user=sFG2eMYAAAAJ&hl=en

- Dr. Hussein Abulkasim
  Cybersecurity Research Lab, School of Information Technology Management Ryerson University, Toronto, Canada.
  abulkasim@ryerson.ca

- Dr. Yousaf bin Zakaria
  Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, South Korea
  yousafbinzikria@ynu.ac.kr
  https://scholar.google.com/citations?user=K90qMyMAAAAJ&hl=en