Editorial

L. Jegatha Deborah*

Department of Computer Science and Engineering,
University College of Engineering Tindivanam,
Tindivanam, 604-001, India
Email: blessedjeny@aucet.in
Email: blessedjeny@gmail.com
*Corresponding author

P. Vijayakumar

University College of Engineering Tindivanam,
Tindivanam, 604-001, India
Email: vijibond2000@aucet.in
Email: vijibond2000@gmail.com

B. Balamurugan

Department of Computer Science and Engineering,
Vellore Campus,
VIT University,
Vellore, Tamilnadu 632014, India
Email: kadavulai@gmail.com

Vassil T. Vassilev

Cyber Security Research Centre,
London Metropolitan University,
166-220 Holloway Rd, Holloway, London N7 8DB, UK
Email: v.vassilev@londonmet.ac.uk

Victor Chang

Xi'an Jiaotong Liverpool University,
BS 246, IBSS Building, 8 Chongwen Road,
Suzhou Dushu Lake Science and Education Innovation District,
Suzhou Industrial Park, Suzhou 215123, China
Email: victor.chang@xjtlu.edu.cn

Biographical notes: L. Jegatha Deborah completed her PhD in Computer Science and Engineering in Anna University Chennai in 2013 and completed her Master of Engineering in the field of Computer Science and Engineering in 2005. She completed her Bachelor of Engineering in 2002. She is currently working as an Assistant Professor in University College of Engineering Tindivanam and her research interests include database security and data mining.

P. Vijayakumar completed his PhD in Computer Science and Engineering in Anna University Chennai in 2013. He completed his Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology in 2005. He completed his Bachelor of Engineering under Madurai Kamarajar University in 2002. He is currently working as the Dean at University College of Engineering, Tindivanam. He is guiding many PhD scholars in the field of network and cloud security. He has published various quality papers in the reputed journals like *IEEE Transactions*, Elsevier, Springer, IET, Taylor & Francis, Wiley etc. His main thrust research areas are key management in network security and multicasting in computer networks.

B. Balamurugan is with VIT University as an Associate Professor in School of Information Technology and Engineering. His research interests have evolved from cloud computing, cloud security to big data and his PhD thesis is on cloud access control.

Vassil T. Vassilev is a Senior Lecturer and completed his PhD in Computer Science and his MSc in Automatic Control. He has professional affiliations with the British Computer Society and has knowledge transfer partnerships with Underscore Plc, New Brand Vision, and Rockfig. His research interests are in semantic web, intelligent technologies, web services, system integration, and distributed systems. His research projects include linguistic services for the semantic web and security of mobile banking.

Victor Chang is an Associate Professor (Reader) and Director of PhD at IBSS, Xi'an Jiaotong-Liverpool University, Suzhou, China, after working as a Senior Lecturer at Leeds Beckett University, UK, for 3.5 years. Within four years, he completed his PhD (CS, Southampton) and PGCert (Higher Educati on, Fellow, Greenwich) while working for several projects at the same time. He has published three books as sole author and the editor of two books on cloud computing and related technologies. He has given and will give 12 keynotes at international conferences.

In this digital era powered by information, there seems to be no doubt that information is wealthier than any other entity in this world. Thus, mining and learning any useful information from the huge datasets may reveal path breaking predictions for the benefit of the humankind (Fayyad, 1996). In such a context, machine learning coupled with high performance computing has become a matter of great concern in the field of computer science and seems to have robust application in geospatial systems, robotics, data analytics and security breaches among other applications (Wu et al., 2014). The concept of machine learning from the data posted in cloud servers and their efficient processing tools such as Hadoop portray the value of machine learning. Though cloud computing which provides elastic computing and storage facilities in the recent times, the reason for business and individual data movement to cloud seems to be reluctant due to security vulnerabilities (Zissis and Lekkas, 2012; Hashem et al., 2015). In such a context, providing confidentiality and ensuring integrity is of great concern. Though machine learning can be applied in multiple domains, there is scope for improvement in terms of security, data storage and retrieval techniques, prediction methodologies and others. The proposal for this special issue has received manuscripts from the 2nd International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM'17) held in India between the 3rd and 4th of February 2017. As part of the conference, 118 papers on various topics were received from authors belong to diverse disciplines.

