Call for Papers
Special issue on
Secure Communications
Journal of Communications Software and Systems (JCOMSS)

Secure communication for is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate. We invite high-quality research papers and review articles addressing communication quality, security policy, and privacy protection across all kinds of sensor networks.

The aim of this special issue (SI) is focused on communications mediated or intercepted by technology. Trusted Computing also is an approach under present development that achieves security in general at the potential cost of compelling obligatory trust in corporate and government. Authors wishing to submit papers for this SI should register and submit the article (PDF format) in the corresponding SI track by using the OJS system **https://jcomss.fesb.unist.hr/**.

Guest Editors Team:

1. **Rajesh Manoharan**, Professor, Dept. of Computer Science and Engineering, Vandavasi, India., Email: rajesh@ragaacademics.in
2. **Natarajan Prasad**, Asso. Professor, Dept. of Computer Science and Engineering, Addis Ababa University, Addis Ababa, Ethiopia., Email: natrajanethiopia@gmail.com
3. **Toni Perković**, University of Split, Croatia, toperkov@fesb.hr

Topics include, but not limited to, researches and developments in the field of Smart Cities:
- Hiding the content or nature of a communication
- Code – a rule to convert a piece of information
- Encryption
- Identity Based
- Steganography covers a broad spectrum of techniques, which include, among others:
- Digital Image Steganography
- Digital Video Steganography
- Steganalysis
- Hiding the parties to a communication – preventing identification, promoting anonymity
- Crowds and similar anonymous group structures
- Anonymous communication devices – unregistered cell phones, Internet cafes
- Anonymous proxies
- Hard to trace routing methods – through unauthorized third-party systems, or relays
- Hiding the fact that a communication takes place
- Security by obscurity – similar to needle in a haystack

IMPORTANT DATES	
Submission deadline	September 15, 2019
Notification of acceptance	November 25, 2019
Final manuscript due	December 20, 2019
Published	Jan 2020

Journal of Communications Software and Systems (JCOMSS) is the peer reviewed **open access journal** offering to authors the quick promotion of the published articles, since the whole research community can freely access the valuable scientific information. The accepted papers are electronically published at the journal website shortly after acceptance. JCOMSS is an all electronic processing journal, published quarterly, offering typically **2 months window** for final decision about publishing for well prepared regular papers that are accepted after one round of review.
JCOMSS is indexed in Scopus, EBSCO, Inspec, Google Scholar, CrossRef and DOAJ.