# Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices

Md. Abdur Rahman, *Senior Member, IEEE*, M. Shamim Hossain, *Senior Member, IEEE*, Nabil A. Alrajeh, and Fawaz Alsolami

***Abstract*—Medical IoT devices are rapidly becoming part of management ecosystems for pandemics such as COVID-19. Existing research shows that deep learning (DL) algorithms have been successfully used by researchers to identify COVID-19 phenomena from raw data obtained from medical IoT devices. Some examples of IoT technology are radiological media, such as CT scanning and X-ray images, body temperature measurement using thermal cameras, safe social distancing identification using live face detection, and face mask detection from camera images. However, researchers have identified several security vulnerabilities in DL algorithms to adversarial perturbations. In this article, we have tested a number of COVID-19 diagnostic methods that rely on DL algorithms with relevant adversarial examples (AEs). Our test results show that DL models that do not consider defensive models against adversarial perturbations remain vulnerable to adversarial attacks. Finally, we present in detail the AE generation process, implementation of the attack model, and the perturbations of the existing DL-based COVID-19 diagnostic applications. We hope that this work will raise awareness of adversarial attacks and encourages others to safeguard DL models from attacks on healthcare systems.**

***Index Terms*—Adversarial examples (AEs), COVID-19, deep learning (DL), medical IoT.**

## I. Introduction

RECENTLY, medical IoT devices have become increasingly connected to the Internet as part of the connected healthcare ecosystem. In order to automate healthcare processes, machine learning and deep learning (DL) applications are used to access hospitals' electronic health records and medical records generated by medical IoT devices. Due to the widespread epidemic caused by the human-to-human spreading pattern of COVID-19, healthcare authorities have used medical IoT devices to diagnose COVID-19 patients. In order to facilitate quicker diagnoses, DL models are used in areas, such as symptom inferencing through ultrasound, CT scan images, X-ray images, noninvasive face recognition-based hospital profile checking, ICU data collection, and others. However, researchers have shown that the existing DL algorithms have major flaws through which an attacker can compromise the security of the DL model itself [1].

Existing DL models use training data to train a set of parameters, which is then termed a model [2], [3]. During the inferencing phase, when given a new COVID-19 input sample, the DL model infers the corresponding output. For example, in the case of a DL algorithm that uses CT scan images as classifiers, a doctor inputs a new CT scan image and the model returns the classification results, i.e., positive or negative for COVID-19. Existing research has shown that all steps in a DL model, from training to inference, may be subject to adversarial attacks. Attackers can mislead DL models by perturbing certain aspects of the DL process without being discovered [4]. Fig. 1 provides an illustration of an adversarial example (AE) that can fool a DL algorithm into failing to recognize a photograph of a human wearing a mask by adding a skillfully crafted perturbation [5].

As shown in the figure, before the attack, the DL algorithm correctly classifies the input image and detects a mask on a subject with 98.7% accuracy, while below, after the input image is poisoned with the perturbation, the algorithm falsely classifies the subject as maskless with a confidence level of 99.13%. Data from medical IoT devices can be evaded, extracted, poisoned, and inferred by adversaries. This makes DL algorithms used in COVID-19 applications vulnerable to attacks. AE detection from the existing media, such as images, audio, and video, is becoming increasingly common. Agarwal *et al.* [5] have proposed a universal image-agnostic adversarial perturbation detection system that uses pixel value and PCA as its features and SVM as its classifier. A detailed survey of the existing AE for compromising DNN-based facial recognition systems along with effective countermeasures has been presented by Goswami *et al.* [6]. While many researchers have studied image-based AE, audio-based and speech-based AE are increasingly gaining attention. An adversarial attack

Manuscript received May 14, 2020; revised July 7, 2020; accepted July 29, 2020. Date of publication August 3, 2020; date of current version June 7, 2021. This work was supported by the Deanship of Scientific Research at King Saud University through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing. *(Corresponding author: M. Shamim Hossain.)*

Md. Abdur Rahman is with the Department of Cyber Security and Forensic Computing, College of Computer and Cyber Sciences, University of Prince Mugrin, Madinah Al Munawwarah 41499, Saudi Arabia (e-mail: m.arahman@upm.edu.sa).

M. Shamim Hossain is with the Chair of Pervasive and Mobile Computing, and the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Nabil A. Alrajeh is with the Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: nabil@ksu.edu.sa).

Fawaz Alsolami is with the Computer Science Department, King Abdulaziz University, Jeddah 21341, Saudi Arabia (e-mail: falsolami1@kau.edu.sa).

