# Preface

## Naveen Chilamkurti

Department of Computer Science and IT,
La Trobe Cybersecurity Research Hub,
La Trobe University,
Melbourne, 3086, Australia
Email: n.chilamkurti@latrobe.edu.au

## Ganesh Gopal Deverajan*

Department of Computer Science and Engineering,
UIET,
Chandigarh University,
Mohali, Punjab, 140413, India
Email: dganeshgopal@gmail.com
*Corresponding author

## Lakshmana Kumar Ramasamy

Centre of Excellence for Artificial Intelligence and Machine Learning,
Hindusthan College of Engineering and Technology,
Valley Campus, Pollachi Highway, Othakkalmandapam,
Coimbatore, 641-032, Tamil Nadu, India
Email: drlakshman@ieee.org

**Biographical notes:** Naveen Chilamkurti is a Professor and Head of Cybersecurity Discipline in the La Trobe University, Melbourne, VIC, Australia. He obtained his PhD from the La Trobe University, in 2005. He is also the inaugural Editor-in-Chief for *International Journal of Wireless Networks and Broadband Technologies* launched in July 2011. He has published over 320 journal and conference papers. He has edited and authored nine books with various publishers. He has been an associate editor for various IEEE journals and also a guest editor for various high impact international journals. Since 2010, he contributed to 80 special issues in various international journals, including the IEEE and Elsevier journals. His current research areas include cybersecurity, IoT, anomaly detection in IoT, internet of medical things, wireless security, federated learning in IoT, wireless multimedia, wireless sensor networks, and so on.

Ganesh Gopal Deverajan is currently working as a Professor and Vertical Head for Artificial Intelligence and Machine Learning in Department of Computer Science and Engineering, Chandigarh University, India. He has published around 40+ publications in international journals and conferences. He has successfully completed the special issues by serving as a guest editor for 28 reputed journals. He is an Editor-In-Chief for the book series, *Advances in Cyber Security* for Wiley-Scrivener. His research interest includes artificial intelligence, internet of things (IoT), wireless communication and blockchain. He has received from VIT University a research award as a top performer for three consecutive years, 2015, 2016 and 2017.

Lakshmana Kumar Ramasamy is working as the Head – Center of Excellence for Artificial Intelligence and Machine Learning at Hindusthan College of Engineering and Technology, Tamil Nadu, India. He is currently pursuing his post-doctoral fellowship at Thu Dau Mot University, Vietnam. He represents the Technical Group Committee-National Cyber Defence Research Centre (NCDRC), Government of India. He is a member in IEEE, ACM distinguished speaker and IEEE Brand Ambassador. He himself involves in research and expertise in AI and blockchain technologies. As part of his professional career, he has around 19 patents, 40+ publications and eight edited book from various renowned publishers.

According to many research studies, including the Gartner analysis, there will be about 21 billion connected internet of things (IoT) devices by the year 2020. IoT is built upon the premise of connectivity as it uses automation and smart technology so that devices can communicate between themselves. With regard to communication, privacy is the largest challenge for this connected ecosystem. Many IoT security issues are raised because of how much personal data the devices and systems collect and transmit. Each device that is connected increases privacy and security concerns surrounding the IoT. IoT network security is more challenging than traditional network security because there is a wider range of communication protocols, standards and device capabilities, all of which pose significant issues and increased complexity.

When it comes to IoT encryption, encrypting data at rest and in transit between IoT edge devices and back-end systems uses standard cryptographic algorithms, which helps in maintaining data integrity and preventing data sniffing by hackers. Collecting, aggregating, monitoring and normalising data from IoT devices and providing actionable reporting and alerting on request are starting to incorporate sophisticated machine learning, artificial intelligence and big data techniques to provide more predictive modelling and anomaly detection, but these capabilities are still emerging. There is a lot of positive hype, but IoT security issues are not to be taken lightly, especially in healthcare – possibly one of the most private and sensitive areas of our lives, which can reap benefits and create risks. The healthcare industry will need preventative security measures built into its IoT systems to begin with. Overall, the security concerns that have been raised with IoT must be considered by both individuals and companies moving forward.

IoT technologies are still immature to a large extent, and being little paranoid about their security is indeed helpful. All these factors could prove to be an inhibiting factor in encryption and other robust security measures. With the enormous amount of data, IoT devices generate and communicate back to the cloud for analysis, it would be unwise to assume that all systems can scale to accommodate the bandwidth, power, storage and computing ability needed to handle this load.

After a careful and meticulous blind review process, we have finalised nine papers for this special issue of the *International Journal of Internet Technology and Secured Transactions* (*IJTST*).

The first paper titled ‘Security and detection mechanism in IoT-based cloud computing using hybrid approach’ authored by Megha Vashishtha, Pradeep Chouksey, Dharmendra Singh Rajput, Somula Ramasubba Reddy, M. Praveen Kumar Reddy, G. Thippa Reddy and Harshita Patel. This paper presented a secure environment of IoT-based cloud computing. This approach used and enhanced Rivest cipher (RC6)

method along with blowfish algorithm. The combination of RSA and RC4 is accepted for the generation of key to get the superior security method, on image, Blowfish algorithm is applied. In this method, initially cloud provider registers the cloud user which authenticates the user, then text and image data can be uploaded in the existing four servers. The uploaded data can be viewed directly by the self-verified account without any constraint, but if those files are demanded by the other cloud users, then data classification encryption standard have been applied. The textual data is practiced with the enhanced RC6 method with key processing method of RC4 and RSA algorithm. These keys are used for the data decryption from the further side. The TA gives the information of the mismatch in the last prefix of the combination of the user detail and the data. If it does not match, then the data will be corrupted by the blocker algorithm and no useful information has been visualised and any type of contravention is traced at the admin side and the cloud user both. The whole parametric comparison implies that the performance of our framework is better in comparison to the traditional techniques.

