Multimed Tools Appl (2018) 77:9203–9208
DOI 10.1007/s11042-017-5301-x

GUEST EDITORIAL

Advances in Security and Privacy of Multimedia Big Data in Mobile and Cloud Computing

B. B. Gupta[1] · **Shingo Yamaguchi**[2] · **Dharma P. Agrawal**[3]

Published online: 13 November 2017

Abstract In recent years, the use of mobile and cloud Computing is rapidly growing. In other word, mobile and cloud Computing play an important role in everybody's life today. It carries rich computational resources to mobile users, network operators, as well as cloud computing providers. Moreover, the explosion of multimedia big data (image, video, 3D, etc.) in mobile and cloud computing have created unprecedented opportunities and fundamental security and privacy challenges as they are not just big in volume, but also unstructured and multi-modal. Therefore, the papers of this special issue address variety of security and privacy issues of multimedia big data in mobile and cloud computing and security of other aspects of mobile and cloud networks and also emphasizes many open questions. We anticipate that papers of this special issue will open new entrance for further research and technology improvements in this important area.

1 Introduction

Today, cyber security and privacy is an essential need for modern society where information technology and services pervade every aspect of our lives [1, 6, 8]. Specially, security and privacy of multimedia big data in mobile and cloud computing which is becoming a part of daily life to access different multimedia systems, services and applications is a serious issue, today. Moreover, protecting user privacy and multimedia data/application secrecy from adversary is a key to establish and maintain consumers' trust in the mobile and cloud platform [3, 4, 11, 16]. However, it is challenging to achieve, as technology is changing at rapid speed and our systems turn into ever more complex. Moreover, cyber space is considered as fifth battle-field after land, air, water and space. The explosion of multimedia data (image, video, 3D, etc.) in mobile and cloud computing have created unprecedented opportunities and fundamental

✉ B. B. Gupta
bbgupta@nitkkr.ac.in

[1] National Institute of Technology Kurukshetra, Kurukshetra, India

[2] Yamaguchi University, Yamaguchi, Japan

[3] University of Cincinnati, Cincinnati, OH, USA

security and privacy challenges as they are not just big in volume, but also unstructured and multi-modal [9, 12, 14].

These considerations have led to this special issue and security solutions have evolved to detect and prevent attacks in mobile and cloud computing. Specifically, this special issue addresses various security and privacy aspects in multimedia big data in mobile and cloud computing, with a focus on simulations of mobile and cloud networks, representation, applications/tools and analysis of mobile and cloud networks, particularly on advances computing technologies and related areas [7, 10, 12]. Papers were invited for this special issue considering aspects of this problem, including:

- Security and privacy of multimedia big data in mobile cloud computing
- Security and privacy management of multimedia big data in Cloud Computing
- Mobile cloud computing intrusion detection systems
- Security of pricing and billing for mobile cloud computing multimedia services
- Cryptography, authentication, authorisation and usage control for multimedia big data in cloud
- Security and privacy of multimedia big data in smartphone devices
- Security of Mobile, peer-to-peer and pervasive multimedia services in clouds
- Security of multimedia big data in Mobile commerce and mobile internet of things
- Security and privacy of multimedia big data in sensor networks
- Multimedia big data-enabling social networks on Clouds
- Resource management for multimedia big data on Clouds
- Cryptography, authentication, authorisation and usage control for multimedia big data in mobile devices
- Multi-modal information retrieval for big data on Clouds Multidimensional visualization systems of multimedia big data on Clouds
- Security and privacy of multimedia big data in social applications and networks
- Multimedia Web service security

This special issue contains eleven papers which were selected after rigorous review process to deal with different aspects of security and privacy issues in online social networks and other related areas [2, 5, 13, 15].

2 Contributions

The first article entitled, “Integrated QoUE and QoS approach for optimal service composition selection in internet of services (IoS)” (https://doi.org/10.1007/s11042-016-3837-9) authored by S. M. Balakrishnan, et al. presents an optimization strategy oriented to efficient composite service selection for IoS model is designed through use of Particle Swarm Optimization (PSO) technique. Furthermore, prior to optimization, the services are assured of rich QoUE, especially trustworthiness in terms of reputation. The proposed work evaluates QoUE using the fuzzy based inference algorithm for identifying QoUE satisfied composite service. Authors claim that the experimental evaluation on a set of real world web services demonstrates the effectiveness of proposed methodology.

