Editorial

Security, Trust and Privacy in Cyber (STPCyber): Future Trends and Challenges

Priyadarsi Nanda [a] , Xiangjian He [a] , Laurence T. Yang [b]

[a] Faculty of Engineering and IT, University of Technology Sydney, Australia

[b] Department of Computer Science, St. Francis Xavier University, Canada

ABSTRACT

Today’s world experiences massively interconnected devices to share information across variety of platforms between traditional computers (machines), Smart IoT devices used across smart homes, smart interconnected vehicles etc. and of course the social networks apps such as Facebook, Linkdn, twitter etc. We experience the growth has been skyrocketing and the trend will continue exponentially to the future. At one end, we find life becomes easier with such developments and at the other end; we experience more and more cyber threats on our privacy, security and trustworthiness with organizations holding our data. In this special issue, we summarize contributions by authors in advanced topics related to security, trust and privacy based on a range of applications and present a selection of the most recent research efforts in these areas.

1. Introduction

With the rapid development and increasing complexity of computer systems and communication networks, user requirements for trust, security and privacy are becoming more and more demanding. Hence, there is a grand challenge that traditional security technologies and measures may not meet user requirements in open, dynamic, heterogeneous, mobile, wireless, and distributed computing environments. Thus, there is a strong need to build systems and networks in which various applications allow users to enjoy services that are more comprehensive while, preserving trust, security and privacy at the same time. In addition, useful and innovative technologies, trusted computing and communications are attracting researchers with more and more attention.

The scope of this special issue is broad and is representative of many important topics involving emerging technologies in the field of Trust, Security, Privacy, Forensics and Data analytics. In addition, the articles selected through this special issue also present strong aspects on theoretical analysis, algorithms, and practical experience in their proposed schemes.

The submissions to this special issue were extended versions of the selected papers from the 16th IEEE International conference on Trust, Security and Privacy in Computing and Communications (Trustcom 2017) conference along with many open submissions whose topics fit in the scope of this special issue. All the submissions for this special issue have been reviewed rigorously following the guidelines of Elsevier Journal on Future Generation Computer Systems (FGCS). After a rigorous review process, among 60 very high quality submissions received, only 21 papers have been accepted for publication in this issue.

A majority of the reviewers who have reviewed submitted articles for this special issue represent expertize in their fields. All reviewers have provided high quality reviews for the submitted manuscripts. The selected articles in this special issue have gone through a rigorous reviews process and are briefly presented in the rest of this guest editorial.

The guest editors sincerely believe that this special issue on Security, Trust and Privacy will be a great resource for the researchers worldwide.

2. Content of the special issue

In this special issue, the accepted papers are mainly grouped into three areas; Security, Trust and Privacy.

2.1 Security

The first paper in security domain, “Security in Cognitive Radio Network: Defense Against Primary User Emulation Attacks Using Genetic Artificial Bee Colony (GABC) Algorithm” by Elghamrawy et al. [Elghamrawy, 2019] presents a hybrid Genetic Artificial Bee Colony (GABC) algorithm optimizing the spectrum utilization in cognitive Radio Networks (CRN) by detecting attacks with higher probability. The author presents simulations results validating performance of their scheme and comparing with recent detection algorithms. Yin etal. [Yin, 2019] propose a conjunctive multi-keyword ranked secure search scheme for multiple data owners. They design an ingenious secure query scheme allowing each data owner to adopt randomly chosen temporary keys and build secure indexes for different data files. Based on their extensive experiments the authors also demonstrate the correctness and practicality of the proposed scheme.

Shen et al. [Shen, 2019] propose efficient cloud-aided verifiable secret sharing scheme based on the polynomial commitment for smart cities. The authors also extend their scheme supporting batch verification with the aid of a third-party arbitration centre. The security analysis shows that the proposed scheme enhances efficiency in terms of the communication and computational cost. Next paper by Nanda et al. [Nanda, 2019] presents a secure Geo-Location Oriented Routing (SecureGLOR) protocol for wireless mesh networks by incorporating a hybrid encryption scheme. Their proposed scheme improves the network’s overall performance using a combination of symmetric as well as asymmetric key. Usman et al. [Usman, 2019] presents secured and reliable data delivery method for Mobile Adhoc Networks (MANET) by proposing a novel scheme. Their proposed scheme prevents the malicious nodes from data exchange with legitimate intermediate nodes on any established path between the source and the destination. Experimental results show that their proposed scheme performs better in terms of packet-loss rate, jitter and end-to-end delay as well as, proposed scheme is efficient against various attacks and has a much better performance in terms of associated costs, such as key generation, encryption, and storage and communication.

