Multimedia Tools and Applications (2018) 77:31517–31524
https://doi.org/10.1007/s11042-018-6426-2

GUEST EDITORIAL

Guest Editorial: Recent Advances on Security and Privacy of Multimedia Big Data in the Critical Infrastructure

B. B. Gupta[1] · Shingo Yamaguchi[2] · Zhiyong Zhang[3] · Konstantinos E. Psannis[4]

Published online: 2 August 2018

In recent years, cyber security and privacy is an essential need for modern society where information technology and services pervade every aspect of our lives. Specially, security and privacy of multimedia big data in the critical infrastructure (a nation's strategic national assets, i.e. banking and finance, communications, emergency services, energy, food chain, health, water, mass gatherings, transport, etc) which is an essential part of our daily life to access different systems, services and applications is a serious issue [4, 5, 7–9]. However, it is challenging to achieve, as technology is changing at rapid speed and our systems turn into ever more complex. The explosion of multimedia big data has created unprecedented opportunities and fundamental security 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 challenges and developments in multimedia big data in critical infrastructure from the perspective of providing security awareness and its best practices for the real world and also emphasizes many open questions [3, 10, 11, 13, 15]. We anticipate that papers of this special issue will open new entrance for further research and technology improvements in this important area. Papers were invited for this special issue considering aspects of this problem, including:

- Security and privacy of multimedia big data in banking systems
- Security and privacy of multimedia big data in telecommunication systems
- Security and privacy of multimedia big data in finance systems
- Security and privacy of multimedia big data in communication systems
- Security and privacy of multimedia big data in eCommerce
- Security and privacy of multimedia big data in emergency services, energy, food chain

✉ B. B. Gupta
bbgupta@nitkkr.ac.in

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

[2] Yamaguchi University, Yamaguchi, Japan

[3] Henan University of Science & Technology, Luoyang Shi, China

[4] University of Macedonia, Thessaloniki, Greece

- Security, privacy and forensics of multimedia big data in critical infrastructure
- Security and privacy of multimedia big data in mobile cloud computing
- Security and privacy management of big data in Cloud Computing
- Security and privacy of Industrial control systems
- Security, privacy and forensics of multimedia big data in stock trade
- Mobile cloud computing intrusion detection systems
- Cryptography, authentication, authorisation and usage control for big data in cloud
- Security and privacy of multimedia big data in smartphone devices
- Security of Mobile, peer-to-peer and pervasive services in clouds
- Security of big data in Mobile commerce and mobile internet of things
- Security and privacy of multimedia big data in sensor networks
- Big data-enabling social networks on Clouds
- Resource management for multimedia big data on Clouds
- Cryptography, authentication and authorisation for big data in mobile devices
- Security and privacy of multimedia big Data in Web service
- Evolutionary algorithms for mining social networks for decision support
- Artificial neural network and neural system applied to social media and mitigating the privacy risks in critical infrastructure

This special issue contains twenty-two papers focuses on security and privacy challenges and developments in multimedia big data in critical infrastructure and other related areas [1, 2, 6, 12, 14, 16] which were selected after rigorous review process. The first article entitled, "A multithreaded programming approach for multimedia big data: encryption system" (https://doi.org/10.1007/s11042-017-4873-9) authored by S. Aljawarneh, et al. presents a resource-efficient encryption algorithm system which applies the multithreaded programming process for the encryption of the big multimedia data. This proposed system describes a multi-level encryption model which uses the Feistel Encryption Scheme, genetic algorithms and the Advanced Encryption Standard (AES). Proposed system has been assessed for actual medical-based big multimedia data and compared to the benchmarked encryption algorithms like the RC6, MARS, 3-DES, DES, and Blowfish with regard to the computational run time and its throughput for the encryption and decryption procedures. In addition, the multithreaded programming approach is adopted to implement the proposed encryption system in order to enhance the system efficiency and performance. Furthermore, authors have also compared the proposed system with its sequential version for showing its resource efficiency. The results indicated that proposed system had the least run time and a higher throughput for the encryption and decryption processes in comparison to the already existing standard encryption algorithms. Also, the propsoed system could improve the computation run time by approximately 75% and its throughput was also increased by 4-times in comparison to its sequential version.