Digital Object Identifier 10.1109/JIOT.2020.3013710

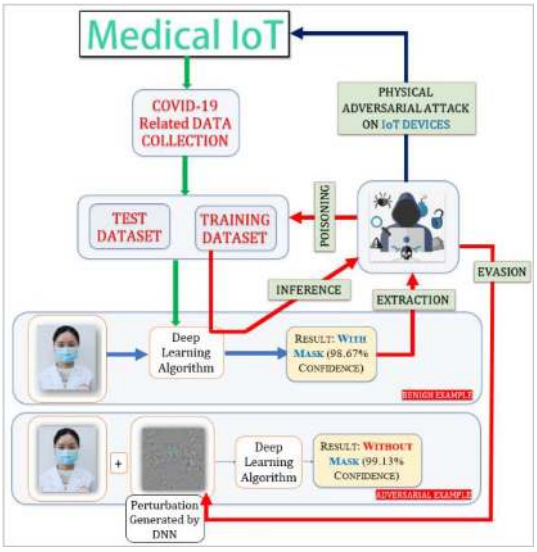


Fig. 1. Illustration of an AE as malware on a medical IoT application.

against DNN-based X-ray and CT scan recognition systems in which the classifier is targeted for both targeted and non-targeted AEs is shown in [7]. Yahya *et al.* [8] have proposed a design using a targeted watermark that generates AEs and techniques to evaluate the impact of the embedded AEs. A novel method of generating AE using generative adversarial networks (GANs) from benign input images, instead of only focusing on the constraints that make the generated perturbed image look similar to the benign image, is presented in [9].

In order to mitigate AE, researchers have proposed multiple solutions. For example, the work presented in [10] used blockchain to store the existing known and benign attributes and parameters of each of the DL models and then turned them into explainable AI allowing high-level users to verify whether a particular model has been compromised or not. Xu *et al.* [11] developed from images with adversarial patches and audio media a lightweight AE detection model that can mitigate physical adversarial attacks. Blockchain was used by Goel *et al.* [12] to stop the alteration of input data, feature vectors, model attributes, classifiers, and the final decision-making process. In order to mislead the attacker's classifier, Jia *et al.* [13] proposed an AE defense mechanism that can effectively defend against membership inference attacks.

While researchers have made extraordinary advancements in the design of defense mechanisms against AE using different types of media, the attacks on medical IoT devices used in COVID-19 diagnosis still require further study. Because healthcare databases and services have been subject to ransomware attacks in the past, and because healthcare systems are currently overwhelmed with COVID-19 patients, the study of these adversarial attack vectors is urgent, especially to uncover the vulnerabilities of medical IoT devices using DL algorithms. However, little research has been conducted in this domain. Although much work has been done in the area of AE, to the best of our knowledge, this is one of the first studies of adversarial attacks on COVID-19 DL applications. The main innovations of this article are as follows.

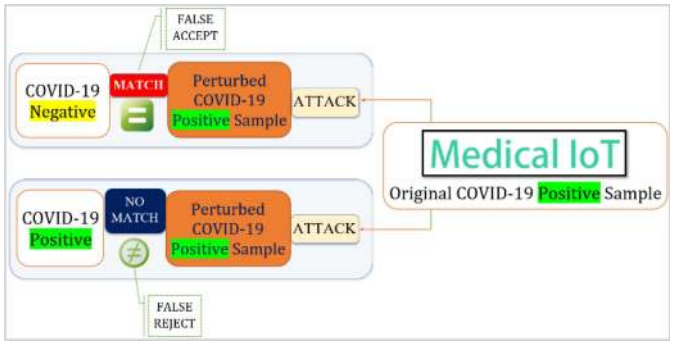


Fig. 2. Design of AE to generate false acceptances (creating the false impression that COVID-19 negative and positive samples are equal) and false rejections (a truly positive COVID-19 sample is labeled negative).