Security and privacy of data protection is one of the important aspects for android applications. Bhandari et al. [Bhandari, 2019] proposed a novel scheme to address the threat emanating from multiple colluding Android applications (apps). They present SneakLeak+, a model checking based technique for detection of app collusion. Their proposed method is aimed at analysing multiple apps simultaneously using reverse engineered intermediate code for each app and extract information into a compact form suitable for formal verification. Tahir et al. [Tahir, 2019] develop a parallelized disjunctive query based searchable encryption scheme for big data where, the scheme is based on probabilistic trapdoors that are formed by making use of the property of modular inverses. Probabilistic trapdoors help resist distinguishability attacks. The rigorous security analysis provides advantage of their scheme. Another article by Yu et al. [Yu, 2019] develop a framework for analyzing structural security in e-commerce business process. The authors develop a Petri net-based modelling for e-commerce business processes and analyze structural security issues within them.

2.2 Trust

Trust is an important issue in Cybersecurity domain as it provides robust measure for data security. In this regards, we selected number of articles where proposed schemes by various authors make good contributions to this special issue. The first paper by Shah Rahman et al. [Rahman, 2019] propose trustworthiness with the help of a broker facilitating negotiation between two parties in a highly distributed fog-computing environment. The authors claim their broker-based trust evaluation framework is the first one to identify and fulfil user requests. Their Request Matching algorithm identifies a user request, and Fuzzy-based Filtering algorithm is used to match the request with one of the predefined sets created and managed by the broker. Another important contribution on trust issues in Fog computing were by Wang et al. [Wang, 2019] in which the authors present their scheme for fog-based hierarchical trust mechanism in Sensor-Cloud Systems (SCS). Their hierarchical mechanism consists of two parts, trust in the underlying structure and trust between cloud service providers (CSPs) and sensor service providers (SSPs). For trust in the underlying structure, the behaviour monitoring part is established and implemented in Wireless Sensor Networks (WSNs), and the fine-grained and complicated data analysis part is moved to the fog layer. For trust between CSPs and SSPs, it focuses more on the real-time comparison of service parameters, the gathering of exception information in WSNs, the targeted quantitative evaluation of entities. The reliability of edge nodes is well guaranteed by data analyses in the fog layer and an evaluation strategy based on similar service records are very well presented in this paper.

Zhang et al. [Zhang, 2019] develop iFlask: Isolate Flask Security System From Dangerous Execution Environment by Using ARM TrustZone. In their article, the authors identify security issues involving complicated mobile runtime environment, solve the problem by isolating security server subsystem into the enclave provided by the ARM TrustZone, and avert the negative impacts of the malicious environment. The prototype is implemented on SELinux, which is the widely used Flask-based MAC system, and the base of SEAndroid. Experimental results show that SELinux receives reliable protection resisting all known vulnerabilities and remains unaffected by the attacks in the test set. The article by Fan et al. [Fan, 2019] presents preventing leakage of sensitive information (such as the contact lists, or private pictures) for mobile users through a fine-grained access-control scheme based on Cipher text-Policy Attribute-Based Encryption (CPABE) and Trusted Execution Environment (TEE). In their scheme, CPABE is adopted in a novel way to solve the important security problems by supporting fine-grained access control during the access period and by supporting the critical operations running in the trusted execution environment. Their proposed scheme compares traditional access-control mechanisms and results from this research indicate better performance. The final paper accepted under trust issues is by Xiong et al. [Xiong, 2019] in which the authors present a Client/Server framework and create a private recommender system (PrivateRS). Their proposed system assumes that the Server side is untrustworthy. On the Client side, each user firstly rates the items and randomizes the ratings with a differential privacy mechanism. The ratings are further substituted by private symbols, which are autonomously defined by each user to hide the ordinal meaning of the ratings. The Server then applies a private collaborative filtering algorithm to predict the ratings of items for the user. Their experimental results demonstrate that the proposed algorithms can still generate accurate recommendations with acceptable loss even if ordinal meaning of the rating is significantly obfuscated.

