

---

## Preface

---

### Ganesh Gopal Deverajan\*

Department of Computer Science and Engineering,  
SRM Institute of Science and Technology,  
Delhi-NCR Campus, Ghaziabad,  
Uttar Pradesh, 201204, India  
Email: dganeshgopal@gmail.com  
\*Corresponding author

### Rashmi Agrawal

Department of Computer Science and Engineering,  
Manav Rachna International University,  
Sector 43, Delhi-Surajkund Road,  
Faridabad, 121004, Haryana, India  
Email: drrashmiagrawal78@gmail.com

**Biographical notes:** Ganesh Gopal Deverajan is currently working as a Professor and Research Coordinator in the Department of Computer Science and Engineering, SRM Institute of Science and Technology, Delhi-NCR Campus, India. As part of his professional career, he has around 40+ publications in international journals and conferences. He has successfully completed several special issues by serving as a guest editor for many reputed journals. He is the Editor-in-Chief for book series, *Advances in Cyber Security* for Wiley – Scrivener. He has contributed his ideas and shared his research experience as a technical program committee (TPC) member, program committee member and session chair member in premium international conferences.

Rashmi Agrawal is a PhD working as a Professor and Head of Department in the Department of Computer Applications, Manav Rachna International Institute of Research and Studies, Faridabad, India. She is a Life Member of the Computer Society of India and Senior Member of IEEE, and chapter chair and professional member of ACM. She is a book series editor of many series with reputed publishers like Wiley and CRC Press. She has authored/co-authored 80+ research papers in peer reviewed national/international journals and conferences which are SCI/SCIE/ESCI/SCOPUS indexed. Her research area includes machine learning, deep learning, artificial intelligence, educational data mining and sentiment analysis.

---

IoT grows massively in all strengths due to its usage and easy adoption for various fields. As of late, the collection, processing, and analysis of individual information have become necessary and easy since the advancement of emerging applications like IoT. Since IoT provides ubiquitous service on heterogeneity of networks naturally it becomes vulnerable. Despite the fact that edge computing, fog computing has an incredible strength to uplift the networking, resource utilisation security and privacy concerns are more. The threats exist because. Also, the threats were involved at different layers of IoT.

So, detection of threat and providing insightful security system a solution is the primary aim of this special issue. Blockchain is an upcoming and promising technique to solve the aforesaid problems. Blockchain can provide intelligent secure solutions layer wise security for IoT. Also, it can build the trust on the IoT system for users.

After a careful and meticulous blind review process, we have finalised five papers for this special issue of the *International Journal of Electronic Business (IJEBS)*. The first paper titled 'Security framework for IoT and deep belief network-based healthcare system using blockchain technology' authored by Senthil Murugan Nagarajan, Prathik Anandhan, V. Muthukumaran, K. Uma and U. Kumaran. This paper presented a healthcare system to provide a secure and reliability of data transmission. Furthermore, IoT-based wearable devices are used to collect the data from the patients. Moreover, deep belief network (DBN) is proposed to classify the obtained data in order to predict the type of disease or problems for patients. The experimental results shows that the proposed framework and classification model abruptly outperforms when compared with other existing techniques. The efficiency of the proposed framework is analysed based on the performance metrics like throughput and latency. The loss ratio for the proposed model seems obtain very less of 0.0126 when compared with other existing techniques like MLP, SVM, ANN and CNN. The accuracy obtained for the proposed DBN classifier is above 95% for the increase in the number of patients.

The second paper titled 'RPL enhancement with mobility-aware two-stage objective function for improving network lifetime in IoT' authored by Robin Cyriac and M.A. Saleem Durai. This paper presents two stage objective function (TS-OF) for improving network lifetime in IoT. In the first stage, a simple objective function (OF) that considers ETX and path delay and rank parents as per RPL specification. A fixed number of best ranked parents from the first stage OF are considered for further processing in the second stage OF. Fuzzy-based second stage OF considers mobility history, queue availability and remaining energy of the parents to select the preferred route. Second stage OF is run only on limited number of parents which improves performance of RPL. Performance evaluation shows that our TS-OF reduces packet loss by 28% and energy consumption by 34% compared to the state-of-the-art RPL OF.

The third paper titled 'A Markov decision process-based secure consensus framework for leveraging blockchain technology in IoT applications' authored by Nonita Sharma, Monika Mangla and Sachi Nandan Mohanty. This paper proposed a secure consensus framework that implements Markov decision process (MDP) for blockchain technology in IoT applications. The proposed framework presents projection for the sojourn time and stationary efficiency measures for any transaction or block. Implementing MDPs provides a group of states and a collection of actions to choose from. MDP also offers instantaneous reward purpose and a probabilistic transition matrix. The proposed framework that suggests implementation of MDP in blockchain technology further escalates the security of the network. The paper demonstrates the architecture of the proposed framework.

The fourth paper titled 'Blockchain-based consensus algorithm for solving security issues in distributed internet of things' authored by Bhabendu Kumar Mohanta, Kalpana Samal, Debasish Jena, Somula Ramasubbareddy and Marimuthu Karupiah. This paper presents different security and privacy challenges which were identified in an IoT application. Secondly, analysis regarding blockchain technology is done which gives the idea to solve some of the IoT security challenges. Blockchain-based consensus algorithm PBFT is used to perform secure computation in a smart transportation system.

Security analysis shows that the proposed protocol worked correctly in presence of malicious or faulty nodes.

The fifth paper titled ‘Modified handshake protocol-based secure authentication using blockchain technology in WLAN’ authored by Manoj Diwakar, Prabhishek Singh and Achyut Shankar. The paper presents a brief description of the wireless networks, their advantages over wired networks and security issues requiring immediate attention. It is then followed with blockchain feature integrated with 802.11 architecture and various services offered by it and then than the motivation for conducting the research. Thereafter, a problem statement outlining the inherent flaws in the present IEEE 802.11i standard is presented. Hence a method is proposed to overcome the denial of service using modified three way handshaking approach. Finally, results are discussed and concluded.

As the guest editors of this special issue, we were extremely thankful to the editor and journal manager of *International Journal of Electronic Business (IJE)* for their valuable support.