Analysis of Edge Intelligent Frameworks and their Security Issues

Waleed, Muhammad; Kosta, Sokol; Skouby, Knud Erik

Published in:
Journal of Mobile Multimedia

DOI (link to publication from Publisher):
10.13052/jmm1550-4646.1916

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Analysis of Edge Intelligent Frameworks and their Security Issues

Muhammad Waleed, Sokol Kosta and Knud Erik Skouby*

Department of Electronic Systems, Aalborg University Copenhagen, Denmark
E-mail: muhammadw@es.aau.dk; sok@es.aau.dk; skouby@es.aau.dk
**Corresponding Author*

Received 20 April 2022; Accepted 31 May 2022;
Publication 15 September 2022

Abstract

Edge Intelligence has become increasingly popular and has already made its place to increase the overall system performance by reducing the burden of the cloud and the network. In edge intelligent frameworks, a massive amount of data generated are not provided to the central cloud, and data analysis is carried out at the edge. Edge intelligence IoT environments comprise heterogeneous devices that communicate over the network, making it essential to protect the data and users' information. Through these edge frameworks, numerous users and devices take part in communication where the exchange of sensitive data occurs. Therefore, security in such frameworks is crucial and a key challenge for reliable communication. This paper performs an analysis of popular AI/ML applications toward edge intelligence focusing on highlighting the critical security and privacy concerns desired in such systems. After a thorough investigation, we show that although several promising edge intelligent frameworks have been developed to address energy and performance issues, they do not consider the security and privacy of the data as the researchers are more focused on the performance predicaments.

Keywords: Wireless devices, IoT, edge intelligence, security and privacy.

Journal of Mobile Multimedia, Vol. 19_1, 117–134.
doi: 10.13052/jmm1550-4646.1916

1 Introduction

With the fast development and recent advancement in the field of the internet of things (IoT), the number of smart devices connected to the internet is growing day by day, resulting in large-scale data, which has induced concerns such as slow response speed, bandwidth load, and insufficient security, and privacy in traditional cloud computing models. Furthermore, traditional cloud computing can no longer handle the increasing amount of data and other requirements for data processing. To address these issues, today's intelligent society and its diverse needs lead to edge computing technology [1].

Edge computing is a widely used solution nowadays, which among other things, provides artificial intelligence services for rapidly growing terminal devices and data, making such services more stable, a concept known as Edge Intelligence (EI) [2, 3]. Figure 1 depicts an overview of an edge intelligence system, showing computational resources being close to the data source, such as smart terminals and IoT devices, enabling storing and processing of data at the network's edge [4].

Generally, in traditional frameworks, intelligent intervention occurs at the cloud level to deal with a massive amount of data and its management. On the other side, edge intelligence determines the artificial intelligence endorsed towards the edge of the network away from the cloud, incorporating a certain amount of intelligence at the edge of the network where edge devices communicate [3]. The main goal of utilizing edge intelligence is to reduce the workload of cloud computations and bring it to the edge level. This causes immense improvement in reducing the resource demand at the cloud level leading to lower cloud pressure.

Edge computing has several applications, and it is extended enormously to modern industries, taking part in fields such as energy, industrial productions, smart home and healthcare systems, and transportation [5, 6]. Edge intelligence is leading in the area related to performance, and several frameworks have been developed to accelerate the services at the edge. Performance and energy consumption are both essential factors considered by proposed solutions [8]. Efforts were conducted in developing and employing edge intelligent frameworks to make data analysis possible intelligently at the edge with the help of AI algorithms and to reduce energy consumption while dragging the processing power towards the edge [9, 10].

However, the interaction of the various heterogeneous IoT devices with the edge or with the cloud is vulnerable and exposes users' data to possible malicious attacks [11, 12]. Furthermore, artificial intelligence inherited

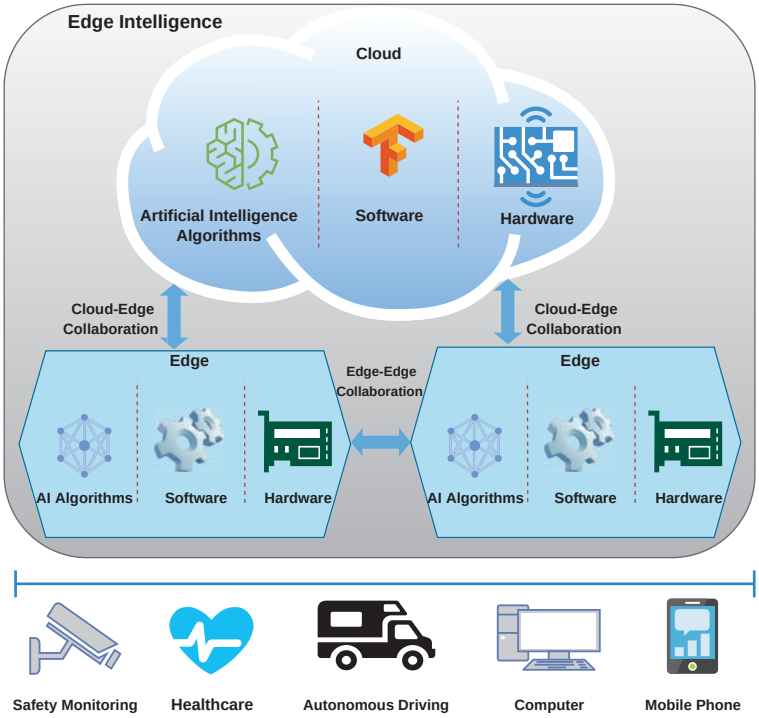


Figure 1 Overview and collaboration of Edge Intelligence example.