The second article entitled, "Privacy preserving security using biometrics in cloud computing" (https://doi.org/10.1007/s11042-017-4966-5) authored by, S. Kumar, et al. emphasizes on cloud security and privacy issues and provides the solution using biometric face recognition. Authors propose a biometrics face recognition approach for security and privacy preservation of cloud users during their access to cloud resources. The proposed approach has three steps: (1) acquisition of face images (2) preprocessing and extraction of facial feature (3) recognition of individual using encrypted biometric feature. The experimental results show that the proposed recognition approach can ensure the privacy and security of

biometrics data. The third article entitled, "A robust and efficient bilinear pairing based mutual authentication and session key verification over insecure communication" (https://doi.org/10.1007/s11042-017-4996-z) authored by Ruhul Amin, et al. presents an efficient scheme, which resolves all the existing problems in a pairing based session key agreement with user authentication scheme. The AVISPA simulation results on the propsoed scheme ensured that active and passive attacks are protected. The informal security discussion claims that the scheme resists all kinds of security attacks. Authors have shown that the performance of the proposed scheme is relatively superior in comparison with existing works. As an application area, anyone can execute this protocol in multimedia big data environment for making secure connection between the client and server.

The fourth article entitled, "A secure mutual authenticated key agreement of user with multiple servers for critical systems" (https://doi.org/10.1007/s11042-017-5078-y) authored by Azeem Irshad, et al. presents a multi-server authentication protocol that withstands below mentioned drawbacks of existing approaches using lightweight cryptographic operations: 1) free from storage of server-based parameters (public keys or other values) in smart card by registration authority, 2) free from the assumption of publishing of server-based public keys publicly and 3) free from a single secret sharing with all servers so that it could avoid server masquerading (insider) attack. The rationale of the proposed work was to present an efficient RC-Offline MSA scheme. Proposed scheme is also backed by formal security analysis based on GNY logic and automated security verification using ProVerif tool. The fifth article entitled, "Providing security and privacy to huge and vulnerable songs repository using visual cryptography" (https://doi.org/10.1007/s11042-017-5240-6) authored by S. Shivani, et al. presents a novel and efficient approach for providing security and privacy to huge and vulnerable songs repository using visual cryptography. Presented approach not only provides confidentiality to the songs but also provides integrity verification with access control to the songs repository. Authors have also removed various basic security constraints of (2, 2) visual cryptography existed in most of the state of art approaches like meaningless pattern of the shares, explicit codebook requirement, contrast loss, lossy recovery, etc. which are eliminated in the proposed approach. The sixth article entitled, "Secure data-exchange protocol in a cloud-based collaborative health care environment" (https://doi.org/10.1007/s11042-017-5294-5) authored by Mehedi Masud, et al. presents a two-phase security protocol that uses pairing-based cryptography in a cloud-based collaborative health care environment. Each cloud computes a secret session key dynamically by computing a pairing in an elliptic curve. Validating the presented protocol, a formal verification proves that the proposed protocol is robust and safe against the masquerade, man-in-the-middle, and replay attacks.

The seventh article entitled, "A code protection scheme by process memory relocation for android devices" (https://doi.org/10.1007/s11042-017-5363-9) authored by Xiaosong Zhang, et al. presents a code protection approach for Android devices which protects certain processes from memory acquisition by process memory relocation. The protected processes are relocated to the special memory area where the kernel is loaded, and thus these processes will be covered when android reboots and attackers cannot recognize which protected programs have been performed on the devices. The experiment results show that the proposed approach disables forensics tools like FROST to obtain these processes and has little impact on the normal operation of the protected program. Compared with the similar methods, the proposed method can protect greater data quantity but it occupies no additional storage resources. The eighth article entitled, "Semantic-integrated software watermarking with tamper-proofing" (https://doi.org/10.1007/s11042-017-5373-7) authored by Zhe Chen, et al. presents a

semantic-integrated watermarking with tamper-proofing to mitigate such problems. This work chooses neural network as the "integrator" and skillfully integrates the watermarking and tamper-proofing module into program semantics. The difficult of reverse engineering or tampering with watermarked program is equal to extracting the rules from neural networks, which had proven as a NP-hard problem. Authors have mentioned that they have deployed the proposed approach in SPECint-2006 benchmarks to evaluate the overhead, strength and resilience. Experiment results show that their proposed approach could effectively resist the state-of-the-art reverse engineering, and the introduced overhead is acceptable. The ninth article entitled, "User profiling for big social media data using standing ovation model" (https://doi.org/10.1007/s11042-017-5402-6) authored by Muhammad Al-Qurishi, et al. presents an integrative solution entailing a combination of the methodological advances within a single framework that could facilitate attribution and differentiate OSN members. Specifically, authors examined peer effects within Twitter and assessed the propensity of members to alter their views on commonly discussed matters based on their exposure to alternative views expressed by respected and influential members. Authors availed of abundant available resources and tracked historical interactions of selected users to create a workable model that captured differences in opinions. The resulting solution enables peer influence within the online environment to be quantified and the level of investment of identified social media users in particular topics to be assessed.