2.3 Privacy

Data privacy is utmost important with proliferation of massive amount of data in the Internet. Starting from location based privacy to anonymous privacy in the cloud, there has been significant research efforts in the last decades to preserve integrity and confidentiality of user data. In this special issue, we present some of the novel schemes contributed by researchers on privacy preserving schemes, which identify and apply their novelty in future applications.

Zhang et al. [ZhangS, 2019] develop their privacy enhancement scheme for location based services (LBS) using Caching and Spatial K-anonymity. Using existing approach, users transmit the location query data to an untrusted location service provider (LSP) and obtain query results. These results are then discarded immediately after using them. Such approach is inefficient and also results higher privacy risk to user from the LSP. In this paper, the authors propose their enhanced user privacy scheme through caching and spatial K-anonymity (CSKA). Their scheme adopts multi-level caching to reduce the risk of exposure for users' information to untrusted LSPs. Using Markov model to predict the next query location according to the user mobility, cell's cache contribution rate, and data freshness, the paper then describes efficiency of the proposed CSKA scheme supporting higher privacy protection.

Yousra et al. [Yousra, 2019] present privacy preserving scheme for online social networks (OSN) using Community-Centric-Brokerage-Aware access control in which the proposed method utilizes Social Network Analysis (SNA) and provide improved privacy. For community detection, Attribute-Based Community Detection (ABCD) algorithm is being used comparing the results with Louvain, Newman's Eigenvector, and Clauset algorithms. The results of the ABCD algorithm outperform other methods in terms of modularity and the number of communities for large and dense networks. Liu et al. [Liu, 2019] present their works on Privacy-preserving matrix product based static mutual exclusive roles constraints violation detection in interoperable role-based access control (IRBAC) to achieve security between two or more RBAC administrative domains. Through efficiency analysis and experimental results comparison, their scheme is more efficient and practical. Luo et al. [Luo, 2019] present a novel privacy-preserving matching scheme based on both identity authentication and private matching in mobile social networks. Their proposed scheme uses encryption and authentication techniques to guarantee failure of the attacker to get information of user's attribute profile, and hence, protects personal privacy during friend matching process.

Sharma et al. [Sharma, 2019] present a scalable two-phase improved MaxMin BB-KHT using MapReduce framework (MR-I MaxMin). The proposed MapReduce approach helps achieving the feasibility by processing large voluminous data in a parallel fashion. Experimental results and evaluations shows proposed MR-I MaxMin technique outperforms similar existing approaches and vanquishes the identified challenges along with much-needed privacy preservation. Asikis et al. [Asikis, 2019] propose parameterizations of privacy settings that regulate the trade-off between maximum utility, minimum privacy and minimum utility, maximum privacy, where utility refers to the accuracy in the estimations of aggregation functions. The authors develop generic and novel computational framework for measuring privacy-utility trade-offs and their Pareto optimization. The practical use of the framework is experimentally evaluated using real-world data from a Smart Grid pilot project in which energy consumers protect their privacy by regulating the quality of the shared power demand data, while utility companies make accurate estimations of the aggregate load in the network to manage the power grid.

In another novel contribution, Nhien-An Le-Khac et al. [Nhien-An Le-Khac, 2019] present privacy issues related to smart vehicles and investigate forensics aspects in their article. Smart or driverless cars, store a wealth of digital information, such as recent destinations, favourite locations, routes, and personal data (e.g. such as call logs, contact lists, SMS messages, pictures, and videos). The authors identify some of the challenges associated with vehicle data forensics, and present a case study on forensic acquisition and data analysis of an entertainment system used on a Volkswagen car for criminal investigation. Finally, Shen et al. [Shen, 2019] present secured Content-based image retrieval (CBIR) scheme that supports Multiple Image owners with Privacy Protection (MIPP). The proposed scheme encrypts image features with a secure multi-party computation technique, which allows image owners to encrypt image features with their own keys. This enables efficient image retrieval over images gathered from multiple sources, while guaranteeing that image privacy of an individual image owner will not be leaked to other image owners. Theoretical analysis and experimental results demonstrate that MIPP achieves retrieval accuracy and efficiency simultaneously, while preserving image privacy.

3. Conclusion

Security, Trust and Privacy are significantly important elements of Cybersecurity due to tremendous growth in smart devices and the way we share our information. There have been significant advancement of technologies such as Arificial Intelligence (AI), Machine Learning (ML) etc., which are now used to develop better solutions to defend against emerging cyber-attacks. In spite of all such efforts by the research community, cyber attackers also have been able to use these technologies in many wrong ways, which open up a new front in creating additional attack surface. Core devices such as the routers, home assistants, IoT, Autonomous systems etc. are the kinds of equipment that interact most in the Internet. Hence, they are likely to be the primary targets for attackers. Observing the research trend and their significance on the research community, in this special issue, we outline a list of important research contributions by authors and their potential for the future.