security issues in Edge Intelligence systems due to its learning parameters, which distracts communication upon exposure. At the training stage, the hacker can inject malicious data into the dataset, which leads to manipulating data labels or input features. These attacks aim to expose the datasets at the training phase or model structure [7]. As such, securing sensitive information and users' data in such communication is imperative. In this study, we perform a thorough analysis of recent edge intelligence frameworks in the literature along with how they address the security aspects of authentication and data encryption.

The paper is organized so Section II presents the edge intelligent frameworks with a subsection describing our methodology, followed by the desired security properties in edge computing and EI, and concludes with the analysis of the selected EI frameworks and their security issues. Finally, Section III presents our findings and the possible future directions for adequately addressing the lack of security measures in the EI frameworks.

2 Edge Intelligence and Security

2.1 Methodology

We have thoroughly analyzed recent studies on edge intelligent frameworks, focusing on their approach to handling device authentication and data security. For this purpose, we performed extensive research on identifying relevant papers published in the last years based on edge intelligent frameworks and their security and privacy issues in international conferences and journals. We used IEEE Xplore and Google Scholar databases and targeted keywords like edge intelligence, security and privacy. As a result, we gathered more than 50 papers and studied them. We show what security and privacy issues are associated with these AI-backed frameworks and present the future directions to take a roadmap for developing a security framework for edge intelligence.

2.2 Desired Security Properties in Edge Computing

In this section, we elaborate on the essential security features imperative for an EI framework based on the study of recent works [7, 11, 13–15]. Several researchers worked on various security features according to the requirement of their AI-based models [16–19]. Analyzing these features gives us the view that placing these security properties will significantly benefit EI frameworks, reducing or bouncing the possible malicious attacks. Several IoT models have been developed with these security features like smart cities and healthcare systems [20].

1. *Authentication*: A heterogeneous IoT environment is composed of various devices that communicate and exchange information to and from the system. This makes it imperative to place an authentication scheme where each device properly goes through an authorization process to avoid malicious intrusion. The authentication is provided based on access control, which permits and provides access only after identifying a permissible device [13]. With authentication and access control in place, unauthorized users will not be able to use protected resources.
2. *Privacy*: For sensitive communications, several key aspects need to be ensured when private data like user location or identity, among others, are collected or transmitted [14]. Data sending or retrieving from the system are some of the main activities that may lead to unwanted data exposure. In addition, attackers always search for other holes in the system to grasp the data in different ways to expose user identity, location, or other sensitive information.

3. *Data Sharing*: Quite often, devices collaborate by sharing data to provide reliable services to the users. However, numerous devices share a considerable amount of data in mobile networks, which is highly vulnerable to several types of attacks like DoS, data leakage, etc. [15]. Moreover, the heterogeneous environment of IoT also poses difficulties in data sharing as it needs a lot of computation and data management to avoid security gaps.
4. *Data Integrity*: This part of security aims to prevent unauthorized modification of the data. The data integrity is attained by placing strict models for unauthorized control and access management [21]. Various kinds of intrusion detection methods like anomaly-based approach, signature, and specification-based techniques are also a significant addition to the system security [22]. The attacker's target is injecting false data or modifying the device information to affect data and distract the communication.
5. *Availability*: On-time availability of IoT resources such as data, applications, etc., is crucial from a security perspective as delayed access to these resources may lead to a malicious attack. To address this, consistent monitoring and adapting handling capabilities for the resources is essential for the IoT system. Attackers target the system with DDoS attacks to prevent the users' access to the IoT assets timely [23].
6. *Accountability*: This crucial security feature guarantees the feasibility of events and actions associated with the individual user [21]. Therefore, tracing all the events while interacting with a user is essential to prevent possible malicious intrusions. However, according to J. Singh et al., it is interesting to notice that IoT-based models are still chasing to comply with the accountability feature, as it has not acquired any thorough consideration [24].

2.3 Edge Intelligent Frameworks and Their security

As an emerging technology, edge computing deploys computing and storage resources (such as cloudlets, micro data centers, fog nodes, etc.) at the edge of the network closer to mobile devices or sensors [6]. Zhao et al. define edge computing as *a computing model that unifies resources that are close to the user in geographical distance or network distance to provide computing, storage, and network for applications service* [25]. This platform integrates core capabilities such as networking, computing, storage, and applications and provides edge intelligent services nearby to meet the industry agility key

requirements in connection, real-time business, data optimization, application intelligence, security, and privacy [26].