The technical content, methodology of the research work, the contributions of this research work for the benefit of the society, the scope and real time implementation feasibility of the works are the driving factors behind the careful finalisation of the manuscripts. After careful examination, we feel delighted to submit eight research manuscripts of genuine contribution from the authors of different groups whose contribution may prove to be vital in the field of high performance computing and machine learning. The acceptance rate of the conference papers is around 6%.

In the paper titled 'Design and analysis of smart card-based authentication scheme for secure transactions', Pradhan et al. have proposed a remote authentication scheme utilising smart cards which have become a prevalent mode of communication due to their convenience and simplicity. Previously in line with this work, Lee et al. had proposed a low cost authentication scheme without verifier tables. But, the authors have clearly proved that Lee's scheme is susceptible to multiple attacks such as offline password guessing, user impersonation and fails to preserve the user's anonymity and other essential security properties. Hence, the authors have proposed a novel secure and efficient dynamic ID-based remote authentication scheme and have clearly proved that, the scheme is resistant to all the known attacks. The performance analysis portrays that, this work is efficient in terms of computation, communication and storage complexities which makes this protocol is an ideal candidate for secure electronic transactions. For a geospatial system where data grows exponentially, storage in public clouds and processing methods using Hadoop makes the data management convenient and manageable. In this context, Karthi and Prabu in the paper 'Secure geospatial data storage using SpatialHadoop framework in cloud environment' have proposed a remedy to the problems appearing in secure storage and processing of geospatial data in cloud. This work provides a framework that deals with protocol for authentication to handle security in a unique manner and also provides the scalability of execution of large-scale queries on SpatialHadoop. The affordability and simplicity to share the information using this approach provides decision effectively with higher confidence in the cloud. The improvement in the ability of storage, integration and correlation of data in an efficient way has also been dealt with in this research work. Though cloud storage provides elasticity at low costs, the data owners seem to be reluctant for remote data storage, fearing that the integrity of the data may get compromised either intentionally or unintentionally. Hence, Santhosh Kumar et al. in the research work entitled 'Secured data storage and auditing of data integrity over dynamic data in cloud' suggested a novel method for secure storage of data in cloud and the auditing of the stored data for ensuring the integrity of the same. Most of the existing schemes lack the security feature, which can withstand collusion attacks between the cloud server and the unauthorised users. But, this research work presents a technique to overthrow the collusion attacks and also the data auditing mechanism is achieved by means of vector commitment and backward unlinkable verifier local revocation group signature. This work involves double encryption technique to deal with the privacy measures in cloud server. To ensure data integrity, a single file has been split into different blocks and stored with different file names which avoids tracing out the original data. The performance of the proposed work is thoroughly analysed and results suggest that the experimental results are satisfactory in terms of computational and time complexity compared to the recent works in the literature.

Ezilarasan et al. in the paper titled 'Propels in compiler construction for versatile figuring' have proposed a compiler machine for adaptable figuring. The proposed technique assembles the flexibility and comfort in a way that grants to port the structure to different centres with an irrelevant effort. In light of a present arrangement stream, the authors accomplish another tier of handiness in the way of exploring and dividing programs written in C and the results confirm that the examination on this level is more successful than on lower ones as a result of usage of more communicative fabricate of programming. The authors have depicted an improved procedure for a compiler which sections an irregular state dialect program actually for midway hardware implementation on adaptable machines and produces fitting gear records courses from context free grammars. This approach is a new methodology for an added composed dividing and refining data way eminence.

