We are IntechOpen,
the world's leading publisher of Open Access books
Built by scientists, for scientists

6,600
Open access books available

178,000
International authors and editors

195M
Downloads

154
Countries delivered to

Our authors are among the

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

BOOK CITATION INDEX CLARIVATE ANALYTICS INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Introductory Chapter: Data Privacy Preservation on the Internet of Things

Jaydip Sen and Subhasis Dasgupta

1. Introduction

Recent developments in hardware and information technology have enabled the emergence of billions of connected, intelligent devices around the world exchanging information with minimal human involvement. This paradigm, known as the Internet of Things (IoT), is progressing quickly, with an estimated 27 billion devices by 2025 (almost four devices per person) [1, 2]. These smart devices help improve our quality of life, with wearables to monitor health, vehicles that interact with traffic centers and other vehicles to ensure safety, and various home appliances offering comfort. This increase in the number of IoT devices and successful IoT services has generated tremendous data. The International Data Corporation report estimates that by 2025 this data will grow from 4 to 140 zettabytes [3].

However, this humongous volume of data poses growing concerns for user privacy. Gartner predicts approximately 15 billion connected devices will be linked to computing networks by 2022 [4]. These gadgets could be vulnerable, and the massive amounts of unsecured online data create a liability. In addition, users having difficulty controlling the data from their devices has highlighted privacy as a major issue. To guarantee high levels of user data protection, IoT systems must adhere to regulations such as the European Union's *general data protection regulation* (GDRP) of 2018 [5]. GDPR is a law enacted in the European Union that specifies rules for how organizations and companies must use personal data without violating their integrity. These regulation policies focus on giving users control over what is collected, when, and for what purpose. By 2023, the regulators will demand organizations protect consumer privacy rights for more than 5 billion citizens and comply with more than 70% of the GDPR requirements [5].

Traditional privacy protection schemes are insufficient for IoT applications which necessitate new techniques such as distributed cybersecurity controls, models, and decisions that take into account vulnerabilities in system development platforms as well as malicious users and attack surfaces. Machine learning techniques can provide improved detection of novel cyberattacks when dealing with large volumes of data in IoT systems. Furthermore, they can enhance how sensitive data are shared between components to keep them secure. Machine learning-based schemes thus improve the operations related to privacy protection and more

effectively comply with the regulations. This chapter presents a survey on the currently existing machine learning-based approaches for the privacy preservation of data in the IoT.

The rest of the chapter is organized as follows. Section 2 identifies some of the existing surveys on the privacy preservation of data in the IoT. Section 3 discusses current privacy schemes for IoT based on a centralized architecture. Section 4 highlights the existing schemes working on the principles of distributed learning. In Section 5, some well-known privacy schemes on distributed encryption mechanisms are discussed. The concept of differential privacy and some schemes working on this principle are presented in Section 6. Finally, the chapter is concluded in Section 7, highlighting some emerging trends in the field of privacy in the IoT.

2. Some existing survey works on privacy issues in the IoT

In the literature, several studies have reviewed privacy issues in IoT environments, focusing mostly on threats and attacks on such systems. A comprehensive survey is carried out on various threat models and the classification of various attack types in the context of IoT [6]. The study found that the training dataset used for building the machine learning model for designing the privacy protection system is the most vulnerable to attack. Other sensitive assets are the model, the parameters and hyper-parameters involved, and the model architecture. On the other hand, the sensitive actors are the owners of data, the owners of the model, and the users of the model. Another important observation of this study is that among the machine learning models, the ordinary least square regression model, decision tree, and support vector machine model are the most vulnerable ones. Another recently published paper presented a comprehensive survey on various machine learning and deep learning-based approaches used for protecting user data privacy in the IoT [7].