Penghua Zhen et al. [27] designed an efficient and lightweight novel framework called CareEdge for edge intelligence. It was developed for smart applications based on IoT Edge and cloud integration. The system is tested in the healthcare ECG-based heartbeat detection system. They noted that the latency is lower compared to the other same frameworks. The system is developed for healthcare and entirely focuses on latency, where the security of patients' data is far more critical; however, they do not mention the security aspects of the patient's data in their proposed work. None of the security features like authentication, integrity, availability, and accountability are discussed or employed in their model.

In order to improve and accelerate artificial intelligence algorithm training for edge computing and increase the performance of applications processing, V. Gupta et al. [28] presented GViM, which is considered the early implementation of GPU virtualization. Multiple virtual machines are hosted on a single node to make access possible to the same physical GPU. The virtualization is achieved by utilizing API interception so that the host machine quickly receives the CUDA function call from an application running on the virtual machine. However, the paper only addresses the problem of sharing accelerators and resource management, leaving a gap for authentication of different devices when accessing the resources.

Several other distinct approaches in this direction were presented, such as DSCUDA [29] and Grid-CUDA [30]. The scheme based on DSCUDA is developed for cloud use. This approach uses the redundancy method by comparing two cloud accelerators on a single virtual accelerator. For improving the accuracy, if the results are not similar, it automatically executes the CUDA API again to get the same results. On the other hand, the Grid-CUDA enables parallel execution by outsizing the Remote Procedure Call (RPC) to transmit workload among nodes. It is observed that using the RPC leads to high operating costs and may cause a lowering of the overall performance of Grid-CUDA. Although the technique improves accuracy and enhances security somehow as it only allows the data and commands related to GPU to be stored on the cloud side, it does not provide any notable security mechanism like the authentication of devices and access control to avoid nonrelated devices while distributing the workload among nodes. Further, the work focused on increasing performance and accuracy.

In the same direction, G. Giunta et al. have designed GVirtuS as a solution for GPU remoting and virtualization [31, 32]. The mechanism offers remote

acceleration, and the solution is based on a virtual machine working on a TCP/IP model, offering remote-enabled facilitation for the virtualization. GVirtuS is independent of the hypervisor; however, taking it as an option affects the performance. The hypervisor makes the interaction of multiple virtual machines or devices possible with the same physical accelerator. Although the work shows pretty good results with respect to remote computation execution, it does not consider any authentication mechanism to secure data exchange between multiple devices.

Chen et al. [33] target to achieve the size of the neural network (NN) and the memory resource, which are essential and primary factors for making the training efficient. However, their work targeted the training efficiency of the AI algorithm at the edge, leaving behind security deployments like integrity and availability as attackers try to inject data in the training stage to expose the model structure. Furthermore, the authentication of devices at the edge is also crucial, lacking in their work.

Li et al. [34] proposed DeepCham, an object recognition framework mainly used for mobile devices. The framework comprises edge servers considered a single master and mobile devices deemed multiple workers. In the developed framework, the mobile workers recognize objects in the visual domain while the master is responsible for training the model using data generated by multiple workers (i.e., mobile devices). However, the work does not mention the security of the data exchange between mobile and edge. Further, none of the security features has been discussed for their model.

In their work, Xing et al. [35] developed a framework named RecycleML to speed up the training of NNs while employing cross model transfer on mobile devices. On the other hand, in [36], the authors proposed a technique based on transfer features learned by a trained model. For enabling the collaboration between CPU and GPU, they used the shared memory of the edge devices. However, both works focused on the features transfer; no security mechanisms like authentication and integrity (i.e., intrusion detection approaches like anomaly-based techniques, etc.) are deployed in their model, leading to high chances that a malicious attack could expose these features.

Shah Mohammadi et al. [37] presented iML on HAR, and they found that simply a few training instances are sufficient to reach a reasonable recognition accuracy. Following the above work, Flutura et al. in [38] designed a DrinkWatch to recognize drink activities based on sensors on smartwatches. Unfortunately, although their work addresses the issue of recognition accuracy pretty well, they do not mention anything about the security side of these recognition frameworks.

Several researchers worked on complex edge intelligence frameworks as in [39], their work shows that initially, the mobile devices or multiple workers gather the profile of training instances and put up the request to the server for training purposes. Then, based on the availability, the cloud employs edge computing to accomplish the training. Some efforts took the leverage of transfer learning to make the training process fast [40, 41]. The models employed in transfer learning utilized the learned features of prior models, which considerably reduced the learning time. Further, a framework was developed to optimize the setting of federated learning and speed up the training process. The above studies presented increased performance while making the training process fast. This significantly reduces the time; however, no security measures like authentication, data integrity, availability, and access control are mentioned to secure the edge where training is accomplished.