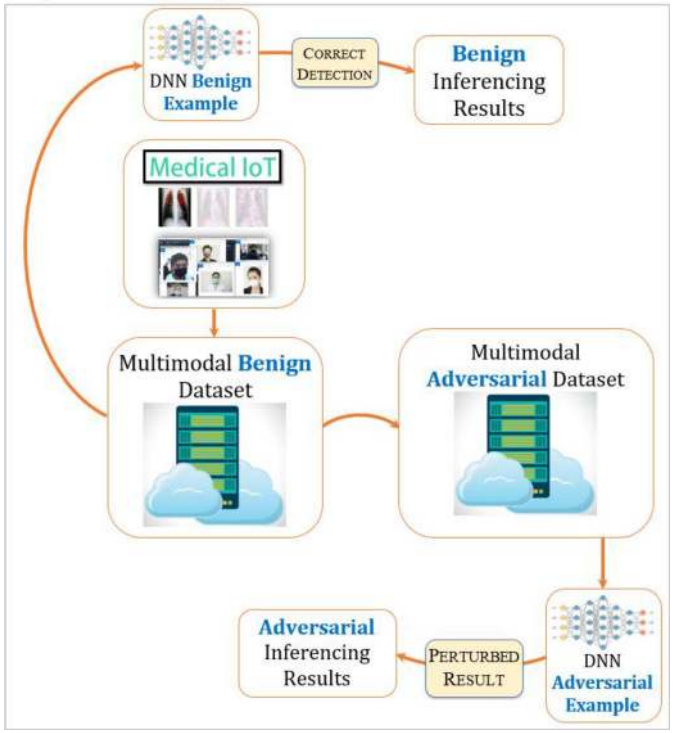


Fig. 3. Illustration of an AE fooling a DL algorithm into either false rejection or false acceptance.

1) We have studied six different DL applications used to diagnose COVID-19.
2) We have researched the relevant AE to mount attacks on the COVID-19 diagnostic systems.
3) We have presented multimodal AE attacks on diversified COVID-19 diagnostic systems.

The remainder of this article is organized as follows. Section II presents system design as an AE. Section III outlines the system implementation. The test results are summarized in Section IV, and Section V concludes this article and introduces our vision for future study.

## II. COVID-19 Adversarial Example Framework Design

*Proposed AE Generation Environment:* Since COVID-19 results in respiratory disorders, different medical IoT-based