Many surveys focus on reviewing the mechanisms and models for preserving data privacy. Various issues include differential privacy, homomorphic encryption, and learning architectures and models. In one study, the threats and vulnerabilities of privacy protection systems in IoT are classified into four groups (i) attacks on authentication, (ii) attacks on the components of edge computing, (iii) attacks on the anatomization and perturbation schemes, and (iv) attacks on data summarization [8]. In another survey work, the existing privacy protection systems with centralized architectures and machine learning approaches are analyzed by categorizing the data generated at different layers [9]. Kounoudes and Kapitsaki [10] analyzed several privacy-preservation solutions to determine basic characteristics. The authors proposed a mix of machine learning techniques for providing user protection, along with the policy languages to set user privacy preferences and negotiation techniques that improve services while preserving user rights. Zhu et al.'s survey work included several approaches, including differential privacy, secure multi-party computing, and homomorphic encryption for training models [11]. The authors classified the models based on collaborative or aggregated scenarios to protect user identity or information. Ouadrhiri et al. analyzed the current methods within federated learning environments classifying them into three distinct groups: (i) k-anonymity, (ii) l-diversity, and (iii) t-closeness to protect datasets [12]. The authors also observe that differential privacy-based technologies are

mostly used for training the privacy models. This approach, however, suffers from a high computational complexity for the encryption and decryption operations.

3. Centralized architecture-based encryption schemes

The data privacy mechanisms and systems under this category use encryption techniques such as homomorphic encryption, attribute access control, multi-party computation, and lightweight cryptography. These approaches are usually resource hungry and involve high computational resources and large memory spaces. On the other hand, homomorphic encryption systems provide a very high level of privacy even when deployed in third-party computations. Researchers designed several variants of homomorphic encryption systems such as partially homomorphic and somewhat homomorphic encryption [13–15]. While somewhat homomorphic encryption systems minimize communication overhead by using a smaller key size, partially homomorphic encryption systems are suitable for lightweight protocols of IoT since they yield shorter ciphertexts.

In building privacy models, the modelers encounter a difficult challenge. While data owners do not want what to expose their sensitive information to untrusted and potentially malicious models, the model owners prefer not to share information about their models as they are valuable assets. As such, classification protocols utilize machine learning classifiers over encrypted data to protect privacy on both sides. Bost et al., De Cock et al., Rahulamathavan et al., Wang et al., Zhu et al., and Jiang et al. all proposed several protocols for privacy-preserving classification using different datasets and models including hyperplane decision, naive Bayes, decision trees, support vector machines, multilayer extreme learning machine among others. These models have yielded an accuracy of results varying between 86% and 98% [16–21]. These efforts also reduce training and execution times compared to traditional deep learning models like convolutional neural networks.

4. Distributed learning-based solutions

Of late, privacy protection of data using distributed machine learning [22, 23] has gained considerable popularity in the context of the IoT. Distributed machine learning allows the learning models to be generated at each participant device, while the central server acting as the coordinator, creates a global model and distributes the knowledge to the participating nodes. Shokri and Shmatikov proposed a collaborative computing system that works on deep learning to protect a user's sensitive data while utilizing the information content of nonsensitive data of other users in the system [22]. The deep learning algorithms use the stochastic gradient descent algorithm because of the parallelization and asynchronous execution capability of the latter. The privacy model yields a very high accuracy on the test dataset. A distributed learning-based mechanism for data privacy preservation on IoT devices is proposed by Servia-Rodriguez et al. [23]. The scheme does not involve any data communication to the cloud environment. The system works in two phases. In the first step, the model is trained on data voluntarily shared by some users and possibly not containing any privacy-sensitive information. Once the model is trained, no further user data are shared. The model, tested on a public dataset, yields high accuracy. This scheme assumes user data privacy preservation since the original data

never leaves their device. However, this is incorrect as the distributed machine learning models are vulnerable to privacy inference attacks that attempt to access privacy-sensitive data or model inversion attacks recovering original data [24, 25]. This enforces protection techniques such as encryption or differential privacy into distributed learning systems.