S. Theodorou and N. Sklavos [46] presented a security scheme based on the smart cities cloud system. The chapter focused on less use of resources and an increase in privacy to improve the life of an ordinary citizen. Furthermore, they have mentioned that smart contracts and their applications can be utilized for e-governance. Unfortunately, although there are good suggestions regarding security for ballot stuffing, bad mouth, and identification of malicious attacks, there are no practical implementations to show the results of the suggested schemes.

A *belief based trust evaluation mechanism* (BTEM) was proposed to detect the affected node and separate it from other nodes [47]. They have used the Bayesian estimated technique to counter the DoS, On-Off, and bad mouth attacks. Qureshi et al. in [38] also presented a scheme for the bad mouth and On-off attacks for the same purpose. Both schemes were developed to detect malicious nodes; they have thoroughly discussed the security feature like availability and the attacks associated with it; however, the work does not mention authentication and how different nodes taking part in the communication are permitted. Also, they did not mention access control, which is critical in such an environment.

Ji Wang et al. proposed a cloud-based framework called Arden by utilizing the deep neural network [49]. The goal was to increase performance on the cloud side, the imaging data sent from mobile to cloud for testing. They also introduced a lightweight privacy-preserving scheme; however, there was no specific security mechanism presented, and most of the focus was on the system's robustness. Other approaches were developed [50–52] to address the security issues but mostly lacked a comprehensive authentication framework,

Table 1 Analysis of edge intelligence frameworks

Reference	Model	Enabler	Setup	Security Features	Performance
Xuehai Hong and Yang Wang (2018)[26]	GPU-accelerated Virtual Machines (GViM)	Hardware acceleration	GPGPU system based on a Xeon quad-core attached NVIDIA graphics accelerators	No Specific Security features mentioned	Improved concerning fairness in accelerator use by multiple VMs
Zhen, Penghua et al. (2021) [27]	Distributed-shared compute unified device architecture (DS-CUDA)	Hardware acceleration	Cloud computing	No Specific Security features mentioned	Showed 58 and 36 times more speed compared to locally installed GPU
V. Gupta et al. (2009) [28]	Remote GPU virtualization for clusters	Hardware acceleration	Cloud computing	No Specific Security features mentioned	Increase in throughput and reduce energy consumption up to 40%
M. Oikawa et al. (2012) [29]	GPU virtualization service (GVirtuS)	Hardware (nVIDIA GPUs Tesla 1060C+ nVIDIA Quadro FX 5600)	Cloud computing based HPC clusters	Only GPU associated commands and data store on cloud for security reason	High performance compared to existing virtualization systems
Zhao Ziming et al. (2018) [25]	Deep Neural Network	Software (Gateway and Edge interface)	Edge computing (Healthcare-Heartbeat detection system)	No Specific Security features mentioned	86% accuracy and Lower latency compared to HealthFog healthcare system
T. Liang et al. (2011) [30]	Deep Neural Network	Hardware acceleration	Mobile computing	Focused on accuracy and performance No Specific Security features mentioned	Prototype of TensorFlow+
Y. Chen et al. (2018) [33]	Convolutional Neural Network	Software acceleration	Human activity recognition	Focused on training efficiency, no security aspects addressed	Faster 50 times than scratch training
D. Li et al. (2016) [34]	Convolutional Neural Network	Hardware acceleration	Mobile computing	No Specific Security features mentioned	Faster compared to Caffe-OpenCL
T. Xing et al. (2018) [35]	RF, ET, NB, SVM, LR	Human annotation	Human activity recognition	Focused on features transfer, no security modeled in their work, leading high chances of features expose	Accuracy 93.3%
O. Valery et al. (2017) [36]	Naive Bayes	Human annotation	Human activity recognition	Focused on features transfer, no security modeled in their work, leading chance of malicious attack on model structure	Training time 6-8 hours
Y. Huang et al. (2018) [39]	Convolutional Neural Network	Hardware acceleration Parameter quantization	Mobile computing	Focused to reduce time; no security measures like authentication	Faster compared to Caffe-OpenCL
O. Valery et al. (2018) [40]	Deep Neural Network	Hardware acceleration	Analog computing	Focused on efficiency and time reduction; no security measures discussed	Close to software baseline 97.9
G. W. Burr et al. (2019) [41]	Statistical Model	Software acceleration	Multitask learning	Focused on efficiency and time reduction; no security measures discussed	Outperform global, local manners
V. Smith et al. (2017) [42]	Deep Neural Network	Hardware acceleration	Mobile computing	Training efficiency, No specific security features mentioned	TensorFlow+, Efficient response time (ms) is 0.24 for CPU and 0.21 for GPU
Zhao Ziming et al. (2018) [43]	Virtual OpenCL for remote GPUs	GPU hardware	On several applications kernels	No specific security features	Significantly reduced the overhead

(*Continued*)