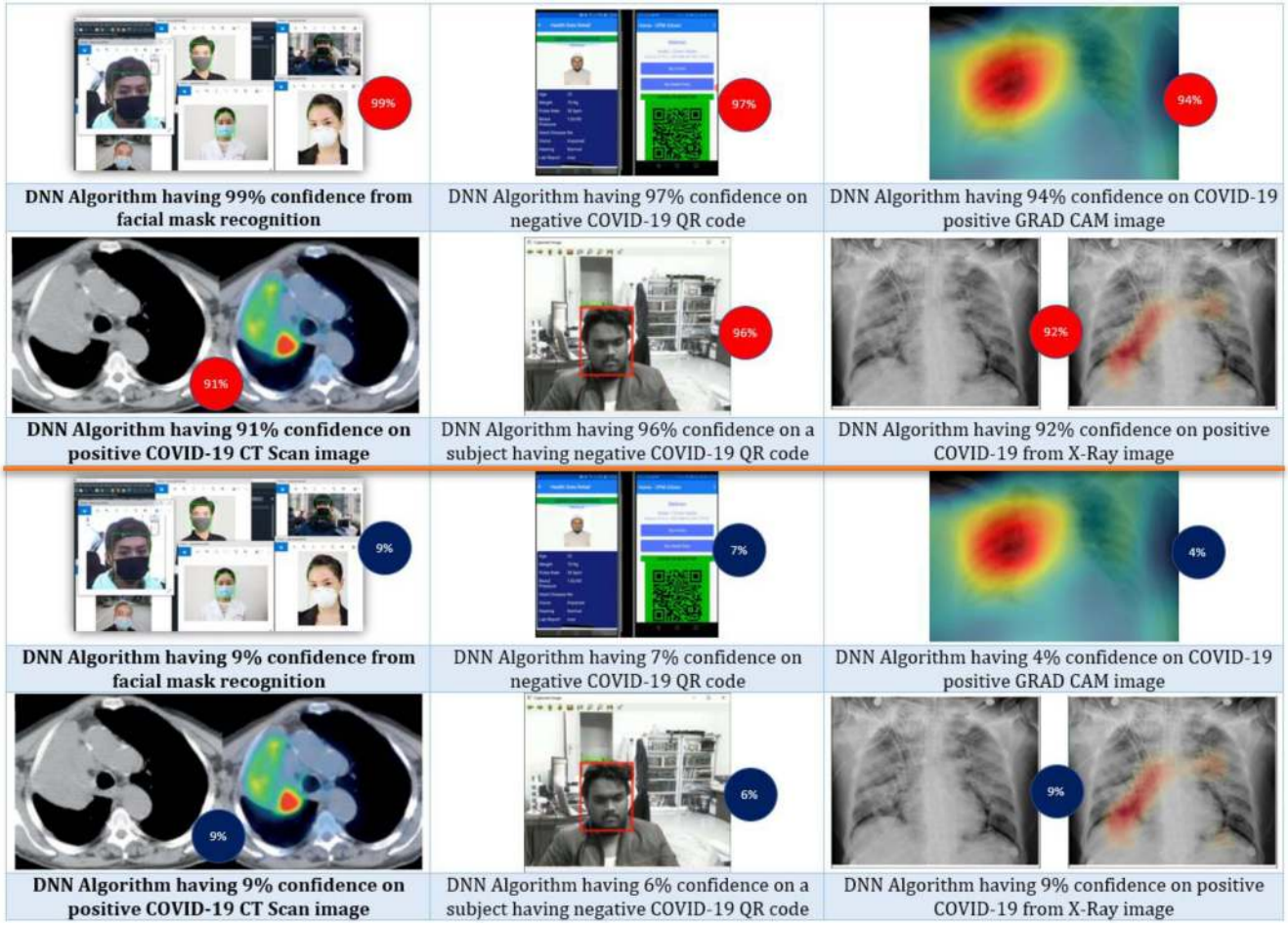


Fig. 4. (Top two rows with red circles) Six COVID-19 DL-based applications have been tested within the scope of this research with the normal recognition rate shown within the red circles. (Bottom two rows with blue circles) After a DL-based adversarial perturbation attack, the recognition ability of DL algorithms is compromised, though human experts can still recognize the actual class.

testing methods are available that can lead to a diagnosis, detection, and recognition of the viral infection. Researchers have used DNN algorithms to recognize COVID-19 symptoms from various testing modalities. In this article, we have studied researchers' existing works and open source initiatives, testing and evaluating the ability of candidate DL algorithms to diagnose COVID-19 from medical IoT devices [14]. Some examples of IoT media used are radiological media, such as CT scan and X-ray images and face mask detection from camera images. Fig. 2 shows a generic AE in which DL-based perturbations are added to the existing COVID-19 benign samples to craft attacks on either targeted or nontargeted samples, which results in either a false acceptance or false rejection scenario.

Fig. 3 illustrates the architecture through which benign and AE data sets are used to train benign and adversarial DL algorithms. In the case of a white-box attack, we assume an attacker has access to the underlying architecture, gradient, training process, training data, the defense method, and parameters of the victim learning model. In the case of a black-box attack, an attacker is assumed to have only access to the underlying DL network's input/output and the training data set. In the case of a gray-box attack, the adversary has knowledge about the target DL network, its gradients and parameters, and data used during the training process, except the defense mechanism. We have also developed a DL algorithm that misclassifies facial recognition and works in a nontargeted mode [15]. In this mode, the DL algorithm fails to recognize the face in the image or video. The AE used attributes ResNet-101 with kernel size = 1 and type = uniform. We have used ResNet-101, kernel size = 30, and type = uniform and ResNet-101, kernel size = 300, and type = uniform. Behind the scenes, the DL prediction model was fooled to predict the input sample as a microphone, a Windsor tie, and a tie, respectively.

Fig. 4 shows the six targeted applications we built for the proof of concept. The purposes of these applications are to: 1) recognize whether a subject is wearing a mask from a live camera feed; 2) maintain DL-based QR codes as immunization certificates; 3) add explainability of GRAD-CAM DL algorithms; 4) recognize COVID-19 from CT scan images; 5) detect noninvasive biometrics and identify social distancing from a live camera feed; and 6) recognize COVID-19 from X-ray image analysis. As the figure shows, we have developed six AE DL models that can add noise or perturbations specific to the type of media used in COVID-19 diagnosis.