Geetha Ramani and Sivaselvi in the research work titled 'Automatic segmentation of pathological region (tumour and oedema) in high grade glioma multi-sequence MR images through voted prediction from pixel level feature sets' have come out with a novel approach to segment the abnormal regions such as tumour and oedema of the brain in glioma images through preprocessing, feature extraction and classification. The extracted features are grouped and random forest procedure is applied on each set and the prediction is obtained which minimises the randomisation. The final prediction of a pixel is obtained by aggregation of individual predictions from feature set through maximum voting which increases the ensembling and improves the outcome appreciably. The average dice coefficients of tumour and oedema segmentation are 0.96 and 0.94 respectively with three-fold cross validation. The results show the significant improvement when compared to earlier methodologies. This method based on the image analysis can be used to predict the valuable prediction of the brain tumour onset in a human during pre-diagnosis, treatment and complete recovery from that deadly disease. In the paper 'Improving performance an artificial bee colony optimisation on CloudSim', Saravanan and Gokulraj strive to identify an accurate data search and to generate data that comes from anywhere. Furthermore, the data itself may be too large to store on a single machine such that the computers are inter connected with each other by the massive internet storage technologies. The proposed approach focuses mainly on the design of search engines and its infrastructure grave. Improved micro partitioning is a modularised approach of cloud computing mainly framed to overcome the pitfalls in the traditional search engine and also in manipulation of large information stored in a single computer. Artificial bee colony (ABC) count is an improvement figuring which re-enacts the watchful scavenging behaviour of honey bees. The results exhibit the fact that, the mix of the proposed algorithm estimation, masterminding in context of the level of assignments, and the book making sense played a superior than normal execution orchestrating the structure in changing conditions and acclimating work stack which can reduce the make traverse of information prepare time.

Kavisankar et al. in the paper 'Enhanced efficient SYN spoofing detection and mitigation scheme for DDoS attacks' claim that the protection of the critical servers from the cyber attacks is vital in this digital era especially from distributed denial of service (DDoS). A number of attack packets are generated from the single attacking system to cause a denial of service to the legitimate users or impairs the authorised use of networks, systems, or applications by exhausting the resources, such as central processing units (CPU), memory, bandwidth, and disk space. The main objective of this research is to detect and defend the spoofed SYN packet, during a DDoS/DoS attack. The proposed

efficient SYN spoofing detection and mitigation scheme controls the resources to a three-way TCP handshake connection and uses the probing method to query the availability of the client as in IP puzzle method, which reduces the performance of the attacker and makes the attack ineffective. The concept of bloom filter is used which is a probabilistic data structure algorithm, for doing existence/membership tests in less memory as it does not require full list of keys. This method is deployed in both the IPv4/IPv6 in the SSE test bed environments and it is found that, this work provides better control in both the internet protocol versions. TCP SYN flooding is targeted to affect end host, thus the solution is given at the host-based solution. Hemamalini et al. in the research work titled 'An efficient probabilistic authentication scheme for converging VANET' have proposed a novel scheme to provide seamless connectivity and secure message transmission in vehicular ad-hoc networks during vehicle mobility. In such contexts, the presence of adversarial nodes could provide false position information or disrupt the acquisition of such information. Thus, in VANETs, the discovery of neighbour positions should be performed in a secure manner. The proposed solution does not require the use of a-priori trustworthy nodes, but it leverages the information exchange between neighbours. The analysis proves that the current scheme to be very effective in identifying independent as well as colluding adversaries. Results derived using realistic vehicular traces confirm such ability of the proposed approach and highlights the performance of 107 kbps compared with our solution in terms of both false negatives/positive and uncertain neighbour classifications and delay is reduced by 4%, thereby packet drop has been reduced to 5% which in turn reduces overhead by 19%. Thus, the results suggest that, the proposed protocol is highly effective in detecting falsified position information, while maintaining a low rate of false positive detections.

References

Fayyad, U.M. (1996) 'Data mining and knowledge discovery: making sense out of data', *IEEE Expert: Intelligent Systems and Their Applications*, Vol. 11, No. 5, pp.20–25.

Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A. and Khan, S.U. (2015) 'The rise of big data on cloud computing: review and open research issues', *Information Systems*, Vol. 47, pp.98–115 [online] https://doi.org/10.1016/j.is.2014.07.006.

Wu, X., Zhu, X., Wu, G-Q. and Ding, W. (2014) 'Data mining with big data', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 26, No. 1, pp.97–107.

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation Computer Systems*, Vol. 28, No. 3, pp.583–592.