Table 1 Continued

Reference	Model	Enabler	Setup	Security Features	Performance
Theodorou, Sophocles, and Nicolas Sklavos (2019) [46]	Theory of belief	Software (Gateway and Edge interface)	Wireless Sensor Network (WSN)	Authentication and identification for ballot stuffing, bad mouth, identify	Good compared to other detection schemes
Anwar et al. (2019) [47]	Bayesian belief based method	Software simulation	IoT Cloud-WSN	Availability and associated attacks, detection of node isolation and its behaviour	Preforms good in node detection and isolation got DoS, Bad Mouthing and On-off attacks
Qureshi et al. (2020) [48]	Policy based	Software experiments	IoT Cloud	Identification of bad Mouthing and On-off attacks	Detect Bad Mouthing and On-off attacks
J. Wang et al. (2018) [49]	DNN splitting, Arbitrary data nullification, Random noise addition	Arden	Mobile cloud	Information leakage	Perform well compared to other DNNs in the context of energy and time
Y. Liu et al. (2020) [50]	Self-learning Model	Homomorphic encryption	IoT Cloud	Designed for information leakage	Slight drop in accuracy
K. Wei et al. (2020) [51]	MLP network	Differential privacy	IoT Cloud	Designed for information leakage	Privacy retained
K. Cheng et al. (2019) [52]	Data split	RL SecureBoost	IoT Cloud	Tracing Information leakage	Increase in accuracy

where data at the edge could be secure after authorization. These schemes narrowly focus on information leakage and mostly tilt towards performance and accuracy.

The malicious adversarial actions occur both for data and learning framework, which distract the communication and users' data [53]. Moreover, the deployment of learning-based systems creates new security and privacy challenges, as the attackers target the system during a time of training or datasets to expose the model structure and acquire the features. In most cases, the main goal of deploying these AI systems is to achieve the best performance. However, these malicious actions concerning security crucially affect the performance and paralyze the whole system. Table 1 shows a recap of the analysis of the various edge intelligence frameworks discussed in this section.

3 Conclusion

This paper presents a thorough analysis of edge intelligent frameworks, focusing on their potential security concerns. Numerous edge intelligence frameworks have been designed for different cloud platforms to enhance

the overall efficiency in communication and data processing. However, these frameworks are mainly utilized for performance, latency, and energy consumption in edge and cloud computing; they need to be secured with authentication in the environment of multiple interconnected systems. Furthermore, even though these frameworks are promising, they are developed primarily for a specific environment comprising only specific IoT devices. Therefore, analysis shows that these frameworks need to be extended for heterogeneous IoT environments, which comprise both intelligent and non-intelligent devices. Moreover, these frameworks mainly focuses on the system's output (i.e., throughput, latency, and performance), leaving behind a significant gap in the security of edge intelligent systems. We also presented some security critiques of the existing schemes.

As part of our future work, we will take inspiration from the learning of this study and we will work on designing and developing a novel framework that focuses on the security aspects of edge intelligence. The developed security-based scheme will be adopted in future edge intelligence frameworks for secure and reliable communication.

Acknowledgement

This work was supported by IoTalentum, funded by the European Union Horizon 2020 research and innovation program within the framework of Marie Skłodowska-Curie Actions (MCSA) ITN-ETN with grant number 953442.

References

[1] Yu, Wei and Liang, Fan and He, Xiaofei and Hatcher, William Grant and Lu, Chao and Lin, Jie and Yang, Xinyu. A survey on the edge computing for the Internet of Things. *IEEE access*, (6):6900–6919, (2017), 10.1109/ACCESS.2017.2778504.

[2] Sodhro, Ali Hassan and Pirbhulal, Sandeep and de Albuquerque, Victor Hugo C. Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications. *IEEE Transactions on Industrial Informatics*, 15(7):4235-4243, (2019), 10.1109/TII.2019.2902878.

[3] Xu, Dianlei and Li, Tong and Li, Yong and Su, Xiang and Tarkoma, Sasu and Jiang, Tao and Crowcroft, Jon and Hui, Pan. Edge Intelligence:

Empowering Intelligence to the Edge of Network. *Proceedings of the IEEE*, 109(11):1778-1837, (2019), 10.1109/JPROC.2021.3119950.

[4] ETSI, MECISG. Multi-access edge computing (MEC) framework and reference architecture. ETSI GS MEC 3 V2. *Proceedings of the IEEE*, (2019).

[5] Kennedy, Jason and Varghese, Blesson and Reaño, Carlos. AVEC: Accelerator Virtualization in Cloud-Edge Computing for Deep Learning. *arXiv*, (2021), 10.48550/ARXIV.2103.04930.

[6] M. Satyanarayanan. The Emergence of Edge Computing. *Computer*, 50(1):30-39, (Jan. 2017), 10.1109/MC.2017.9.

[7] Oseni, Ayodeji, Nour Moustafa, Helge Janicke, Peng Liu, Zahir Tari, and Athanasios Vasilakos. Security and Privacy for Artificial Intelligence: Opportunities and Challenges. *arXiv preprint arXiv:2102.04661*, (2021), 10.48550/ARXIV.2102.04661.

