FGCS Special Issue on Key Management and Key Distribution for Secure Group Communication in Mobile and Cloud Network

Overview

One of the widely well-known methods of middleware is Group Communication Systems (GCSs). Reliable and secured point-to-point and multicast messaging services are supported in a GCS used in mobile and cloud networks. In such networks, the processes will dynamically join and leave a group during communication. Group membership is dynamic, as group membership changes over time, and frequent notification messages are exchanged among group members consistently.

Such reliable and authenticated group communication is facilitated through secure keys. Such key generation primitives must be managed and distributed appropriately for secure group communication especially in mobile and cloud networks. The process of generating, distributing and maintaining the cryptographic keys is taken care by key management schemes. The key management schemes that are available in the literature are used to support secure multicast communication. There are several algorithms developed in the past to support such group communication. However, there are many technical challenges that arise with the rapid development of these new technologies. The key challenges identified with most of the existing works are with respect to computation and communication complexity.

Efficient techniques that could address these challenges will be suitable for mobile and cloud networks. Moreover, people are exchanging much useful information to a group of users in mobile as a message or voice. This must be protected using a secure group communication scheme which is possible by developing new efficient key management schemes. In cloud also, the data is shared to a group of users using multicast communication to minimize the bandwidth.

Therefore, this proposal purely focuses on developing new key distribution and key management protocols for supporting multicast communication in mobile and cloud networks. The key management is generally divided into distributed and centralized key management schemes. In this special issue, we will focus on latest advances in research from both academia and industrialists on the topic of secure group communication in key management and key distribution protocols.

Topics of Interest

- Secure Key exchange for multiparty communication in mobile
- Key management and key distribution for secure multicast communication in mobile
- Gesture based Authentication and secure key distribution for mobile
- Anonymous authenticated key management for mobile
- Secure Key exchange for multiparty communication in cloud
- Cryptanalytic Attacks and solution for key distribution in cloud

- Trust Establishment and Key Management for cloud network
- Multicast security in cloud
- Key management for data access control in public cloud
- Key management for ensuring data deduplication in cloud
- Cryptographic Key Management Challenges in the Cloud
- Key Distribution and Key Management for Wireless Sensor Networks (WSNs)
- Key distribution issues on mobile cloud network

Important Dates:

Tentative schedule

Submission deadline: April 05, 2017

Pre-screening notification: April 25, 2017

First round notification: June 28, 2017

Revision due: August 16, 2017

Final notification: September 16, 2017

Final Manuscript due: October 16, 2017

Tentative publication date: January - February 2018

Instructions for Manuscripts:

Papers will be evaluated based on their originality, presentation, relevance and contributions, as well as their suitability to the special issue. The submitted papers must be written in excellent English and

describe original research that has not been published nor currently under review by other venues. Previously published conference papers should be clearly identified by the authors at the submission stage and an explanation should be provided about how such papers have been extended to be considered for this special issue. Extended conference contributions must have at least 50% difference from the original works (the authors must indicate the conference name and make a reference to the base conference paper). Guest editors will make an initial determination on the suitability and scope of all submissions. Papers that either lack originality, clarity in presentation or fall outside the scope of the special issue will not be sent for review and the authors will be promptly informed in such cases.

The submitted papers will be reviewed by at least three independent reviewers. Final decisions on accepted papers will be based on their qualities and their relevance to the theme of this special issue and should be approved by the journal editors.

Main Guest Editor

Dr. P. Vijayakumar,

Dean,

University College of Engineering Tindivanam,

Tindivanam,

India- 604 001.

Mail: vijibond2000@aucet.in, vijibond2000@gmail.com

Guest Editors

Dr.Victor Chang,

Associate Professor,

International Business School Suzhou, Xi'an Jiaotong Liverpool University, Suzhou, China- 215123

Email: ic.victor.chang@gmail.com, Victor.Chang@xjtlu.edu.cn

Dr. L. Jegatha Deborah,

Assistant Professor & Head i/c,

Department of Computer Science and Engineering,

University College of Engineering Tindivanam,

Tindivanam.

India- 604 001.

Mail: blessedjeny@aucet.in, blessedjeny@gmail.com

Dr.Bharat S. Rawal Kshatriya

Assistant Professor ,

IST Faculty,

Penn State University,

Abington, Pennsylvania 19001.

Email:bsr17@psu.edu