Guest Editorial Preface

Special Issue on Intelligent Informatics and Computing for Security

Vikrant Bhateja, Department of Electronics and Communication Engineering, Shri Ramswaroop Memorial Group of Professional Colleges, Lucknow, India

Musheer Ahmad, Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi, India

Suresh Chandra Satapathy, Department of Computer Science Engineering, PVP Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

Security has always been an indispensable means of secure communication. Today's technologically progressed era demands to assure confidentiality, integrity, authenticity and availability of user's secret information. The modern-day security system should be able to mitigate the malicious and other types of possible security threats. The aim of this special issue is to bring closer the ideas of researchers, academicians, scientists, and scholars applying hybrid, multidisciplinary and contemporary concepts for the design of effective and advanced solutions to cope with the recent modern challenges in the areas of information security. This special issue would be beneficial for academicians, scholars, application developers, industry professionals, and experts as well as researchers working in any of the area of security.

Our goal through this special issue is to focus upon the recent advancements in the techniques relating hybrid concepts, latest informatics, computational intelligence for fulfilling the requirements and challenges in the broad development area of security and allied domains. The scope is to acquire understanding and usefulness of most later intelligent informatics and computing applied for building robust and effective security systems.

In this regard, the first paper of this special issue "Detection of automobile insurance fraud using feature selection and data mining techniques" talks about fraud detection in automobile insurance claims. It is achieved by applying various data mining techniques. The authors choose the most relevant attributes from the original dataset using evolutionary algorithm based feature selection method. A test set is then extracted from the selected attribute set and the remaining dataset is subjected to the Possibilistic Fuzzy C-Means (PFCM) clustering technique for under-sampling approach. The 10-fold cross-validation method is then used on the balanced dataset for training and validating a group of weighted extreme learning machine (WELM) classifiers generated from various combinations of its parameters. The efficacy of proposed system is obtained by conducting several experiments on a real world automobile insurance defraud dataset. Besides, a comparative analysis with another approach justifies the superiority of the proposed system.

The second paper "Secure mechanisms for key shares in cloud computing" suggested the algorithm and technique for protection of key in cloud computing scenarios. The algorithm to select the number of virtual machines is presented to protect the key. The existing key management algorithm is modified to address the key leakage issue. The novel techniques such as validation of key shares and key share re-sharing are introduced and analyzed for protection of the key. These techniques make the attackers incompetence to reconstruct the key. Further, for immediate access of protected resource, key reconstruction for key sizes of cryptography algorithm is also analyzed.

Another paper in sequence, titled: "Reversible data hiding scheme for ECG signal" discusses about authentication of ECG signals in tele-medicine system. In telemedicine, remote electrocardiography (ECG) monitoring systems are widely used to examine the cardiac health of a patient. ECG data is collected in real time and send over the network along with patient's identity to his/her doctor who is geographically away. In that scenario, it is very important to protect patient's confidential information. To serve the purpose, the authors, developed a novel reversible watermarking algorithm with high embedding capacity based on wavelet transform. The proposed reversible data hiding scheme allows ECG signals to hide its corresponding patient's confidential data and being reversible the original signal can be completely restored at the same time. Performance has been evaluated in terms of ECG signal distortion and embedding capacity.

The fourth in sequence portrays: "8-bit quantizer for chaotic generator with reduced hardware complexity" focuses on high speed processing hardware machine with reduced complexity meant for security of the data. In chaos-based pseudorandom keys, the generated chaotic values are analog in nature, these analog values are digitized to generate encryption key like 8-bit, 16-bit, 32-bit. To generate 8-bit key, 8-bit quantizer is required. The design of 8-bit quantizer requires 256 levels which needs lot of complex hardware to implement. In this paper, the authors, designed an 8-bit quantizer with reduced complexity where hardware requirement is reduced. To increase the randomness and confusion timed hop random selection is used. The randomness of the sequence generated by the chaotic generators is analyzed by NIST test suite, to test for its randomness.

Lastly, the concluding paper in sequence is entitled: "A rough set based ensemble framework from Intrusion detection system" addresses the issues of designing an effective network intrusion detection system which is becoming a difficult task as the sophistication of the attacks have been increasing. Machine Learning approaches have been proving beneficial in such situations. This paper proposes an ensemble framework based on rough sets to efficiently identify attacks in a multi-class scenario. The framework is validated on benchmark KDD Cup '99 and NSL_KDD network intrusion detection datasets as well as six other standard UCI datasets. The experimental results show that proposed technique RST achieved better detection rate with low false alarm rate compared to bagging and RSM.

Being guest editors, the team hopes that the spectrum of research works covered under this special issue will be of great value to many readers/researchers working in the domain of security using intelligent techniques. We are grateful to all authors for making their esteemed research contributions to this issue and their involvement during crucial review process. The technical standards and quality of published content is based on the strength and expertise of reviewers who have been involved in providing quality reviews for the submitted papers. Our special thanks are due to the Editor-in-Chief of the International Journal of Rough Sets and Data Analysis (IJRSDA), Dr. Nilanjan Dey (Techno India College of Technology, India) for his ample support, and competence rendered to this special issue.

Vikrant Bhateja
Musheer Ahmad
Suresh Chandra Satapathy
Guest Editors
IJRSDA