Guest Editorial Preface

Special Issue on Security and Privacy Issues in Cloud Computing, Big Data and IoT Technology:
Current Progress and Future Directions

Manu Vardhan, Department of Computer Science and Engineering, National Institute of Technology Raipur, Chhattisgarh, India

Malay Kumar, Department of Computer Science and Engineering, National Institute of Technology Raipur, Chhattisgarh, India

Cloud computing provides highly scalable, ubiquitous, and on-demand computing resources over networks, in a very economic pay-per-use model. Cloud computing is enabling the organizations to perform data analytics on very large datasets and in a wide variety of data speeds. Big Data and IoT influence the future development of cloud computing systems. In fact, future technology relies on the integration of Cloud Computing, Big Data and IoT, where applications are capturing data from IoT enabled devices and perform analytics on cloud data centers. Regardless of highly promising benefits, the outsourcing of data and computation to third-party servers bring multifarious security and privacy challenges to the cloud user and the cloud service provider.

This special issue provides knowledge about current research progress and future directions in Cloud Computing, Big Data and IoT security and privacy challenges and their promising solution.

The first article of this special issue presents a novel approach to aid the counter-terrorism and insurgency operations. The application tracks the suspicious vehicles based on their registration number, their type, color and RFID tag. Additionally, the application provides suspicious vehicle classification on the demand of security agencies.

The second article introduces an ensemble feature selection (EFS) technique, where multiple homogeneous feature selection (FS) methods are combined to choose the optimal subset of relevant and non-redundant features. Further, an intrusion detection system, named (SVM-IDS) is developed using the feature selected by the proposed method.

The third article presents spectral clustering and frequent term-based summarization techniques for security related posts on CQA sites. However, the fourth article proposes a secure communication proposal for data transmission as per the priority of message for IoT and wearable devices.

The fifth article proposes a protocol, which elects reliable CHs based on IoT node features such as residual energy, distance to the sink and node's behaviour such as the number of packets transmitted and received successfully, data consistency factor.

The sixth article also addresses an interesting aspect of Internet of Things (IoT). The article contributes: (1) A hierarchical topology for IoT network deployment; (2) symmetric matrix-based

pair-wise key generation for secure communication; (3) A secure and energy efficient secure routing algorithm for the proposed model.

The last article of this special issue includes an interesting work on twitter data sentiment analysis. The proposed work leverages the meta-heuristic clustering method for sentiment mining for the large-scale Twitter dataset.

The work included in this special issue adds value to the current state-of-the-art and open wide opportunities for future research in the contemporary areas including cloud computing, IoT and big-data.

Manu Vardhan
Malay Kumar
IJISP
Guest Editors