The second paper entitled, “A resource-efficient encryption algorithm for multimedia big data” (https://doi.org/10.1007/s11042-016-4333-y) authored by Aljawarneh, S. et al. presents a resource-efficient encryption system for encrypting multimedia big data in IoT. The proposed

system takes the advantages of the Feistel Encryption Scheme, an Advanced Encryption Standard (AES), and genetic algorithms. To satisfy high throughput, the GPU has also been used in the proposed system. Authors claim that this system is evaluated on real IoT medical multimedia data to benchmark the encryption algorithms such as MARS, RC6, 3-DES, DES, and Blowfish in terms of computational running time and throughput for both encryption and decryption processes as well as the avalanche effect. The results show that the proposed system has the lowest running time and highest throughput for both encryption and decryption processes and highest avalanche effect with compared to the existing encryption algorithms. To satisfy the security objective, the developed algorithm has better Avalanche Effect with compared to any of the other existing algorithms and hence can be incorporated in the process of encryption/decryption of any plain multimedia big data. Moreover, it has shown that the classical and modern ciphers have very less Avalanche Effect and hence cannot be used for encryption of confidential multimedia messages or confidential big data. The developed encryption algorithm has higher Avalanche Effect and for instance, AES in the proposed system has an Avalanche Effect of %52.50. Therefore, such system is able to secure the multimedia big data against real-time attacks.

The third paper entitled "Bridging the gap: effect of text query reformulation in multimodal retrieval" (https://doi.org/10.1007/s11042-016-4262-9) authored by Datta, D, et al. uses relevance feedback from the user-generated documents associated with the images for expanding textual query and study its effect on both image and text retrieval. Authors employ a topic decomposition based key phrase extraction technique to expand the textual queries. The results articulate the fact that an insightful textual query expansion always improves retrieval performance for both textual or image retrieval. Moreover, authors adopt optimum weight learning scheme to combine the modalities in a privileged way. Authors perform a comparative study with two well established key phrase extraction techniques which are used for textual query expansion. A detailed set of experiments on a standard real world dataset is also carried out for the same.

The fourth paper entitled, "A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment" (https://doi.org/10.1007/s11042-017-4386-6) is authored by Jian Shen, et al.. In this paper, authors propose a new lightweight RFID grouping authentication protocol for multiple tags in mobile environment. A number of tags are attached to different parts of the large-size object. The proposed protocol can tolerate missing tags. The tags that do not respond will not disturb the entire authentication process, which guarantees that the object can be timely verified. Moreover, the security analysis shows that this protocol can offers sufficient security assurances and resist various attacks. Besides, the proposed protocol has better performance in terms of the execution time compared to previous studies.

The fifth paper entitled, "Face recognition based on the fusion of wavelet packet sub-images and fisher linear discriminants" (https://doi.org/10.1007/s11042-017-4343-4) authored by Tang Wenjing, et al. presents a face recognition algorithm named FW-FLD by combining PCA (Principal Component Analysis) and FLD (Fisher Linear Discriminant) to improve the efficiency and accuracy of face recognition, based on fusion of wavelet packet sub-images. Firstly, the training samples are decomposed using wavelet packet. The fusion weights of the decomposed sub-images are calculated according to their energy distribution and the weighted fusion images are obtained, which reserve the images characteristic in the frequency. Then the features of the fused images are extracted using PCA, and the optimized Fisher space is constructed using FLD. Finally, face images are classified by measuring the projection coefficients of optimized training samples and testing samples in Fisher space. Experimental results on CMU PIE, JAFFE and AR face databases show that the proposed algorithm is robust, and can adapt to face recognition with

various illumination, facial expressions and gestures. Authors also claim that, it not only improves the face recognition rate, but also has a higher time efficiency.