5. Distributed learning and encryption

Encryption techniques are integrated into distributed machine learning to boost data privacy in IoT applications. The most commonly used encryption method used is homomorphic encryption, in which the user data is encrypted before being sent to the computing nodes. A privacy protection system has been proposed based on the joint operation of a multilayer perceptron and a convolutional neural network model [26]. The model has been tested on the *modified national institute of standards and technology* (MNIST) and *street view house number* (SVHN) datasets [27]. A secure information system for healthcare applications in the IoT environment has been proposed [28]. The proposed model uses Pallier additive homomorphic encryption [29]. Another privacy system based on the Pallier system has been presented that works on blockchain technology [30]. The authors tested the system on two datasets of the University of California, Irvine (UCI) data repository [31, 32]. Homomorphic encryption systems offer increased privacy compared to differential privacy-based ones. However, fully homomorphic encryption can be costly in terms of computation overload, while partial homomorphic encryption can only be used for carrying out single operations. Moreover, partial homomorphic encryption methods require trusted third parties in place, or they work on simpler models approximating complex equations using single mathematical operations. A mechanism is proposed for protecting the privacy of data for the Industrial Internet of Things (IIoT) built on the principles of distributed learning [33]. The scheme works on a variational autoencoder model trained using homomorphic encryption. The accuracy of the model is found to be high, while its execution time is low. A hybrid framework for privacy protection is proposed by Osia et al. [34]. The scheme utilizes Siamese architecture and can perform efficient privacy-preserving analytics splitting a neural network IoT devices and cloud [35]. The feature extraction is done at the device, while the classification is carried out in the cloud. The scheme uses a convolutional neural network model evaluated with gender classification datasets *Internet movie database* (IMDB-Wiki) [36] and *labeled faces in the wild* (LFW) [37], achieving an accuracy of 94% and 93%, respectively. A data privacy-preserving scheme known named CP-ABPRE is presented by Zhou et al. that works on a policy-based encryption approach [38]. The scheme is found to be robust against privacy attacks and has a low computational overhead required for its encryption and decryption processes.

6. Distributed learning and differential privacy

In the differential privacy approach, the privacy of data is protected through the addition of some random perturbations into the original data. In other words, a perturbation in the data is done with a predetermined measure of the error caused by modifications to the data [39]. Several well-known techniques of perturbation include swapping, randomized response, micro-aggregation, additive perturbation, and condensation. However, perturbations reduce the quality of the data for analysis as

the original data are modified. Privacy models work on a trade-off between the utility of data and its associated privacy level. In the privacy-utility trade-off, several algorithms and approaches exist in the literature. In the context of differential privacy, Abadi et al. presented a scheme involving training a neural network with differential privacy to prevent the disclosure of sensitive information [40]. The scheme is proved to be highly effective in preserving the privacy of sensitive data, as observed from its performance on the test dataset. Another scheme for privacy preservation of sensitive data is proposed in which a subset of parameters is shared and obfuscated using differential privacy as the training of the deep learning structures is carried out locally [41]. While the differential privacy-based schemes do not need high computational resources, they may be inaccurate since perturbations can reduce training quality. Moreover, these schemes cannot fully protect data privacy (i.e., there is always a trade-off between the model's accuracy-privacy). Wang et al. [42] enhanced the performance of the distributed machine learning system with differential privacy in an IoT environment via their Arden framework [42]. The scheme proposed by the authors involves protecting sensitive information using nullification or noise addition [27]. The model is tested on the MNIST/SVHN datasets and has yielded high accuracy while considerably reducing resource consumption [27]. The scheme proposed by Zhang et al. focused on distributed sensing systems where an obfuscate function was used to preserve training data privacy when shared with third parties [43].

Lyu et al. proposed a privacy mechanism using the random projection method to perturb the original data and embedding fog computing into deep learning [44]. This scheme is able to reduce communication overhead and computation load. The novel method of privacy protection, known as the fog-embedded privacy-preserving deep learning framework, can preserve the privacy of data using a robust defense method. First, a random perturbation is used to preserve the original data's statistical characteristics. Then, differentially private stochastic gradient descent is used to train the fog-level models with a multilayer perceptron model. The multilayer perceptron model consists of two hidden layers equipped with the *rectified linear unit* (ReLU) activation function. The accuracy yielded by the scheme on the test data is quite acceptable, although it is slightly lower compared to models with centralized architecture. However, the communication and computation overheads are significantly reduced.

Some privacy-preservation schemes utilize Gaussian projections to implement collaborative learning environments [45] efficiently. In these schemes, the resource-constrained IoT devices participate collaboratively and randomly apply multiplicative Gaussian projections on the training data records. This process obfuscates the privacy-sensitive input data. The coordinator node applies a deep learning-based model to learn from the complex patterns of the obfuscated data supplied by the Gaussian random projections. The performance results of the scheme demonstrated its efficiency and effectiveness in data privacy protection.