The tenth article entitled, "Running time analysis of the Pareto archived evolution strategy on pseudo-Boolean functions" (https://doi.org/10.1007/s11042-017-5466-3) authored by Xue Peng, et al. makes a first step toward studying the rigorous running time analysis for Pareto archived evolution strategy (PAES). Authors show that the PAES outperforms the simple evolutionary multi-objective optimizer (SEMO) on function PATH when the PAES uses a simple mutation operator. However, it cannot find the whole Pareto front with overwhelming probability on the well-studied function LOTZ. Additional experiments show that the experimental results are in agreement with the theoretical results. The eleventh article entitled, "Robust and efficient face recognition via low-rank supported extreme learning machine" (https://doi.org/10.1007/s11042-017-5475-2) authored by Tao Lu, et al. presents an efficient three-layered low-rank supported extreme learning machine (LSELM) algorithm for face recognition which improves the recognition performance under complex scenarios with high efficiency. In the first layer, a given probe sample is clustered into certain training subspace as pre-clustering. In the second layer, with this subspace, a low-rank subspace of probe sample as robust feature which is insensitive to disguise, noise, variant expression or illumination will be recovered by low-rank decomposition. Furthermore, these low-rank discriminative features are coded to support training a forward neural network termed LSELM. Experimental results indicate that the proposed approach is on par with some deep-learning based face recognition algorithms on recognition performance but with less time complexity over some popular face datasets e.g., AR, Extend Yale-B, CMU PIE and LFW datasets. In the twelfth article entitled, "Privacy preservation based on clustering perturbation algorithm for social network" (https://doi.org/10.1007/s11042-017-5502-3) authored by Fahong Yu, et al., a clustering perturbation algorithm to preserve privacy for social network was proposed considering preservation privacy of vertices properties and community structures simultaneously. The proposed algorithm introduced a strategy of exchanging attributes between vertices with same degree randomly to induce attackers to search for false targets and maintain whole structure of network. Furthermore, a perturbation strategy with tiny influences based on local clustering and modifying edges complementarily was adopted to decrease the risk of privacy

disclosure considering minimum loss of network structure and data information. The experimental results showed that the proposed algorithm has more advantages over other existing state-of-the-art approaches in privacy preservation and effectiveness of social network.

The thirteenth article entitled, "A component-driven distributed framework for real-time video dehazing" (https://doi.org/10.1007/s11042-017-5518-8) authored by Meihua Wang, et al. presents a new framework, particularly designed for video dehazing, to output coherent results in real time, with two novel techniques. Firstly, authors decompose the dehazing algorithms into three generic components, namely transmission map estimator, atmospheric light estimator and haze-free image generator. They can be simultaneously processed by multiple threads in the distributed system, such that the processing efficiency is optimized by automatic CPU resource allocation based on the workloads. Secondly, a cross-frame normalization scheme is proposed to enhance the coherence among consecutive frames, by sharing the parameters of atmospheric light from consecutive frames in the distributed computation platform. The combination of the above three components enables the propsoed framework to generate highly consistent and accurate dehazing results in real-time, by using only 5 PCs connected by Ethernet. The fourteenth article entitled, "An effective information detection method for social big data" (https://doi.org/10.1007/s11042-017-5523-y) authored by Jinrong He, et al. presents a decision graph based outlier detection (DGOD) method for social big data. The DGOD method works by firstly calculating the decision graph score (DGS) for each sample, where the DGS is defined as ratio between discriminant distance and local density, next ranking samples according to their DGS values, and finally, returning samples with top-r largest DGS values as outliers. Experimental results on synthetic and real-world datasets have confirmed its effectiveness on outlier detection problems, and it is a general and effective information detection method, which is robust to data shape and dimensionality. The fifteenth article entitled, "Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem: revisited" (https://doi.org/10.1007/s11042-017-5535-7) authored by Zhimin Yu, et al. presents an analysis which demonstrates that regardless of whether the private key is weak key or not, the equivalent keys from an associated public key can be solved in a reasonable time by a linear algebra attack. For this purpose, the linear equations with coefficients $n^2 \times n^2$ are needed to solve. The equation coefficients are much less than the coefficients $5n^2 \times 2n^2$ in the attack methods of Liu et al. Thus, the proposed attack method is not only more general and but also more efficient.