[8] Sayed, Aya, Yassine Himeur, Abdullah Alsalemi, Faycal Bensaali, and Abbes Amira. Intelligent edge-based recommender system for internet of energy applications. *IEEE Systems Journal*, 1–10, (2021), 10.1109/jsyst.2021.3124793.

[9] Han, Tao, Khan Muhammad, Tanveer Hussain, Jaime Lloret, and Sung Wook Baik. An efficient deep learning framework for intelligent energy management in IoT networks. *IEEE Internet of Things Journal*, 8(5): 3170–3179, (2020), 10.1109/JIOT.2020.3013306.

[10] Liu, Yi, Chao Yang, Li Jiang, Shengli Xie, and Yan Zhang. Intelligent edge computing for IoT-based energy management in smart cities. *IEEE network*, 33(2): 111–117, (2019), 10.1109/MNET.2019.1800254.

[11] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. Towards an analysis of security issues, challenges, and open problems in the internet of things. *IEEE World Congress on Services*, 21–28, (27 June-2 July 2015) New York, NY, USA, 10.1109/SERVICES.2015.12.

[12] Frustaci, Mario, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things*, 5(4): 2483–2495, (2017), 10.1109/JIOT.2017.2767291.

[13] Ari, Ado Adamou Abba, Olga Kengni Ngangmo, Chafiq Titouna, Ousmane Thiare, Alidou Mohamadou, and Abdelhak Mourad Gueroui. Enabling privacy and security in Cloud of Things: Architecture, applications security and privacy challenges. *Applied Computing and Informatics*, (2020), 10.1016/j.aci.2019.11.005.

[14] Sun, PanJun. Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 160, (2020), 102642, 10.1016/j.jnca.2020.102642.

[15] Cao, Keyan, Yefan Liu, Gongjie Meng, and Qimeng Sun. An overview on edge computing research. *IEEE access*, 8: 85714–85728, (2020), 10 .1109/ACCESS.2020.2991734.

[16] Patel, Chintan and Doshi, Nishant. A Novel MQTT Security framework In Generic IoT Model. *Procedia Computer Science* 171, (2020), 10.101 6/j.procs.2020.04.150.

[17] Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. Deep learning models for cyber security in IoT networks. *In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC), Las Vegas, NV, USA*, 0452-0457, (7–9 Jan. 2019), 10.1109/CCWC.2019.86 66588.

[18] Liu, Caiming, Yan Zhang, and Huaqiang Zhang. A novel approach to IoT security based on immunology. *In 9^{th} International Conference on Computational Intelligence and Security, Emeishan, China*, 771–775, (14-15 December 2013), 10.1109/CIS.2013.168.

[19] Cui, Qimei, Zengbao Zhu, Wei Ni, Xiaofeng Tao, and Ping Zhang. Edge-Intelligence-Empowered, Unified Authentication and Trust Evaluation for Heterogeneous Beyond 5G Systems. *IEEE Wireless Communications*, 28(2): 78–85, (2021), 10.1109/MWC.001.200032 5.

[20] Ghazal, Taher M. Internet of Things with Artificial Intelligence for Health Care Security. *Arabian Journal for Science and Engineering*, 1–12, (2021), 10.1007/s13369-021-06083-8.

[21] Neshenko, Nataliia, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys and Tutorials*, 21(3): 2702–2733, (2019), 10.1109/COMST.2019.2910750.

[22] Tavallaee, Mahbod, Natalia Stakhanova, and Ali Akbar Ghorbani. Toward credible evaluation of anomaly-based intrusion-detection methods. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(5): 516–524, (2010), 10.1109/TSMC C.2010.2048428.

[23] Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (IoT) security: Current status, challenges and prospective measures. *In 2015 10th international conference for internet*

technology and secured transactions (ICITST), London, UK, 336-341, (14–16 December 2015), 10.1109/ICITST.2015.7412116.

[24] Singh, Jatinder, Christopher Millard, Chris Reed, Jennifer Cobbe, and Jon Crowcroft. Accountability in the IoT: Systems, law, and ways forward. *Computer*, 51(7): 54–65, (2018), 10.1109/MC.2018.3011052.

[25] Zhao Ziming, Liu Fang, Cai Zhiping, Xiao Nong. Edge Computing: Platforms, Applications and Challenges. *Journal of Computer Research and Development*, 55(2): 327–337, (2018), 10.7544/issn1000-1239.20 18.20170228.

[26] Xuehai Hong, Yang Wang. Edge Computing Technology: Development and Countermeasures. *Strategic Study of Chinese Academy of Engineering*, 20(2): 20–26, (2018), 10.15302/J-SSCAE-2018.02.004.

[27] Zhen, Penghua and Han, Yubing and Dong, Anming and Yu, Jiguo. CareEdge: A Lightweight Edge Intelligence Framework for ECG-Based Heartbeat Detection. *Procedia Computer Science.*, 187, 329–334, (2021), 10.1016/j.procs.2021.04.070.