Among other approaches, obfuscation-based methods are also used in distributed machine learning to control the computation overhead involved in the encryption procedures in massively large-sized data. A scheme proposed by Alguliyev et al. protects big data in the context of IoT [46]. The mechanism involves the transformation of sensitive data into data that can be publicly shared. The proposed method works in two phases. In the first phase, data is transformed through a denoising type autoencoder. The parameter for designating the sparsity parameter of the autoencoder is specified for minimizing the loss in the autoencoder objective function during the data compression process. In the second phase, the transformed data from the output

of the denoising autoencoder is classified using a convolutional neural network model. The proposed scheme was tested on several disease datasets and was found to be highly accurate in its prediction. Du et al. proposed a novel privacy-preserving scheme for big data in IoT deployed in edge computing applications [47]. The mechanism is based on a differential privacy approach built on machine learning models, which can improve query accuracy while minimizing the exposure of sensitive data to the public. The working mechanism involves two steps. In the first step, a Laplacian noise is added to the output data to carry out perturbation, while in the second step, random noise is added to the objective function that reduces the disturbance to the objective values. The data perturbation is carried out before transferring the data to the edge nodes. The model is tested on four diverse datasets and is found to be highly accurate in its performance. The machine learning models used in the scheme are stochastic gradient descent and generative adversarial networks.

Speech recognition systems, commonly found in IoT services, are susceptible to breaching user privacy as voice information is generally transmitted as plaintext and sometimes used for authentication purposes. To address this issue, Rouhani et al. proposed a scheme called *deepsecure* [48]. The working principle of the scheme is based on the garbled circuit protocol of Yao [49], and it executes much faster than the homomorphic encryption-based schemes. However, the proposition suffers from issues related to reusability and difficulty in implementation [50]. Differential privacy has been utilized in work by adding perturbations to user data [40]. However, the proposed scheme has a lower level of accuracy. Ma et al. [51] have thereby improved upon this by proposing a secret-sharing-based method that improves accuracy and reduces the computation and communication overhead for both linear and nonlinear operations using a long-and-short-term memory network model with interactive protocols for each gate. The proposed scheme was tested on a private dataset yielding a very high accuracy. Although privacy-preservation approaches based on obfuscation methods, in most cases, overcome the shortcomings of distributed machine learning and encryption-based distributed machine learning methods, these schemes are found to be vulnerable to some attacks [52–54].

7. Conclusion

This introductory chapter has presented a brief survey of some of the existing data privacy-preservation schemes proposed by researchers in the field of the Internet of Things. However, the design of privacy protection schemes in resource-constrained devices is still in its early stages. Reducing the latency and throughput of neural network training on encrypted data for privacy protection is a big challenge. Most of the existing schemes deploy their deep learning tasks to some external resources with adequate computing resources and storage spaces while keeping user data protected, making the schemes computationally efficient. New approaches should explore alternatives, such as quantum computing techniques, for designing more efficient and precise systems. In terms of future possibilities, parallel learning and cost optimization are being pursued, like network pruning and how different malicious activities interact. The relevant standard bodies should also make effective standardization efforts for all privacy protection schemes [55]. Finally, evaluating and assessing privacy solutions in real-world scenarios is tough, especially when considering the balance between IoT quality-of-service and privacy protection.

Author details

Jaydip Sen* and Subhasis Dasgupta
Department of Data Science, Praxis Business School, Kolkata, India

*Address all correspondence to: jaydip.sen@acm.org

IntechOpen

References

[1] State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally. Available from: https://iot-analytics.com/number-connected-iot-devices/ [Accessed: March 27, 2023]

[2] Cisco Cybersecurity Report Series—Security Outcomes Study. Available from: https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-main-report.pdf [Accessed: March 27, 2023]

[3] The State of Cybersecurity Resilience 2021. Available from: https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf [Accessed: March 27, 2023]

[4] Gartner Press Release. Available from: https://www.gartner.com/en/newsroom [Accessed: March 27, 2023]

[5] Complete Guide to GDPR Compliance. Available from: https://gdpr.eu/ [Accessed: March 27, 2023]

[6] Rigaki M, Garcia S. A survey of privacy attacks in machine learning. arXiv. 2021 arXiv:2007.07646 DOI: 10.48550/arXiv.2007.07646

[7] Rodriguez E, Otero B, Canal R. A survey of machine and deep learning methods for privacy protection in the Internet of Things. Sensors. 2023;**23**. DOI: 10.3390/s23031252

