DOI 10.12694/scpe.v18i3.1299
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 18, Number 3, pp. iii–iv. http://www.scpe.org

INTRODUCTION TO THE SPECIAL ISSUE ON SECURE SOLUTIONS FOR NETWORK IN SCALABLE COMPUTING

This special issue aimed at incarceration of new insights, dimensions, visionaries and accomplishments achievable for security. Security is a foremost concern in scalable computing. With the progression in ICT (Information and Communication Technologies), secure solutions are the need; as the number and kinds of attacks too are progressive. Keeping this in mind, the papers selected for this issue talks about all our visualizations from the same. In todays Internet-connected world, the advance cyber-attacks are being launched on the critical infrastructure. It has shifted the pursuit of financial profit and political gains, which lead to cyber warfare on various scales. The first paper points that malware is one of the most alarming security threats being faced by the Internet today. They have the capability to circumvent the earlier developed methods of detection and mitigation which clearly shows the need of shifting from traditional cyber security to cyber threat intelligence. Authors have proposed the design of a framework for generating malware threat intelligence which has the capability to detect, analyze, and predict the malware threats and can act as an Early Warning System (EWS). The second paper talks about the current status of sentiment analysis and opinion mining focusing on the problem of sarcasm identification and detection. The article discusses the present scenario and the problem faced by the community due to the usage of sarcasm. Authors have tried a technique based on the deep convolution neural networks where they are using a single layer convolution before the classification task and claim to have higher accuracy in the classification of sarcasm as compared to existing methods.

The third paper talks about Wireless sensor networks (WSNs) that are widely used in various fields such as health monitoring, medical line, intrusion detection, and are often placed in open environment, thus vulnerable to different attacks. Various techniques were introduced to deal with security related issues of WSNs; among them trust management has been proved as an effective measure. A new protocol called Energy Efficient and Trust Aware framework for secure routing in LEACH (EETA-LEACH) has been proposed. A trust management system for WSNs has been presented to monitor the sensor nodes behaviors and evaluate their trust values based upon remaining energy, packet delivery ratio and distance. This approach is a combination of trust-based routing module and trust management module that works together to select trusted Cluster Head (CH). Simulation results have proved that proposed algorithm consumes less energy and improves packet delivery ratio.

Almost all the important services are available in the application market of Android. Unfortunately, at the same time, the prosperity of these applications also attracts abusers and malicious attackers to perform different types of attacks. The fourth paper is an exploration and all-inclusive study about various approaches to perform Android applications analysis. This gives improved identification of the problem, accessible elucidation space and possible research scope to evaluate Android devices against the possible attacks.

The fifth paper focused on the dynamics of worm propagation in the Wireless Sensor Networks (WSNs). Authors proposed a modified Susceptible-Infectious-Quarantined-Recovered-Susceptible (SIQRS) model based on epidemic theory and demonstrated the effect of quarantined state on worm propagation. This paper also describes the Stability of the worm free equilibrium and Endemic equilibrium, as well as, studies the effect of communication radius and node density.

Kavita Sharma, NIT, Kurukshetra, India
Suman Bala, Orange Labs, Meylan, France
Himani Bansal, JIIT, Noida, India
Gulshan Shrivastava, NITP, India