Future Generation Computer Systems 133 (2022) 169–170

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Editorial

Preface of special issue on Artificial Intelligence: The security & privacy opportunities and challenges for emerging applications

Qin Liu [a,*], Guojun Wang [b], Jiankun Hu [c], Jie Wu [d]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan Province, 410082, PR China
[b] School of Computer Science, Guangzhou University, Guangzhou, Guangdong Province, 510006, PR China
[c] School of Engineering and IT, University of New South Wales, ACT 2600, Australia
[d] Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA

ARTICLE INFO

Article history:
Available online 17 March 2022

Keywords:
Preface
Artificial intelligence
Security
Privacy
Emerging applications

ABSTRACT

With the increasing awareness of data security in emerging applications, Artificial Intelligence (AI)-enabled security mechanism has begun to receive growing attention. This special issue assembles a set of 14 papers, which provide in-depth research results to report the advance of security and privacy in AI and AI-enabled secure emerging applications. This preface provides an overview of all articles.

In recent years, the collection, processing, and analysis of personal data have become greatly convenient and widespread, as the continuous advancement of emerging applications such as social networks, Internet of Things (IoT), and cloud computing. This also makes sensitive information more vulnerable to abuses, and thus secure mechanisms and technologies tailored for emerging applications need to be explored urgently [1,2].

Artificial Intelligence (AI) with the benefits of enhancing efficiency and improving accuracy has been widely used in academia and industry [3]. From a privacy and security angle, AI brings about both opportunities and challenges for emerging applications. On the one hand, AI can help interested parties to better protect privacy in challenging situations, improving the state-of-the-art of security solutions. On the other hand, AI also presents risks of opaque decision making, biased algorithms, and safety vulnerabilities, challenging traditional notions of privacy protection.

The purpose of this special issue is to bring together researchers and practitioners working on network security and AI communities to present their recent researches and applications, and also to show how to seize opportunities and overcome challenges brought about by AI in security and privacy of emerging applications. After a thorough review process, this special issue has selected a set of 14 papers, which provide new insights on the above-mentioned research areas.

Zhang et al. [4] propose a distributed edge Quality of Service(QoS) prediction with privacy-preserving model (DEQP2) in edge computing networks. Based on this model, they design a distributed edge differential privacy QoS prediction algorithm to provide a comprehensive consideration for the influence of user preferences and the edge environment. The experimental results show that DEQP2 provides measurable privacy preservation without significantly reducing the accuracy.

Aguilar et al. [5] propose a pattern-based classifier for one-class classification problems, PBC4occ. Besides, they introduce the first contrast pattern mining algorithm utilizing decision trees for one-class classification. The comparable experiments show that PBC4occ achieves the best average value for both area under the curve (AUC) and equal error rate (EER) metrics.

Yang et al. [6] design a privacy-and-integrity-protecting density peaks clustering algorithm in the ciphertext domain (PIDPC). Specifically, PIDPC leverages BFV homomorphic encryption and order-preserving encryption to achieve batch homomorphic operations and ciphertext comparisons, respectively. In addition, they design three optimization algorithms to improve efficiency. Extensive experiments demonstrate that PIDPC guarantees clustering accuracy while ensuring the privacy of training data and the integrity of returned results.

Chen et al. [7] focus on ℓ_0-norm attacks in the deep neural network. To improve the performance of classifying low quality images, they propose a method named space transformation pixel defender (STPD) to transform an image into a latent space and separate the perturbed pixels from the normal pixels. The results on three real datasets show that STPD can effectively defend against ℓ_0-norm attacks.

Ren et al. [8] propose a privacy-protected intelligent crowdsourcing scheme based on reinforcement learning (PICRL). PICRL

* Corresponding editor.
E-mail address: gracelq628@126.com (Q. Liu).

https://doi.org/10.1016/j.future.2022.03.021
0167-739X/

selects appropriate participants without knowing the environment of the sensing model by utilizing Q-learning. In addition, PICRL provides effective trust evaluation by considering privacy trust, crowd trust, and hybrid active trust. Extensive simulation experiments verify the effectiveness of the proposed PICRL.

Wu et al. [9] propose a malicious user detection method based on the Hidden Markov Model in the crowdsensing system. The proposed method takes users' observations as input and reports malicious users with the assistance of a pre-detection phase. Besides, the authors present an anti-malicious task allocation mechanism to prevent malicious users from taking assignments. Experimental results show that the proposed detection algorithm can identify malicious users with high accuracy.

Wu et al. [10] propose a federated learning scheme by combining the adaptive gradient descent strategy and differential privacy mechanism. The proposed scheme is suitable for multi-party collaborative modelling scenarios. Experimental results demonstrate that the proposed scheme performs better than the traditional models under fixed communication costs.

Bugshan et al. [11] propose a differential privacy model that suites Radial Base Function Network (RBFN). They utilize a Gaussian mechanism to perturb the hidden layer gradients during the training phase to minimize privacy leakage. Furthermore, they fine-tuned the hyperparameters and noise coefficient to achieve a reasonable tradeoff. Experiments results on five datasets of differing distributions show that accuracy degradation is minimal when the dataset has high intra-class variation.

Haseeb et al. [12] propose an Autoencoder (AE)-based feature construction approach to determine the behavioural patterns of IoT attacks. Their approach removes the dependency of manually correlating commands and generates an efficient representation by automatically learning the semantic similarity. Evaluation results show that the proposed approach has high accuracy in determining IoT attacks.