[8] Seliem M, Elgazzar K, Khalil K. Towards privacy preserving IoT environments: A survey. Wireless Communications and Mobile Computing. 2018;**1**:1-15. DOI: 10.1155/2018/1032761

[9] Amiri-Zarandi M, Dara RA, Fraser E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. Computers & Security. 2020;**96**:21-45. DOI: 10.1016/j.cose.2020.101921

[10] Kounoudes AD, Kapitsaki GM. A mapping of IoT user-centric privacy preserving approaches to the GDPR. Internet of Things. 2020;**11**:100179. DOI: 10.1016/j.iot.2020.100179

[11] Zhu L, Tang X, Shen M, Gao F, Zhang J, Du X. Privacy-preserving machine learning training in IoT aggregation scenarios. IEEE Internet of Things Journal. 2021;**8**(15):12106-12118. DOI: 10.1109/JIOT.2021.3060764

[12] Ouadrhiri AE, Abdelhadi A. Differential privacy for deep and federated learning: A survey. IEEE Access. 2022;**10**:22359-22380. DOI: 10.1109/ACCESS.2022.3151670

[13] Pisa PS, Abdalla M, Duarte OCMB. Somewhat homomorphic encryption scheme for arithmetic operations on large integers. In: Proceedings of the Global Information Infrastructure and Networking Symposium (GIIS). December 17-19, 2012; Choroni, Venezuela. Piscataway, NJ, USA: IEEE; pp. 1-8. DOI: 10.1109/GIIS.2012.6466769

[14] Sen J. Homomorphic encryption – Theory and application. In: Sen J, editor. Theory and Practice of Cryptography and Network Security Protocols and Technologies. London, UK, London, UK: IntechOpen; 2011. pp. 1-30. DOI: 10.5772/56687

[15] Mahmood ZH, Ibrahem MK. New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing. In: Proceedings of the

1st Annual International Conference on Information and Sciences (AiCIS). November 20-21, 2018; Fallujah, Iraq. Piscataway, NJ, USA: IEEE. 2018. pp. 182-186. DOI: 10.1109/AiCIS.2018.00043

[16] Bost R, Popa RA, Tu S, Goldwasser S. Machine learning classification over encrypted data. In: Proceedings of NDSS Symposium. San Diego, CA, USA: Internet Society; 2015. DOI: 10.14722/ndss.2015.23241

[17] De Cock M, Dowsley R, Horst C, Katti R, Nascimento ACA, Poon WS, et al. Efficient and private scoring of decision trees, support vector machines and logistic regression models based on pre-computation. IEEE Transactions on Dependable and Secure Computing. 2019;**16**(2):217-230. DOI: 10.1109/TDSC.2017.2679189

[18] Rahulamathavan Y, Phan RC-W, Veluru S, Cumanan K, Rajarajan M. Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud. IEEE Transactions on Dependable and Secure Computing. 2014;**11**(5):467-479. DOI: 10.1109/TDSC.2013.51

[19] Wang W, Vong CM, Yang Y, Wong P-K. Encrypted image classification based on multilayer extreme learning machine. Multidimensional Systems and Signal Processing. 2017;**28**:851-865. DOI: 10.1007/s11045-016-0408-1

[20] Zhu H, Liu X, Lu R, Li H. Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. IEEE Journal of Biomedical and Health Informatics. 2017;**21**(3):838-850. DOI: 10.1109/JBHI.2016.2548248

[21] Jiang L, Chen L, Giannetsos T, Luo B, Liang K, Han J. Toward practical privacy-preserving processing over encrypted data in IoT: An assistive healthcare use case. IEEE Internet of Things Journal. 2019;**6**(6):10177-10190. DOI: 10.1109/JIOT.2019.2936532

[22] Shokri R, Shmatikov V. Privacy-preserving deep learning. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security; 12 October 2015; Denver, CO, USA. pp. 1310-1321. DOI: 10.1145/2810103.2813687

[23] Servia-Rodriguez S, Wang L, Zhao JR, Mortier R, Haddadi H. Personal model training under privacy constraints. In: Proceedings of the 2018 IEEE/ACM 3rd International Conference on Internet-of-Things Design and Implementation (IoTDI). April 17-20, 2018; Orlando, FL, USA. Washington, D.C., USA: IEEE Computer Society; 2018. pp. 153-164. DOI: 10.1109/IoTDI.2018.00024

