Journal of Computing and Security

January 2014, Volume 1, Number 1 (pp. 1–2)

http://www.jcomsec.org

Editorial Note

I am delighted to introduce this first issue of *Journal of Computing and Security (JCS)*, a joint effort between the Faculty of Computer Engineering and Information Technology at the University of Isfahan, and Iranian Society of Cryptology with active participation of distinct individual faculties from Isfahan University of Technology. Recent technical advances and enormous rise of the number of scientists in the world, especially in many developing countries - as a result of their vast development of graduate studies - and the need for sharing their fine and original research works, motivated us to introduce this journal to publish significant and internationally notable achievements in the aforementioned fields of studies from all over the world. This forum allows them to get published in a journal that is committed to excellence and quality.

JCS attempts to be an "open access" publication, and would provide up-to-date, high-quality, and original contributions in the form of research papers, as well as high standards forum for advancement of scientific knowledge on the field. In many respects, this first issue of the journal exemplifies this approach.

JCS is served by a competent editorial board along with a network of scholars helping to attain high-quality and originality of the contributions and, in so doing, the impact of the work published in the journal. I am thrilled and fortunate to be working with this talented group of board members; and am thankful to all of them for their exceptional efforts. Likewise, I am grateful of many contributors and authors who trusted this journal and sent their articles for possible publication. While limitations in space and scope meant that not all contributions could be passed on to print, those that do appear demonstrate the wealth of the subject matter deeply.

On behalf of the editorial board, I present six outstanding articles in this very first issue, three in information security and three in modern computing. The first paper proposes a "trust-based approach for correctness verification of query results in data outsourcing." Their approach is modeled using a transition system. In this article, through Linear Temporal Logic, Noferesti et al. proposed a verification method for the correctness properties of query results.

The second article is written by Mala who presented "a unified byte permutation design for the block cipher 3D" for both odd and even rounds with the same diffusion property as the original cipher. This new transformation promises to offer cipher's hardware implementation with fewer resources which results into speedy encryption/decryption processes.

The third article offers an "efficient end-to-end key establishment protocol for wireless sensor networks." Fanian et al used several symmetric polynomials to generate polynomial shares for a group of sensors, in a wireless network. Then a combinatorial design is offered for distribution of the shares to each sensor. This allows generating common key between sensors without imposing significant overhead, according to the authors.

In the fourth paper, Alimoradi et. al. studied the effect of correlogram properties on blind steganalysis in JPEG images. They showed that when homogeneity increases, the false image detection of blind steganalysis increases; and when contrast and entropy decreases, error increases.

The author of the fifth paper, Adibi, proposed a "growing hierarchical approach to batch linear manifold topographic map formation" to remove the limitations that relate to their "fixed topology and fixed number of representation elements or neurons." The author applied this method to two real-world problems to show the effectiveness of his approach.

The sixth and last paper in this issue is written by Shabanian et. al. who offered an optimal traffic distribution

method that distributes the input traffic over possible paths for each session while keeps the average end-to-end path delay for individual paths below a required bound. They showed that their algorithm converges and also minimizes the total average delay of all packets in a network.

I look forward to share our first issue and to promote the potential of research connections that all of us at *JCS* rush to keep up with this new journal. Please plan to submit your cutting edge research articles to *JCS*; and consequently ensure that your manuscripts reach the knowledgeable readership that they deserve. All paper submissions are much appreciated and will make a substantial contribution to the advancement and growth of the journal. If you are unsure about the fittingness of your work to *JCS* or have any other questions concerning the journal, please do not hesitate to make a contact.

Best wishes and thank you in advance for your contributions!

Ahmad Reza Naghsh-Nilchi, PhD
Editor-in-Chief
Journal of Computing and Security