In the sixth paper entitled, "Efficient biometric palm-print matching on smart-cards for high security and privacy" (https://doi.org/10.1007/s11042-016-4271-8) authored by Nadia Nedjah, et al. the use smart-cards is adopted as a possible effective yet efficient solution to this problem. Palm-prints have been used as a human identifier for a long time now. This biometric is considered one of the most reliable to distinguish a person from another as its unique yet stable over time. Moreover, authors propose an efficient implementation of palm-print verification on smart-cards. For this implementation, the matching is done on-card. Thus, the biometric characteristics are always kept in the owner's card, guaranteeing the maximum security and privacy. In a first approach, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are improved using upward, downward, leftward and rightward translations of the matched palm-codes. However, after thorough analysis of the achieved results, authors show that the proposed method introduces a significant increase in terms of execution time of the matching operation. In order to mitigate this impact, authors augmented the proposed technique with an acceptance threshold verification, thus decreasing drastically the execution time of the matching operation, and yet achieving considerably low FAR and FRR. It is noteworthy to point out that these characteristics are at the basis of any access control successful usage.

The seventh paper entitled, "Design of efficient shape feature for object-based watermarking technology" (https://doi.org/10.1007/s11042-017-4344-3) authored by Byung-Gyu Kim, et al. proposes the shape representation method using angles, orientations, and locations which is called as Oriented Angular Key-points (OAK) to make help for shape-based watermarking scheme. First, the contour is extracted from input image and is divided into contour blocks. Then, angles and directions from the divided contour blocks are computed to make unique feature. To evaluate the proposed image retrieval algorithm, commonly employed datasets of Gorelick and MPEG-7 are also used in this paper. The performance of the similarity measure that proposed image retrieval algorithm achieves improvement of about 10% compared with Shape Context in terms of Bull's eye score.

The eighth paper entitled, "Context-aware multimodal recommendations of multimedia data in cyber situational awareness" (https://doi.org/10.1007/s11042-017-4681-2) authored by Awny Alnusair, et al. presents a cloud-assisted recommendation system that can identify and retrieve multimedia data of interest based on contextual information and security analysts' personal preferences. This recommendation system benefits security analysts by establishing a bridge between their personal preferences, the contextual information of their analytical process, and the various types of modality of multimedia data. Evaluation of the proposed system shows evidence that these multimedia recommendation mechanisms promotes cyber threat understanding and risk assessment.

The ninth paper entitled, "Formal modeling and verification of security controls for multimedia systems in the cloud" (https://doi.org/10.1007/s11042-017-4853-0) authored by Masoom Alam et al. focuses mainly on the formal verification of the OSTORM a SIEM system. Authors have used High-Level Petri Nets (HLPN) and Z language to model and analyze the system. Moreover, Satisfiability Modulo Theories Library (SMT-Lib) and Z3 solver are used in this research to prove the correctness of the overall working of the OSTORM system. In addition, authors demonstrate the correctness of the underlying system based on four security properties, namely: a) event data confidentiality, b) authentication, c) event data integrity, and d) alarm integrity. The results reveal that the OSTORM system functions correctly.

The tenth paper entitled, "Efficient and secure BIG data delivery in Cloud Computing" (https://doi.org/10.1007/s11042-017-4590-4) authored by Christos Stergiou et al. presents a

survey on BD and CC technology and their basic characteristics, with a focus on the security and privacy issues of both technologies. Specifically, authors try to combine the functionality of the two technologies (i.e BD and CC) with the aim to examine the frequent features, and also to discover the benefits related in security issues of their integration. Finally, authors present a new method that can be used for the purpose of improving cloud computing's security through the use of algorithms that can provide more privacy in the data related to big data technology. At the end, authors present a survey about the challenges of the integration of BD and CC and corresponding security challenges.

The eleventh paper entitled, "A security framework for cloud-based video surveillance system" (https://doi.org/10.1007/s11042-017-4488-1) authored by Mohammad A. Alsmirat, et al. proposes an end-to-end security framework for a cloud-based video surveillance system that supports a large number of cameras. Proposed framework provides mutual authentication, session key management, data confidentiality, and data integrity. Consequently, encrypted video frames can only be sourced from authenticated cameras and only destined to authenticated cloud devices where the integrity of such frames can also be verified against potential change. As video streaming is a very delay-sensitive application, authors study different variations of the proposed framework to find security options that achieve the best trade-off between the added delay and the security of the system.