[24] Shokri R, Stronati M, Song C, Shmatikov V. Membership inference attacks against machine learning models. In: Proceedings of the IEEE Symposium on Security and Privacy. Washington, D.C., USA: IEEE Computer Society. May 22-24, 2017; San Jose, CA, USA. pp. 3-18. DOI: 10.1109/SP.2017.41

[25] Fredrikson M, Lantz E, Jha S, Lin S, Page D, Ristenpart T. An end-to-end case study of personalized warfarin dosing. In: Proceedings of the 23rd USENIX Security Symposium. August 20-22, 2014; San Diego, CA, USA. Berkeley, CA, USA: USENIX Association; 2014. pp. 17-32

[26] Phong LT, Aono Y, Hayashi T, Wang L, Moriai S. Privacy-preserving deep learning: Revisited and enhanced. In: Batten L, Kim D, Zhang X, Li G, editors. Applications and Techniques in Information Security (ATIS), Communications in Computer and Information Science. Vol. vol. 719. Singapore: Springer; 2017. pp. 100-110. DOI: 10.1007/978-981-10-5421-1_9

[27] Netzer Y, Wang T, Coates A, Bissacco A, Wu B, Ng AY. Reading digits in natural images with unsupervised feature learning. In: Proceedings of the NIPS Workshop on Deep Learning and Unsupervised Feature Learning. December 12-17, 2011; Granada, Spain. San Francisco, CA, USA: Google Research; 2011. pp. 1-9

[28] González-Serrano FJ, Navia-Vázquez Á, Amor-Martín A. Training support vector machines with privacy-protected data. Pattern Recognition. 2017;**72**:93-107. DOI: 10.1016/j.patcog.2017.06.016

[29] Katz J, Lindell Y. Introduction to Modern Cryptography: Principles and Protocols. Boca Raton, FL, USA: CRC Press; 2020. ISBN-13: 978-1584885511

[30] Shen M, Tang X, Zhu L, Du X, Guizani M. Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal. 2019;**6**(5):7702-7712. DOI: 10.1109/JIOT.2019.2901840

[31] Breast Cancer Wisconsin Data Set (Diagnostic). Available from: https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+ [Accessed: March 27, 2023]

[32] Heart Disease Databases. Available from: https://archive-beta.ics.uci.edu/ml/datasets/heart+disease [Accessed: March 27, 2023]

[33] Almaiah MA, Ali A, Hajjej F, Pasha MF, Alohali MA. A lightweight hybrid deep learning privacy preserving model for FC-based industrial Internet of Medical Things. Sensors. 2002;**22**(6). DOI: 10.3390/s22062112

[34] Osia SA, Shamsabadi AS, Sajadmanesh S, Taheri A, Katevas K, Rabiee HR, et al. A hybrid deep learning architecture for privacy-preserving mobile analytics. IEEE Internet of Things Journal. 2020;**7**(5):4505-4518. DOI: 10.1109/JIOT.2020.2967734

[35] Chopra S, Hadsell R, LeCun Y. Learning a similarity metric discriminatively, with application to face verification. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR); July 2005; San Diego, CA, USA. Piscataway, NJ, USA: IEEE; 2005. pp. 539-546. DOI: 10.1109/CVPR.2005.202

[36] Rothe R, Timofte R, Van Gool L. Dex: Deep expectation of apparent age from a single image. In: Proceedings of the IEEE International Conference on Computer Vision Workshop (ICCVW), Santiago, Chile. December 7-13, 2015. Piscataway, NJ, USA: IEEE; 2015. pp. 252-257. DOI: 10.1109/ICCVW.2015.41

[37] Huang GB, Mattar M, Berg T, Learned-Miller E. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. In: Proceedings of the Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition. 12-18 October, 2008; Marseille, France. Berlin, Germany: Springer-Verlag; 2008. pp. 1-8

[38] Zhou X, Xu K, Wang N, Jiao J, Dong N, Han M, et al. A secure and privacy-preserving machine learning model sharing scheme for edge-enabled IoT. IEEE Access. 2021;**9**:17256-17265. DOI: 10.1109/ACCESS.2021.3051945

[39] Zhou J, Cao Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine. 2017;**55**(1):26-33. DOI: 10.1109/MCOM.2017.1600363CM