[28] Gupta, Vishakha, Gavrilovska, Ada, Schwan, Karsten, Kharche, Harshvardhan, Tolia, Niraj, Talwar, Vanish and Ranganathan, Parthasarathy. GViM: GPU-Accelerated Virtual Machines. *In Proceedings of the 3rd ACM Workshop on System-Level Virtualization for High Performance Computing*, 17–24, (2009), 10.1145/1519138.1519141.

[29] M. Oikawa et al. DS-CUDA: A Middleware to Use Many GPUs in the Cloud Environment. *In SC Companion: High Performance Computing, Networking Storage and Analysis, Salt Lake City, UT, USA.*, 1207–1214, (10–16 November 2012), 10.1109/SC.Companion.2012.146.

[30] T. Liang et al. GridCuda: A Grid-Enabled CUDA Programming Toolkit. *IEEE Workshops of International Conference on Advanced Information Networking and Applications, Biopolis, Singapore.*, 141–146, (22–25 March 2011), 10.1109/WAINA.2011.82.

[31] G. Giunta et al. A GPGPU Transparent Virtualization Component for High Performance Computing Clouds. *In Euro-Par 2010 – Parallel Processing, Springer, Berlin, Heidelberg.*, 627, 379–391, (2010), 10.1 007/978-3-642-15277-1-37.

[32] Montella, Raffaele, Carmine Ferraro, Sokol Kosta, Valentina Pelliccia, and Giulio Giunta. Enabling android-based devices to high-end gpgpus. *In International Conference on Algorithms and Architectures for Parallel Processing*, 10048, 118–125. Springer, Cham, (2016), 10.1007/978-3-319-49583-5-9.

[33] Y. Chen, S. Biookaghazadeh, and M. Zhao. Exploring the capabilities of mobile devices supporting deep learning. *In Proc. 27th Int. Symp. High-Perform. Parallel Distrib. Comput.*, (Jun. 2018), pp. 17–18, 10.1145/3318216.3363316.

[34] D. Li, T. Salonidis, N. V. Desai, and M. C. Chuah. DeepCham: Collaborative edge-mediated adaptive deep learning for mobile object recognition. *In Proc. IEEE/ACM Symp. Edge Comput. (SEC), Washington, DC, USA.*, (27–28 October 2016), 64–76, 10.1109/SEC.2016.38.

[35] T. Xing, S. S. Sandha, B. Balaji, S. Chakraborty, and M. Srivastava. Enabling edge devices that learn from each other: Cross modal training for activity recognition. *In Proc. 1st Int. Workshop Edge Syst., Anal. Netw.*, (Jun. 2018), 37–42, 10.1145/3213344.3213351.

[36] O. Valery, P. Liu, and J.-J. Wu. CPU/GPU collaboration techniques for transfer learning on mobile devices. *In Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS), Shenzhen, China.*, (Dec. 2017), pp. 477–484, 10.1109/ICPADS.2017.00069.

[37] F. Shahmohammadi, A. Hosseini, C. E. King, and M. Sarrafzadeh. Smartwatch based activity recognition using active learning. *In Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, (Jul. 2017), pp. 321–329, 10.1109/CHASE.2017.115.

[38] S. Flutura et al. DrinkWatch: A mobile wellbeing application based on interactive and cooperative machine learning. *In Proc. Int. Conf. Digit. Health*, (Apr. 2018), pp. 65–74, doi.org/10.1145/3194658.3194666.

[39] Y. Huang et al. Task scheduling with optimized transmission time in collaborative cloud-edge learning. *In Proc. 27^{th} Int. Conf. Comput. Commun. Netw. (ICCCN), 30 July-2 Aug, Hangzhou, China* (Jul. 2018), pp. 1–9, 10.1109/ICCCN.2018.8487352.

[40] O. Valery, P. Liu, and J.-J. Wu. Low precision deep learning training on mobile heterogeneous platform. *In Proc. 26th Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process. (PDP), Cambridge, UK*, (21–23 March 2018), 10.1109/PDP2018.2018.00023.

[41] G. W. Burr, S. Ambrogio, P. Narayanan, H. Tsai, C. Mackin, and A. Chen. Accelerating deep neural networks with analog memory devices *In Proc. China Semiconductor Technol. Int. Conf. (CSTIC), Shanghai, China* (Mar. 2019), pp. 149–152, 10.1109/CSTIC.2019.8755642.

[42] V. Smith, C.-K. Chiang, M. Sanjabi, and A. S. Talwalkar. Federated multi-task learning. *in Proc. Adv. Neural Inf. Process. Syst.*, (2017), pp. 4424–4434, 10.48550/ARXIV.1705.1046.

[43] Zhao Ziming, Liu Fang, Cai Zhiping, Xiao Nong. Edge Computing: Platforms, Applications and Challenges. *Journal of Computer Research and Development.*, (2018), 55(2): 327–337, 10.7544/issn1000-1239.2018.20170228.