In the sixteenth article entitled, "Video abstract system based on spatial-temporal neighborhood trajectory analysis algorithm" (https://doi.org/10.1007/s11042-017-5549-1) authored by Han Huang, et al., a video abstract system based on spatial-temporal neighborhood trajectory analysis algorithm which is mainly used to process surveillance videos is proposed. The algorithm uses the spatial adjacency of foreground targets and tracks the spatial-temporal neighboring moving targets to get their whole trajectories in order to meet the requirement of processing speed and accuracy. The indicators consist of trajectory detection rate, trajectory tracking average continuity and video abstract processing speed are used to evaluate the effectiveness of the system. Authors compare the algorithm with the other three algorithms, and the results show that spatial-temporal neighborhood trajectory analysis algorithm has sufficient trajectory detection rate and processing speed for surveillance video abstraction. The seventeenth article entitled, "A new validity index adapted to fuzzy clustering algorithm" (https://doi.org/10.1007/s11042-017-5550-8) authored by Wei Li, et al. presents an improved validity index for the comprehensive weight index, compactness index and separability index. This validity index first determines the relationship between the features of the data points and the data point itself. By defining the

new compactness function and the separability function, the weight of each feature in the data set is obtained, and then the validity index is combined with the fuzzy c-means clustering algorithm to effectively determine the number of classes to be processed. The proposed algorithm is tested on two artificial data sets and real data sets; the experimental results demonstrated the advantages of this work in image processing and showed that it can effectively obtain reliable data classification results. The eighteenth article entitled, "Specular reflection removal of ocean surface remote sensing images from UAVs" (https://doi.org/10.1007/s11042-017-5551-7) authored by Shengke Wang, et al. presents a method to remove the specular reflection on the RGB images of ocean surface. The intensity of specular highlight components is much larger than that of diffuse components in the images, simply subtracting the highlight component form the original image will leave a lot of holes. Therefore, the proposed method contains two main steps: highlight regions detection and restoration of those regions. Authors use the method based on the intensity ratio to extract the regions affected by the specular reflection. Then, they use the local information around those highlight regions to restore the intensity of those pixels. The experimental results indicate that the proposed method can effectively remove the specular reflection and keep details of ocean surface images.

The nineteenth article entitled, "Implicit authentication protocol and self-healing key management for WBANs" (https://doi.org/10.1007/s11042-017-5559-z) authored by Jian Shen, et al. presents a lightweight implicit authentication protocol based on the Elliptic Curve Qu-Vantone (ECQV) algorithm. Moreover, author take advantage of the bidirectional key chain to design a group key management protocol between the personal digital assistance (PDA) and each of cluster head sensor nodes. The security and performance analysis show that proposed protocol can be performed with perfect forward security and backward security in data communication. In addition, the experimental simulation and theoretic analysis show that the proposed protocol is more suitable for WBANs. The twentieth article entitled, "A hierarchical representation for human action recognition in realistic scenes" (https://doi.org/10.1007/s11042-018-5626-0) authored by Qing Lei, et al. presents two-layer hierarchical codebook learning framework for human action classification in realistic scenes. In the first-layer action modelling, superpixel GMM model is developed to filter out noise features in STIP extraction resulted from cluttered background, and class-specific learning strategy is employed on the refined STIP feature space to construct compact and descriptive in-class action codebooks. In the second-layer of action representation, LDA-Km learning algorithm is proposed for feature dimensionality reduction and for acquiring more discriminative inter-class action codebook for classification. Authors take advantage of hierarchical framework's representational power and the efficiency of BoF model to boost recognition performance in realistic scenes. In experiments, the performance of the propsoed method is evaluated on four benchmark datasets: KTH, YouTube (UCF11), UCF Sports and Hollywood2. Experimental results show that the proposed approach achieves improved recognition accuracy than the baseline method. Comparisons with state-of-the-art works demonstrates the competitive ability both in recognition performance and time complexity.