Tang et al. [13] propose a method based on data mining technology to detect Low-rate Denial of Service (LDoS) attacks. Moreover, they summarize three abnormal features of the network under LDoS attacks. The results from the experimental simulation verify that the developed method can effectively detect LDoS attacks with optimal detection cost and high accuracy.

Jangra et al. [14] propose two hide sensitive high utility itemsets (SHUIs) hiding algorithms, MinMax and Weighted, to improve the data utility by minimizing the misses cost. Experiments on various datasets show that the proposed algorithms perform better than the existing SHUIs hiding algorithms, resulting in fewer distortions of non-sensitive knowledge.

Xu et al. [15] research the problem of secure and verifiable federated learning. They propose a NIVP-DS scheme based on the dual-server model and random matrix coding. In order to realize verifiability, the authors introduce a cross-verification method based on credible matrix exchange. The experiment results verify the effectiveness of the proposed scheme.

Tang et al. [16] focus on detecting the variant of Android malware obfuscation. They propose an Android malware detection system MGOPDroid, which can be deployed on mobile devices to support real-time monitoring and detecting application. Compared with the previous methods, MGOPDroid has obvious advantages in the efficiency of anti-obfuscation.

Croft et al. [17] focus on the privacy protection of images. They propose a facial identity obfuscation method that applies differential privacy to image encodings in a generative adversarial network. In addition, they use principal component analysis to control the magnitude of noises in order to achieve a favourable trade-off between privacy and utility. The comparison experiments demonstrate the effectiveness of their approach.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Q. Liu, Y. Tian, J. Wu, T. Peng, G. Wang, Enabling verifiable and dynamic ranked search over outsourced data, IEEE Trans. Serv. Comput. 15 (1) (2022) 69–82.
[2] Q. Liu, Y. Peng, J. Wu, T. Wang, G. Wang, Secure multi-keyword fuzzy searches with enhanced service quality in cloud computing, IEEE Trans. Netw. Serv. Manag. 18 (2) (2021) 2046–2062.
[3] Q. Liu, J. Yang, H. Jiang, J. Wu, T. Peng, T. Wang, G. Wang, When deep learning meets steganography: Protecting inference privacy in the dark, in: IEEE INFOCOM 2022 - IEEE Conference on Computer Communications, 2022.
[4] Y. Zhang, J. Pan, L. Qi, Q. He, Privacy-preserving quality prediction for edge-based IoT services, Future Gener. Comput. Syst. 114 (2021) 336–348.
[5] D.L. Aguilar, O. Loyola-González, M.A. Medina-Pérez, L. Cañete-Sifuentes, K.-K.R. Choo, PBC4occ: A novel contrast pattern-based classifier for one-class classification, Future Gener. Comput. Syst. 125 (2021) 71–90.
[6] H. Yang, S. Liang, Y. Zhang, X. Li, Cloud-based privacy- and integrity-protecting density peaks clustering, Future Gener. Comput. Syst. 125 (2021) 758–769.
[7] J. Chen, J. Cao, Z. Liang, X. Cui, L. Yu, W. Li, STPD: Defending against ℓ_0-norm attacks with space transformation, Future Gener. Comput. Syst. 126 (2022) 225–236.
[8] Y. Ren, W. Liu, A. Liu, T. Wang, A. Li, A privacy-protected intelligent crowdsourcing application of IoT based on the reinforcement learning, Future Gener. Comput. Syst. 127 (2022) 56–69.
[9] X. Wu, Y.-E. Sun, Y. Du, G. Gao, H. Huang, X. Xing, An anti-malicious task allocation mechanism in crowdsensing systems, Future Gener. Comput. Syst. 127 (2022) 347–361.
[10] X. Wu, Y. Zhang, M. Shi, P. Li, R. Li, N.N. Xiong, An adaptive federated learning scheme with differential privacy preserving, Future Gener. Comput. Syst. 127 (2022) 362–372.
[11] N. Bugshan, I. Khalil, N. Moustafa, M. Almashor, A. Abuadbba, Radial basis function network with differential privacy, Future Gener. Comput. Syst. 127 (2022) 473–486.
[12] J. Haseeb, M. Mansoori, Y. Hirose, H. Al-Sahaf, I. Welch, Autoencoder-based feature construction for IoT attacks clustering, Future Gener. Comput. Syst. 127 (2022) 487–502.
[13] D. Tang, J. Chen, X. Wang, S. Zhang, Y. Yan, A new detection method for LDoS attacks based on data mining, Future Gener. Comput. Syst. 128 (2022) 73–87.
[14] S. Jangra, D. Toshniwal, Efficient algorithms for victim item selection in privacy-preserving utility mining, Future Gener. Comput. Syst. 128 (2022) 219–234.
[15] Y. Xu, C. Peng, W. Tan, Y. Tian, M. Ma, K. Niu, Non-interactive verifiable privacy-preserving federated learning, Future Gener. Comput. Syst. 128 (2022) 365–380.
[16] J. Tang, R. Li, Y. Jiang, X. Gu, Y. Li, Android malware obfuscation variants detection method based on multi-granularity opcode features, Future Gener. Comput. Syst. 129 (2022) 141–151.
[17] W.L. Croft, J.-R. Sack, W. Shi, Differentially private facial obfuscation via generative adversarial networks, Future Gener. Comput. Syst. 129 (2022) 358–379.