3 Conclusion

This special issue presented some selected papers in touching important aspects of security and privacy of multimedia big data in mobile and cloud computing and security of other aspects of mobile and cloud networks and also emphasizes many open questions. Moreover, the wide spread use and importance of multimedia big data in mobile and cloud networks encourage various researchers to look at different security and privacy issues which need to be addressed urgently by developing efficient defense solutions and a lot more work need to be done before it is widely accepted by the user community. We hope the papers covered in this special issue will provide relevant insights into the emerging trends in security and privacy of multimedia big data in mobile and cloud computing.

Acknowledgements We would like to express our special thanks to Prof. Borko Furht, the Editor-in-Chief of Multimedia Tools and Applications, for his great support and efforts throughout the whole publication process of this special issue. Moreover, this special issue is due to the encouragement of Banua, Jay-y, Dramis, Courtney, Christian Malan, Fearon Melissa, Jennifer Evans, and others who are instrumental in the organization process, and to the Springer Journal Editorial Office for their continuous support to publish this special issue. Many individuals have contributed toward the success of this issue. Special thanks are due to dedicated reviewers who found time from their busy schedule to review the articles submitted in this special issue. In addition, we are also grateful to all the authors for submitting and improving their papers.

References

1. Adat V, Gupta BB (2017) Security in internet of things: issues, challenges, taxonomy, and architecture. Telecommun Syst. https://doi.org/10.1007/s11235-017-0345-9
2. Al-Qurishi M, Rahman SMM, Hossain MS, Almogren A, Alrubaian M, Alamri A, Al-Rakhami M, Gupta BB (2017) An efficient key agreement protocol for Sybilprecaution in online social networks. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2017.07.055

3. Atawneh S, Almomani A, Al Bazar H et al (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimed Tools Appl 76(18):18451–18472
4. Dinh HT, Lee C, Niyato D, Wang P (2013) A survey of mobile cloud computing: architecture, applications, and approaches. Wirel Commun Mob Comput 13(18):1587–1611
5. Gai K, Qiu M, Zhao H (2017) Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing. IEEE Transactions on Big Data. https://doi.org/10.1109/TBDATA.2017.2705807
6. Gupta BB, Agrawal DP, Yamaguchi S (2016) Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global Publisher, USA
7. Ibtihal M, Hassan N (2017) Homomorphic Encryption as a Service for Outsourced Images in Mobile Cloud Computing Environment. Int J Cloud Appl Comput (IJCAC) 7(2):27–40
8. Jouini M et al (2016) A Security Framework for Secure Cloud Computing Environments. Int J Cloud Appl Comput (IJCAC) 6(3):32–44
9. Nagar N, Suman U (2016) Analyzing Virtualization Vulnerabilities and Design a Secure Cloud Environment to Prevent from XSS Attack. Int J Cloud Appl Comput (IJCAC) 6(1):1–14
10. Negi P, Mishra A, Gupta BB (2013) Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. International Journal of Computer Science Issues (IJCSI) 10(2) 142–146
11. Stergiou C, Kostas EP, Byung-Gyu K, Gupta B (2016) Secure integration of IoT and cloud computing. Future Generation Computer Systems. https://doi.org/10.1016/j.future.2016.11.031
12. Xiao Z, Yang X (2013) Security and privacy in cloud computing. IEEE Commun SurvTutorials 15(2):843–859
13. Yan Z, Xie H, Zhang P, Gupta BB (2017) Flexible data access control in D2D communications. Future Generation Computer Systems (2017). https://doi.org/10.1016/j.future.2017.08.052
14. Yu C , Jianzhong L, Xuan L, Xuechang R, Gupta BB (2017) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram." Multimedia Tools and Applications 1–24. https://doi.org/10.1007/s11042-017-4637-6
15. Zhang Z et al (2017) CyVOD: a novel trinity multimedia social network scheme. Multimed Tools Appl 76(18):18513–18529
16. Zkik K, Orhanou G, El Hajji S (2017) Secure Mobile Multi Cloud Architecture for Authentication and Data Storage. Int J Cloud Appl Comput (IJCAC) 7(2):62–76