[44] Xuehai Hong, Yang Wang. Edge Computing Technology: Development and Countermeasures. *Strategic Study of Chinese Academy of Engineering.* (2018), 20(2): 20–26, 10.15302/J-SSCAE-2018.02.004.

[45] J. Mandebi Mbongue et al. FPGA Virtualization in Cloud-Based Infrastructures Over Virtio. *in IEEE 36th International Conference on Computer Design, Orlando, FL, USA*. (7–10 Oct. 2018), pp. 242–245, 10.1109/ICCD.2018.00044.

[46] Theodorou, Sophocles, and Nicolas Sklavos. Blockchain-based security and privacy in smart cities. *In Smart Cities Cybersecurity and Privacy.* pp. 21–37. Elsevier,(2019). 10.1016/B978-0-12-815032-0.00003-2.

[47] Anwar, Raja Waseem, Anazida Zainal, Fatma Outay, Ansar Yasar, and Saleem Iqbal. BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. *Future Generation Computer Systems.* 96 (2019): 605–616, 10.1016/j.future.2019.02.004.

[48] Qureshi, Kashif Naseer, Muhammad Moghees Idrees, Jaime Lloret, and Ignacio Bosch. Self-assessment based clustering data dissemination for sparse and dense traffic conditions for internet of vehicles. *IEEE Access.* 8 (2020): 10363–10372, 10.1109/ACCESS.2020.2964530.

[49] J. Wang, J. Zhang, W. Bao, X. Zhu, B. Cao, and P. S. Yu. Not just privacy: Improving performance of private deep learning in mobile cloud. *in Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.* ACM, (2018), pp. 2407–2416, 10.48550/arXiv.1809.03428.

[50] Y. Liu, Y. Kang, C. Xing, T. Chen, and Q. Yang. A secure federated transfer learning framework. *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 70–82, (Jul./Aug. 2020), 10.1109/MIS.2020.2988525.

[51] K. Wei et al. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Trans. Inf. Forensics Security.*, vol. 15, pp. 3454–3469, (2020), 10.1109/TIFS.2020.2988575.

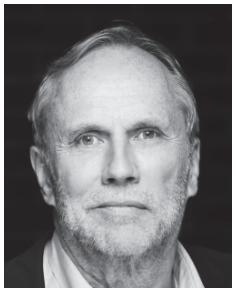
[52] K. Cheng et al. SecureBoost: A lossless federated learning framework. *arXiv:1901.08755. [Online].*, 10.48550/arXiv.1901.08755.

[53] N. Akhtar and A. Mian. Threat of adversarial attacks on deep learning in computer vision: A survey. *IEEE Access,*, vol. 6, pp. 14410–14430, (2018), 10.48550/arXiv.1801.00553.

Biographies

Muhammad Waleed received the B.Sc. and M.Sc. degrees from the University of Engineering and Technology (UET) at Peshawar, Pakistan, in 2015 and 2017, respectively. He then joined the Trust Data Analytics and Management Lab as a Researcher in the Department of Information and Communication Engineering, Chosun University, South Korea. Further, he is currently working as a PhD fellow in the IoTalentum program under the Marie Skłodowska-Curie Actions (MCSA) fellowship in the Department of Electronic Systems at Aalborg University Copenhagen (AAU), Denmark. His research interests include cyber security, Internet of Things, machine learning, trust management, and network communication. He is also interested in future networks, particularly edge computing and mobile communication.

Sokol Kosta holds a BSc, MSc, and PhD in Computer Science from Sapienza University of Rome, Italy. He was a postdoctoral researcher with Sapienza University and a visiting researcher with HKUST in 2015. He is currently associate professor at the Department of Electronic Systems at Aalborg University Copenhagen. He has published in several top conferences and journals including IEEE Infocom, IEEE Communications Magazine, and IEEE Transactions on Mobile Computing. His research interests include networking, distributed systems, and mobile cloud computing.



Knud Erik Skouby is professor emeritus, Aalborg University. Founding director of the center for Communication, Media and Information Technologies, Aalborg University-Copenhagen (2007–17) – a center providing a focal point for multi-disciplinary research and training in applications of CMI. Has a career as a university teacher and within consultancy since 1972; focus on ICT since 1987. Working areas: Techno-economic Analyses; Development of mobile/wireless applications and services: Regulation of telecommunications. Project manager and partner in a number of international, European and Danish research projects. He has served on a number of public committees within telecom, IT and broadcasting. Further served as a member of boards of professional societies; as a member of organizing boards, evaluation committees, and invited speaker on international conferences; published a number of Danish and international articles, books, and conference proceedings. Member of EUs Economic and Social Council 1994–98. Past dep. Chair IEEE Denmark. Editor in chief of Nordic and Baltic Journal of Information and Communication Technologies (NBICT); Chair of WGA in Wireless World Research Forum.