The twenty first article entitled, "An improved method for detection of the pedestrian flow based on RFID" (https://doi.org/10.1007/s11042-017-5303-8) authored by Yuanyuan Fan, et al. presents a method of crowd flow detecting based on RFID by analyzing the factors affecting the RFID link state. The system composed of the RFID tag arrays and the reader which detects the pedestrian flow according to the counts and the RSSI value of reading RFID tag arrays. With the evaluation in different scenarios, the coverage and moving status of the crowd can be verified. The twenty second article entitled, "Containerized resource

provisioning framework for multimedia big data application" (https://doi.org/10.1007/s11042-017-5366-6) authored by Ye Tao, et al. presents fuzzy-logic-based approaches to simplify the user preferences representation and automate the processes of container environment setup. By using fuzzy inference techniques, the approach allows users to define non-quantifiable factors and policies to represent their preferences, and automatically converts the vague requirements to numeric parameters and runtime deployment. Compared to classical methods, the proposed approach presents only the information relevant to user's requirements and preferences. The validation results show that with appropriate customization steps and natural interfaces, user preferences can be reflected effectively in the final configurations of containers. Furthermore, a fuzzy-logic-based schedule algorithm for global container resource allocation is also proposed, and the effectiveness of the provisioning policies are validated by sample use cases. The twenty third article entitled, "Big network traffic data visualization" (https://doi.org/10.1007/s11042-017-5495-y) authored by Zichan Ruan, et al. presents a novel and effective method for visualizing network traffic data with statistical features of high dimensions. Authors combine Principal Component Analysis (PCA) and Mutidimensional Scaling (MDS) to effectively reduce dimensionality and use colormap for enhance visual quality for human beings. Authors obtain high quality images on a real-world network traffic dataset named 'ISP'. Comparing with the popular t-SNE method, proposed visualization method is more flexible and scalable for plotting network traffic data which may require to preserve multi-dimensional information and relationship. Plots also demonstrate the capability of handling a large amount of data. Using the propsoed method, the readers will be able to visualize their network traffic data as an alternative method of t-SNE.

We would like to express our special thanks to Prof. Borko Furht, the Editor-in-Chief of Multimedia Tools and Applications (MTAP) 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 MTAP 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 et al (2017) Security in internet of things: issues, challenges, taxonomy, and architecture. Telecommun Syst 1–19
2. Bhuiyan MZA, Wu J, Wang G, Cao J (2016) Sensing and decision-making in cyber-physical systems: the case of structural health monitoring. IEEE Trans Ind Inf 12(6):2103–2114
3. Gao C-z, Cheng Q, He P, Susilo W, Li J (2018) Privacy-preserving naive Bayes classifiers secure against the substitution-then-comparison attack. Inf Sci. https://doi.org/10.1016/j.ins.2018.02.058
4. Gupta BB, Akhtar T (2017) A survey on smart power grid: frameworks, tools, security issues, and solutions. Ann Telecommun 72(9-10):517–549
5. Gupta BB, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global Publisher, USA
6. 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

7. Jiang F, Fu Y, Gupta BB, Lou F, Rho S, Meng F, Tian Z (2018) Deep learning based multi-channel intelligent attack detection for data security. IEEE Trans Sustain Comput. https://doi.org/10.1109/TSUSC.2018.2793284
8. Keeney M, Kowalski E, Cappelli D, Moore A, Shimeall T, Rogers S (2005) Insider threat study: computer system sabotage in critical infrastructure sectors. National Threat Assessment Ctr Washington Dc
9. Li T, Li J, Liu Z, Li P, Jia C (2018) Differentially private naive Bayes learning over multiple data sources. Inf Sci 444:89–104
10. Li J, Sun L, Yan Q, Li Z, Srisa-an W, Ye H (2018) Significant permission identification for machine learning based android malware detection. IEEE Trans Ind Inf. https://doi.org/10.1109/TII.2017.2789219
11. Li J, Sun L, Yan Q, Li Z, Srisa-an W, Ye H Significant permission identification for machine learning based android malware detection. In IEEE transactions on industrial informatics. IEEE. https://doi.org/10.1109/TII.2017.2789219
12. Li J, Chen X, Chow SSM, Huang Q, Wong DS, Liu Z Multi-authority fine-grained access control with accountability and its application in cloud. J Netw Comput Appl. https://doi.org/10.1016/j.jnca.2018.03.006
13. 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
14. Stergiou C et al (2016) Secure integration of IoT and cloud computing. Futur Gener Comput Syst
15. Zhang Z et al (2016) Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems, Elsevier
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