[40] Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, et al. Deep learning with differential privacy. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. October 24-28, 2016; Vienna, Austria. New York, NY, USA: ACM; 2016. pp. 308-318. DOI: 10.1145/2976749.2978318

[41] Hitaj B, Ateniese G, Perez-Cruz F. Deep models under the GAN: Information leakage from collaborative deep learning. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. October 30–November 3, 2017; Dallas, TX, USA. New York, NY, USA: ACM; 2017. pp. 603-618. DOI: 10.1145/3133956.3134012

[42] Wang J, Zhang J, Bao W, Zhu X, Cao B, Yu PS. Not just privacy: Improving performance of private deep learning in mobile cloud. In: Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. August 19-23, 2018; London, UK. New York, NY, USA: ACM; 2018. pp. 2407-2416. DOI: 10.1145/3219819.3220106

[43] Zhang T, He Z, Lee RB. Privacy-preserving machine learning through data obfuscation. arXiv. 2018, arXiv:1807.01860. DOI: 10.48550/arXiv.1807.01860

[44] Lyu L, Bezdek JC, He X, Jin J. Fog-embedded deep learning for the Internet of Things. IEEE Transactions on Industrial Informatics. 2019;**15**(7):4206-4215. DOI: 10.1109/TII.2019.2912465

[45] Jiang L, Tan R, Lou X, Lin G. On lightweight privacy-preserving collaborative learning for Internet of Things by independent random projections. ACM Transactions on Internet Things. 2021;**2**(2):1-32. DOI: 10.1145/3441303

[46] Alguliyev RM, Aliguliyev RM, Abdullayeva FJ. Privacy-preserving deep learning algorithm for big personal data analysis. Journal of Industrial Information Integration. 2019;**15**:1-14. DOI: 10.1016/j.jii.2019.07.002

[47] Du M, Wang K, Chen Y, Wang X, Sun Y. Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things. IEEE Communications Magazine. 2018;**56**(8):62-67. DOI: 10.1109/MCOM.2018.1701148

[48] Rouhani BD, Riazi MS, Koushanfar F. Deepsecure: Scalable provably-secure deep learning. In: Proceedings of the 55th Annual Design Automation Conference. 24 June, 2018; San Francisco, CA, USA. New York, NY, USA: ACM; 2018. pp. 1-6. DOI: 10.1145/3195970.3196023

[49] Yao AC-C. How to generate and exchange secrets. In: Proceedings of 27th Annual Symposium on Foundations of Computer Science (SFCS). October 27-29, 1986; Toronto, ON, Canada. Piscataway, NJ, USA: IEEE; 1986. pp. 162-167. DOI: 10.1109/SFCS.1986.25

[50] Saleem A, Khan A, Shahid F, Alam MM, Khan MK. Recent advancements in garbled computing: How far have we come towards achieving secure, efficient and reusable garbled circuits. Journal of Network and Computer Applications. 2018;**108**:1-19. DOI: 10.1016/j.jnca.2018.02.006

[51] Ma Z, Liu Y, Liu X, Ma J, Li F. Privacy-preserving outsourced speech recognition for smart IoT devices. IEEE Internet of Things Journal. 2019;**6**(5):8406-8420. DOI: 10.1109/JIOT.2019.2917933

[52] Zhang L, Jajodia S, Brodsky A. Information disclosure under realistic assumptions: Privacy versus

optimality. In: Proceedings of the 14th ACM Conference on Computer and Communications Security. October 31–November 2, 2007; Alexandria, VA, USA. New York, NY, USA: ACM; 2007. pp. 573-583. DOI: 10.1145/1315245.1315316

[53] Wong RCW, Fu AWC, Wang K, Yu PS, Pei J. Can the utility of anonymized data be used for privacy breaches? ACM Transactions on Knowledge Discovery from Data. 2011;**5**(3):1-24. DOI: 10.1145/1993077.1993080

[54] Aggarwal CC. Privacy and the dimensionality curse. In: Aggarwal CC, Yu PS, editors. Privacy-Preserving Data Mining: Advances in Database Systems. Vol. 34. Boston, MA, USA: Springer; 2008. pp. 433-460. DOI: 10.1007/978-0-387-70992-5_18

[55] Bandyopadhyay D, Sen J. Internet of Things: Applications and challenges in technology and standardization. Wireless Personal Communications. 2011;**58**(1):49-69. DOI: 10.1007/s11277-011-0288-5