Acknowledgements

We would like to thank all the authors who submitted their research articles in this special issue. We would also like to thank all the reviewers for their valuable time and effort for reviewing the articles allocated to them and submitting their valuable comments. Their comments greatly enabled us to select papers for this high quality special issue. We would like to thank the FGCS Editor-in-Chief, Professor Peter Sloot and the Elsevier staffs for their continuous help and support that made this special issue possible. We hope this Special issue of FGCS journal will serve a reference for many future research projects.

References

[Elghamrawy, 2019]. S. M. Elghamrawy, Security in Cognitive Radio Network: Defense Against Primary User Emulation Attacks Using Genetic Artificial Bee Colony (GABC) Algorithm, Future Generation of Computer System [this issue]

[Yin, 2019]. H. Yin, Z. Qin, J. Zhang, L. Ou, F. Li, K. Li, Secure Conjunctive Multi-keyword Ranked Search over Encrypted Cloud Data for Multiple Data Owners, Future Generation of Computer System [this issue]

[Shen, 2019]. J. Shen, D. Liu, X. Sun, F. Wei, Y Xiang, Efficient Cloud-Aided Verifiable Secret Sharing Scheme with Batch Verification for Smart Cities, Future Generation of Computer System [this issue]

[Nanda, 2019]. A. Nanda, P. Nanda, X. He, A. Jamdagni, D. Puthal, A Hybrid Encryption Technique for Secure-GLOR: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks, Future Generation of Computer System [this issue]

[Usman, 2019]. M. Usman, M. A. Jan, X. He, P. Nanda, QASEC: A Secured Data Communication Scheme for Mobile Ad-hoc Networks, Future Generation of Computer System [this issue]

[Bhandari, 2019]. S. Bhandari, F. Herbreteau, V. Laxmi, A. Zemmari, M. S. Gaur, P. S. Roop, SneakLeak+: Large-Scale Klepto Apps Analysis, Future Generation of Computer System [this issue]

[Tahir, 2019]. S. Tahir, L. Steponkus, S. Ruj, M. Rajarajan, A. Sajjad, A Parallelized Disjunctive Query based Searchable Encryption Scheme for Big Data, Future Generation of Computer System [this issue]

[Yu, 2019]. W. Yu, Z. Ding, L. Liu, X. Wang, R. D. Crossley, Petri Net-Based Methods for Analyzing Structural Security in Ecommerce Business Processes, Future Generation of Computer System [this issue]

[Rahman, 2019]. F. H. Rahman, T-W. Au, S. H. S. Newaz, W. S. Suhaili, G-M Lee, Find My Trustworthy Fogs: A Fuzzy-based Trust Evaluation Framework, Future Generation of Computer System [this issue]

[Wang, 2019]. T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, M. Xie, A Novel Trust Mechanism Based on Fog Computing in Sensor-Cloud System, Future Generation of Computer System [this issue]

[Zhang, 2019]. D. Zhang, S. You, iFlask: Isolate Flask Security System From Dangerous Execution Environment by Using ARM TrustZone, Future Generation of Computer System [this issue]

[Fan, 2019]. Y. Fan, S. Liu, G. Tan, F. Qiao, X. Lin, Fine-Grained Access Control Based on Trusted Execution Environment, Future Generation of Computer System [this issue]

[Xiong, 2019]. P. Xiong, L. Zhang, T. Zhu, G. Li, W. Zhou, Private Collaborative filtering under Untrusted Recommender Server, Future Generation of Computer System [this issue]

[ZhangS, 2019]. S. Zhang, X. Li, Z. Tan, T. Peng, G. Wang, A Caching and Spatial K-anonymity Driven Privacy Enhancement Scheme in Continuous Location-Based Services, Future Generation of Computer System [this issue]

[Yousra, 2019]. A. Yousra, A. K. Malik, B. Raza, W. Naeem, S. Rathore, Community-Centric Brokerage-Aware Access Control for Online Social Networks, Future Generation of Computer System [this issue]

