Guest Editorial Preface

Special Issue of "The Impacts of Security, Privacy and Trust on IoT"

Rashmi Agrawal, Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies, India
D. Ganesh Gopal, School of Computing Science and Engineering, Galgotias University, Greater Noida, India
R. Lakshmana Kumar, Department of Computer Applications, Hindusthan College of Engineering and Technology, India

The Internet of Things (IoT) that comprises combined cyber and physical objects has the inherent capability and embedded technologies to collect, sense and communicate. IoT has been widely accepted across many fields and will continue to be ubiquitous in the increasingly digital world. As the technology grows thick and fast, the number of connected devices involved are increasing at an unprecedented growth. Indeed, it is estimated that IoT networks will consist of nearly 30 billion objects by 2020.

The requirement for the hefty scale arrangement of IoT like smart cities, smart healthcare smart parking etc. naturally brings security as a huge concern for IoT deployment. More specifically, in the distributed, pervasive and dynamic environments, securing IoT devices presents a tremendous challenge. Every individual device and sensor connected to IoT networks are vulnerable from adversarial attacks. At the same time, computational processing of security protocols and management traditionally requires a lot of processing power, context awareness and reliability. It is expected that data in large quantity can be generated over time by various IoT devices. The processing and distribution of such data over shared networks lead to serious privacy and security concerns, including information confidentiality, authentication and authorisation, etc. Moreover, by the openness and comprehensive infrastructure of IoT, widely distributed devices can be compromised by a large variety of malicious parties. Therefore, trust among devices in the network is concerning and trust management becomes a crucial factor when it comes to the users' information exchange and data of confidentiality.

The papers received in this special issue have concentrated on all aspects and future research directions related to this specific area of IoT Security, Privacy & Trust towards building the reliable and secure systems design and analysis along with the usages of all computing technologies which includes; Big Data, Data Science, Machine Learning, AI and Deep Learning.

This special issue of the International Journal of Knowledge and Systems Science (IJKSS) had received 9 papers. After going through 6 months of review process with several levels of blind review finally 5 papers have been selected for publication.

The first paper that was selected with the title "SDN Based Secure Architecture for IoT" written by the authors Dr. Shailendra Mishra. The main aim of this paper is to bring the first impression of the term Internet of Things (IoT) means connecting things through the internet. The growing market for IoT also attracts malicious individuals trying to gain access to the marketplace. Security issues are among the biggest worries in companies that rely on the cloud of things to do business. SDN Based Architecture have improved the security of IoT network. The centralized controller in SDN manages the network and controls the data flow in the network elements. Controllers in SDN based architecture are still facing security challenges such as unauthorized access, configuration issues, distributed denial of service (DDoS) attacks, and a man in the middle (MITM) attacks. The attack

scenario and security of SDN based IoT networks are evaluated in this research. The simulation result shows that the proposed approach and security solutions are fast and effective in mitigating the attacks.

The second paper selected was titled "QoE-based Multi-Criteria Decision Making for Resource Provisioning in Fog Computing using AHP Technique" written by Ms. Shefali Varshney, Dr. Rajinder Sandhu, Dr. P.K. Gupta. This paper focuses on the Application placement in the Fog environment as it is becoming one of the major challenges because of its distributed, hierarchical, and heterogeneous nature. Also, user expectations and various features of IoT devices further increase the complexity of the problem for the placement of applications in the Fog computing environment. Therefore, to improve the QoE of various end-users for the use of various system services, proper placement of applications in the Fog computing environment plays an important role. In this paper, the authors have proposed a service placement methodology for the Fog computing environment. For a better selection of application services AHP technique has been used which provides results in the form of ranks. The performance evaluation of the proposed technique has been done by using a customized testbed that considers the parameters like CPU cycle, storage, maximum latency, processing speed, and network bandwidth. Experimental results obtained for the proposed methodology improved the efficiency of the Fog network.

The third paper was "Role of Educational Data Mining in students' Learning Process With Sentiment Analysis" written by the authors Mrs. Amala Jayanthi M, Dr. Elizabeth Shanthi. The manuscript is on Educational data mining which is a research field that is used to enhance education system. Research studies using educational data mining are in increase because of the knowledge acquired for decision making to enhance the education process by the information retrieved by machine learning processes. Sentiment analysis is one of the most involved research fields of data mining in natural language processing, web mining, and text mining. It plays a vital role in many areas such as management sciences and social sciences, including Education. In Education Investigating students' opinion, emotions using techniques of sentiment analysis can understand the students' feelings that students experience in academics, personal and societal environment. This investigation with sentiment analysis helps the academicians and other stakeholders to understand their motive on Education is online.This article intends to explore different theories on Education, students' learning process, and to study different approaches of sentiment analysis academics.

The fourth paper that was selected is "Secure Key Storage and Access Delegation through Cloud Storage" written by the authors Mrs. Bharati Mishra, Prof. Debasish Jena, Mr. Ramasubbareddy Somula, Dr. S Sankar. The paper brings the IoT as an emerging concept in the field of information and technology. In this article IoT based patient health monitoring is considered using IoT sensors deployed in devices. IoT devices are vulnerable to many routing attacks such as Blackhole, Grey-hole and Sybil attacks. Sybil attack is the most dangerous attack, which steals the identities of legitimate nodes; this in turn leads to information loss, misinterpretation in the network and maximizes the routing disturbances. Hence, in this paper we propose traditional Caesar Cipher Algorithm (CCA) along with Lightweight Encryption Algorithm (LEA), Received Signal Strength Indicator (RSSI) to detect and prevent Sybil attack in IoT environment. This algorithm detects the false node in the particular path by announcing the attack to another node. And also prevents the attack by choosing the alternative path to forward data packets to desired users. To ensure authentication, privacy and data integrity, Light weight encryption algorithm with 64-bit key is used with AODV as routing protocol.

The final fifth paper entitled "Optimal Elliptic Curve Cryptography Based Effective Approach for Secure Data Storage in Clouds" written by the authors Dr. Anju malik, Dr. Mayank Aggarwal, Dr. Bharti Sharma. Dr. Akansha Singh, Dr. Krishna Kant Singh. In this paper, a technique for secure cloud storage is proposed. Initially, the user sends a file storage request to store a file in a cloud service provider (CSP). The input file is checked whether it is sensitive or non-sensitive by the user. If the file is sensitive then it would be split and stored in different Virtual Machines (VMs) and if the file is non-sensitive then it would be assigned in a single VM. This approach was used for the first time as per our survey. To add further security the sensitive data retrieval needs an encryption process that

is supported by our proposed algorithm. If the data owner stores sensitive data to the cloud server, the data owner's document is encrypted by our double encryption technique. Here RSA and Optimal Elliptic Curve Cryptography (OECC) algorithm are used to encrypt the document with high security. We have used the cuckoo search algorithm to identify the optimal key in ECC. A novel cryptography approach for delivering mass distributed storage by which the user's original data cannot be directly reached by cloud operators.

After a rigorous review we have finalized 5 articles that were suitable and were ready to be within the scope of the special issue. Since this is a special issue, we didn't accommodate any papers that were away from the scope of the theme and after further scrutinizing and several levels of blind review this has been done. Hope this special issue will gather more citation and improve the impact factor of the journal. We greet the editor in chief and manager publications for giving us an opportunity to do a special issue and further we expect to do more special issue with them. Thank You.

Rashmi Agrawal
D. Ganesh Gopal
R. Lakshmana Kumar
Guest Editors
IJKSS