**Cybersecurity for E-Business, E-Services, and E-Society (CEEE)**

Intelligent technology has advanced so swiftly over the last few decades, impacting nearly all aspects of human life. technological innovations are already transforming the way we learn, buy, sell, grow, socialize, entertain, and manage our health. Advances in automation, Artificial Intelligence, Virtual Reality, synthetic intelligence, robotics, quantum computing, and other emerging technologies are anticipated to dominate the next generation of technological developments. So far, e-business, e-service, and e-society have been increasingly adopting electronics and the internet for various activities like business transactions, marketing, telecommunication purposes, and a lot more. Further, information and communication technology has changed various public and government services as e-services including e-commerce, banking, healthcare, education, finance, and others. Therefore, the entire society has gradually started relying on technology and cyber-physical systems.

However, technology and the humongous opportunities haves also brought various challenges like security and privacy, in particular. Since the E-Business focuses on the transmission of assets or data, selling or purchasing of merchandise, and is solely based on electronic appliances and the internet, it provides vulnerabilities for cyberattacks and threats. As the remote working and business exchanges occur between business-to-business, business-to-customer, and customer-to-business, it has increased various issues such as Distributed Denial of Services (DDoS), malware, phishing, spyware threats, hackers, active malicious threats, data thefts, exploitation of known vulnerabilities, SQL injection, bots, and a lot more. With that, e-services of industry and others face diverse issues like eavesdropping, data breaches, data thefts, hacking, defacing of websites, spyware, and security holes, and other major security concerns, which impact the critical industry’s services. Moreover, the fast-changing technological society undoubtedly strengthens people’s time, networking, and building communities and equally encountering security threats. Therefore, enhancing cyber-security is essential for all e-business, e-services, and e-society sectors as these not only causes disruption in these areas but also result in loss of revenue, information, and overall viability for these fields. Hence, embracing innovative digital technologies such as big data analytics, blockchain, Artificial Intelligence, and others plays a prominent role in ensuring cybersecurity in business and society. Furthermore, detecting or understanding the new-age cyber-risks deploying next-generation identity and access control, and adopt robust cybersecurity management. In addition, leveraging new technologies and emerging trends for tackling critical cybersecurity risks may enhance the resiliency and robustness of digital services, organizations, and e-society. In this context, this special issue intends to explore the challenges of cybersecurity for e-business, e-services, and e-society. We invite researchers, practitioners, and scholars from technology, business, and societal disciplines to present novel and innovative solutions for this special issue.

**The topics of interest include the following, but are not limited to:**

* Innovative trends for e-service, e-society, and cybersecurity
* Role of technology for e-business, e-service, and e-society: opportunities and challenges
* Emerging cybersecurity threats and risks in e-commerce
* Cybersecurity and e-business: risks, issues, threats, and challenges
* Cybersecurity solutions for sustainable business management
* Digital security and cyber safety for e-society in the digital era
* Blockchain and AI for cyber security infrastructure in business
* Cybercrime impact in e-governance: innovative solutions and strategies
* Future of cybersecurity management in e-businesses and e-governance
* Security and privacy in e-health sectors
* Innovative ways of building secure digital society: cyberattacks, threats, and risks
* Cybersecurity for financial networks: challenges and threats
* Innovative trends for secure e-infrastructure in critical industries
* Privacy and security challenges in e-society platforms

**Guest Editor and Team:**

**Dr. Ahmad Abdallah Althunibat (MGE)**

Department of Software Engineering,

Faculty of Science and Information Technology,

Al-Zaytoonah University of Jordan, Amman, Jordan

Email Address: [a.thunibat@zuj.edu.jo](mailto:a.thunibat@zuj.edu.jo), [drahmadthunibat@gmail.com](mailto:drahmadthunibat@gmail.com)

Scholar Page: <https://scholar.google.com.my/citations?user=8Vu2g9sAAAAJ&hl=en>

**Dr. Abeer Alsadoon (CO-GE)**

Dean of Scholarship and Research

Kent Institute Australia, Sydney, Australia

Email Address: [abeer.alsadoon@kent.edu.au](mailto:abeer.alsadoon@kent.edu.au)

Scholar Page: <https://scholar.google.com/citations?user=ouKzqC8AAAAJ&hl=en>

**Dr. Ibrahim Abood Eid Almarashdeh (CO-GE)**

College of Applied Studies and Community Service,

Management Information Systems,

Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Email Address: [iaalmarashdeh@iau.edu.sa](mailto:iaalmarashdeh@iau.edu.sa)

Scholar Page: <https://scholar.google.com/citations?user=pmUtI30AAAAJ&hl=en>

|  |  |  |  |
| --- | --- | --- | --- |
| **Important Dates** | | | |
| Submission  Deadline | Author  Notification | Revision  Submission | Final  Decision |
| **30.07.2023** | **05.10.2023** | **10.12.2023** | **15.02.2024** |