The second paper titled 'An evolutionary-based technique to characterise an anomaly in internet of things networks' authored by Alok Kumar Shukla, Sanjeev Pippal, Deepak Singh and Somula Ramasubba Reddy. In this paper to understand different DDoS attacks activities, a teaching learning-based optimisation (TLBO) with learning algorithm is proposed which is then integrated to mitigate denial of service attacks. The approach is based on building an intrusion detection system to the requirements of the monitored environment, called TLBOIDS. Furthermore, TLBOIDS selects the most relevant features from original IDS dataset which can help to distinguish typical low-rate DDoS attacks with the use classifiers namely support vector machine and decision tree.

The third paper titled 'Robust and provable secure three-factor mutual authentication scheme using a smart card' authored by R. Niranchana and M. Amutha Prabakar. In this paper, a provable secure three-factor authentication scheme that makes use of smart card is been proposed. This authentication scheme is developed based on fundamental assumption of discrete logarithm problem and modular exponentiation. The formal and informal security analysis for the proposed scheme shows that the authentication scheme is more secure. The efficiency of this scheme is calculated based on the performance analysis for both computational and communication cost. It shows that the proposed authentication scheme is performing well, when compared to the related authentication schemes.

The fourth paper were 'An improved security approach for attack detection and mitigation over IoT networks using HACABO and Merkle signatures' authored by E.S. Phalguna Krishna and Thangavelu Arunkumar. The paper focuses on detection and prevention mechanism of IoT attacks. For that, an attack detection mechanism with hybrid ant colony African buffalo optimisation and hash-based Merkle signature-prevention mechanism is proposed. The paper also introduces economic DoS (E-DoS) shield mechanism using CloudWatch to prevent high rate DDoS attacks since the conventional approaches cannot prevent it. Also, the efficiency of the developed model is compared with recent works.

The fifth paper which is 'Digital application of analogue-like time perception mechanism based on analogue on digital theory' written by Ziran Fan and Takayuki Fujimoto. The proposed application represents the reality of time passing that is originally provided by analogue clocks. The interface design adopts the time representation of analogue clocks into the schedule display so that it can intuitively

indicates the lapse of time passing for each activity scheduled in a day. Moreover, we design the users' operational experience close to that of analogue tools by realising the real feel of using clocks through the representation of the spring-driven system on digital style.

The sixth paper titled 'An upgraded model of query expansion using inverse-term frequency with pertinent response for internet of things' written by Surbhi Sharma, Abhishek Kumar and Rashmi Agrawal. The objective of the paper is to search the query development strategy utilising reverse term recurrence to improve the proficiency and exactness of the data recovery framework and its accuracy in query processing, which leads to most recent trusted digitising trend IoT. As the technique for assessment of query development, we will expel irrelevant, excess and uncertain words from the recovered report dependent on client query. In proposed work, we present another technique for query expansion (QE) which depends on inverse term recurrence with importance criticism. Getting the top regenerated records and they are used as an importance criticism for extra QE terms and developing applicant terms. Procedure of scoring strategy appoints score to one of a kind terms and applying inverse-term frequency (ITF) to deliver the rank reduce of terms. These terms will channel through semantic activity and reweighting produce refreshed (extended) question which will again send to look through apparatus.

The seventh paper titled 'An architecture for enabling IoT interoperability between cross-platforms' authored by Venkateswara Raju Konduru and Manjula R. Bharamagoudra. The authors have identified two key perspectives critical to the development of an IoT ecosystem:

1 enable interoperability between platform development and cross-platform implementation of applications on Internet platforms

2 market (or trade centre) to exchange and adapt IoT resources.

Given these two important perspectives of an IoT ecosystem, this article introduces the bridging the interoperability gap (BIG) IoT architecture as the basis for the creation of IoT ecosystems. Architecture responds to key needs that have been evaluated by industry and research associations as a key aspect of the BIG IoT project. We present a proof of the application of the concept in the context of a smart healthcare scenario. We adopted the generic RESTful application programming interface (API) methodology to detect and interacts the smart object platforms.

The eighth paper titled 'An effective cloud-based smart home appliances automation in IoT using PHMM model' written by M.R. Sundarakumar, S. Sankar and S.R.S. Reddy. The main goal of the paper is to provide the automation for home appliances using IoT. Wireless sensor networks (WSN)-based home automation systems are very difficult to manage the devices using a centralised approach due to the mobility. To solve this issue, wireless home automation system (WHAS) is proposed, which uses the predictive hidden Morkov model (PHMM) to control the devices efficiently and conserves the energy utilisation among the devices. The status of the devices are monitored continuously and selecting the device operation either in manual mode or automatic mode using the PHMM model. The proposed approach conserves more energy than traditional methods.

The ninth paper titled 'Enhanced adaptive trust management system for socially related IoT' written by Geetha Venkatesan and Avadhesh Kumar. The authors proposed an adaptive trust management design that performs trust assessment considering both

QoS and social parameter for deciding the trustiness of a node in the IoT network. The design uses direct assessment and indirect recommendation, which are aggregated using a dynamic weighted method. The decay factor for the past experiences and dynamic updating of the trust profiles enhances the system performances. The work is compared with static, distributed, social and single trust type of system in terms of resiliency and performance. The proposed work shows very efficient trust assessment and maximum performance.

As the guest editors of this special issue, we were extremely thankful to the editor and journal manager of the *International Journal of Internet Technology and Secured Transactions* (*IJITST*) for their valuable support.