[Liu, 2019]. M. Liu, Y. Luo, C. Yang, D. Puthal, K. Ren, X. Zhang, Privacy-preserving Matrix Product Based Static Mutual Exclusive Roles Constraints Violation Detection in Interoperable Role-Based Access Control, Future Generation of Computer System [this issue]

[Sharma, 2019]. S. Sharma, D. Toshniwal, MR-I MaxMin- Scalable Two-Phase Border Based Knowledge Hiding Technique Using MapReduce, Future Generation of Computer System [this issue]

[Asikis, 2019]. T. Asikis, E. Pournaras, Optimization of Privacy-Utility Trade-offs under Informational Self-determination, Future Generation of Computer System [this issue]

[Nhien-An Le-Khac, 2019]. N-A. L. Khac, D. Jacobs, J. Nijhoff, K. Bertens, K-K. R. Choo, Smart Vehicle Forensics: Challenges and Case Study, Future Generation of Computer System [this issue]

[Luo, 2019]. E. Luo, K. Guo, Y. Tang, X. Ying, W. Huang, Hidden the True Identity and Dating Characteristics Based on Quick Private Matching in Mobile Social Networks, Future Generation of Computer System [this issue]

[Shen, 2019]. M. Shen, G. Cheng, L. Zhu, X.Du, J. Hu, Content-Based Multi-Source Encrypted Image Retrieval in Clouds with Privacy Preservation, Future Generation of Computer System [this issue]

ABOUT THE GUEST EDITORS

Priyadarsi Nanda obtained his PhD in Computing Science from University of Technology Sydney, Australia, Master's degree in Computer and Telecommunication Engineering from University of Wollongong, Australia and Bachelor of Engineering with Distinction in Computer Engineering from Shivaji University, India. He is a Senior Lecturer at the University of Technology Sydney (UTS), Australia with more than 28 years of experience specialising in research and development in Cybersecurity, IoT security, Internet Traffic Engineering, wireless sensor network security and many more related areas. His most significant work has been in the area of Intrusion detection and prevention systems (IDS/IPS) using image processing techniques, Sybil attack detection in IoT based applications, intelligent firewall design. He has authored more than 100 research articles including Transactions in Computers, Transactions in Parallel Processing and Distributed Systems (TPDS), Future Generations of Computer Systems (FGCS) as well as many ERA Tier A/A* conference articles. In 2017, his work in cyber security research has earned him and his team the prestigious Oman research council's national award for best research.

Xiangjian He received his PhD from the University of Technology Sydney (UTS) in 1999 and is currently the Director of Computer Vision and Pattern Recognition Laboratory at the Global Big Data Technologies Centre (GBDTC) at UTS. He has been carrying out research mainly in the areas of image processing, network security, pattern recognition, computer vision and machine learning in the previous years.

Laurence T. Yang got his BE in Computer Science and Technology and BSc in Applied Physics both from Tsinghua University, China and Ph.D in Computer Science from University of Victoria, Canada. He is a professor and W.F. James Research Chair at St. Francis Xavier University, Canada. His research includes parallel and distributed computing, Internet of Things, and big data. He has published around 400 international journal papers in the above areas, of which half on top IEEE/ACM Transactions and Journals, others mainly on Elsevier, Springer and Wiley Journals. In recent years, 4 and 22 papers have been listed as top 0.1% and top 1% highly-cited ESI papers, respectively. He has been involved actively act as a steering chair for 10+ IEEE international conferences. He served as the vice-chair of IEEE CS

Technical Committee of Supercomputing Applications (2001-2004), the chair of IEEE CS Technical Committee of Scalable Computing (2008-2011). He was the vice-chair (2014) and the chair (2015) of IEEE Canada Atlantic Section. Now he is the chair of IEEE CS Technical Committee of Scalable Computing (2018-), the co-chair of IEEE SMC Technical Committee on Cybermatics (2016-) and the vice-chair of IEEE CIS Technical Committee on Smart World (2016-2018).His recent honours and awards include Fellow of Engineering Institute of Canada (2019), AMer's Most Influential Scholar Award (2018) in the field of Internet of Things, IEEE TCCPS Distinguished Leadership Award on Cyber-Physical Systems (2018), IEEE SCSTC Life-Career Achievement Award on Smart Computing (2018), Fellow of Canadian Academy of Engineering (2017), IEEE System Journal Best Paper Award (2017), IEEE TCSC Award for Excellence in Scalable Computing (2017), and the PROSE Award on Engineering and Technology (2010).