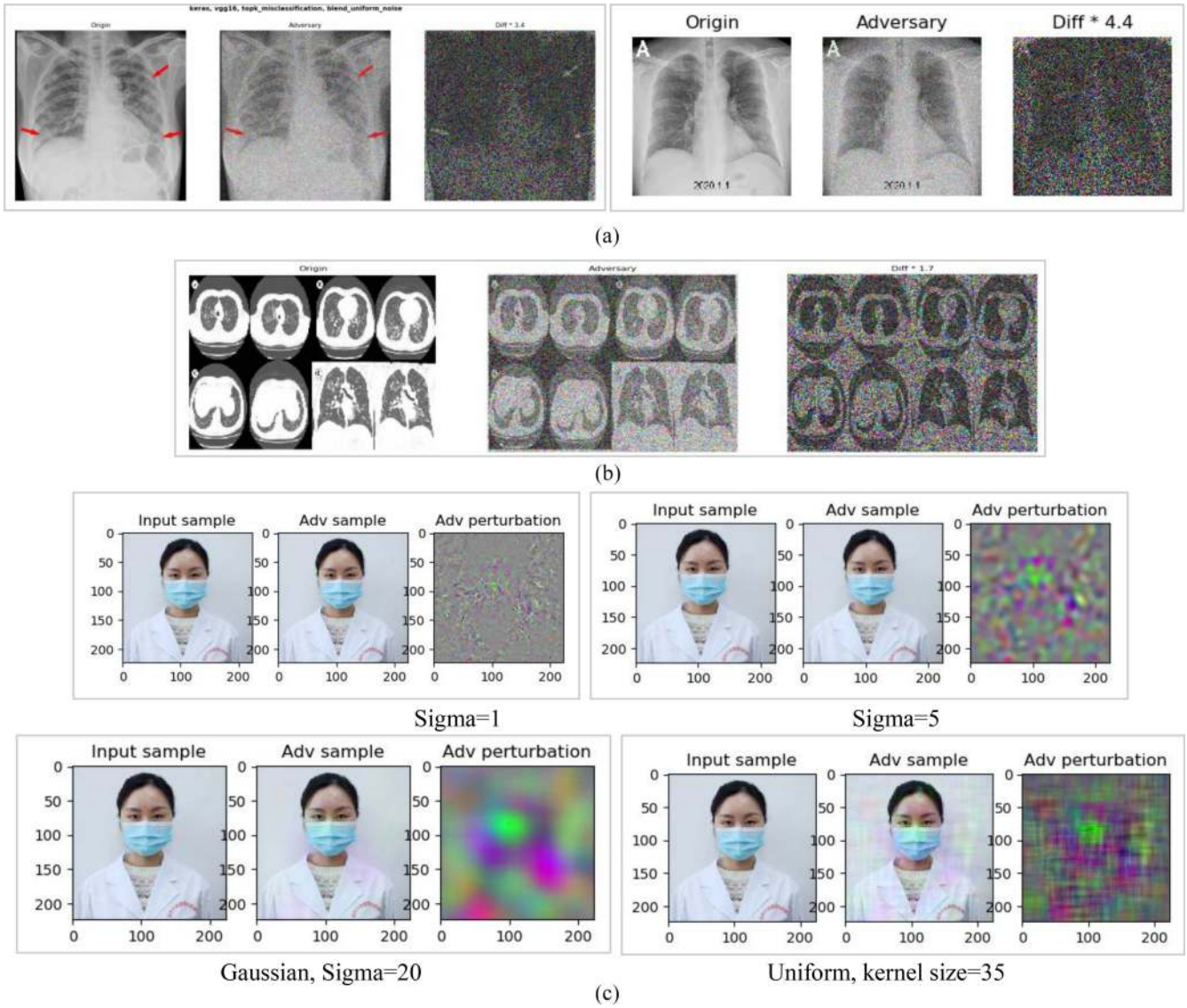


Fig. 5. Illustration of a nontargeted AE fooling different COVID-19 diagnostic measures by fooling the (a) DL model to recognize COVID-19 from X-ray images, (b) DL model to recognize COVID-19 from CT scan images, and (c) face mask recognition processes.

## III. Proof of Concept Implementation

We have developed the sample applications shown in Fig. 4 to test their suitability with regards to COVID-19 and AE attacks. We have implemented each application as part of the proof of concept through various opensource libraries, such as PyTorch, Tensorflow, Keras, and CV2. OpenPose, Docker, Django, NGINX, React, Plotly, and Dash have been used for the Web framework. On an Ubuntu Linux system, we have outfitted the local edge server with NVIDIA GeForce RTX 2080 Ti 11-GB GPU drivers, CUDA 10.0, and cuDNN v7.6.4 for TensorFlow 2.0

Different AE models have been developed to perturb different COVID-19 diagnosis applications. For example, an application has been created to perturb a COVID-19 social distancing alert system that is based on regular and CCTV cameras. The DL algorithm is designed to measure closeness and identify human bodies standing 6 ft apart by leveraging both YoloV4 and Darknet using the COCO data set. We have designed an AE perturbation of the classifier that can drop the "person." Similarly, we have designed an AE classifier for each of the six COVID-19 applications shown in Fig. 3. In each of these cases, we have input an original COVID-19 diagnostic sample into our designed AE generator, which adds a trained patch to the base DL network responsible for COVID-19 phenomena detection.

The perturbation added to the DL network is responsible for compromising the rankings of the recognition results by decreasing the true-positive scores while increasing the false-positive scores. In order to assess the attack success rate, several metrics have been defined, such as true-positive class loss and true-positive shape loss. The former is concerned with decreasing the score of the genuine class by increasing the score of the AE-proposed perturbed class. The latter is concerned with misplacing the location of the bounding box by pointing the correct object detection algorithm to a spatial location further away from the desired object location, thereby

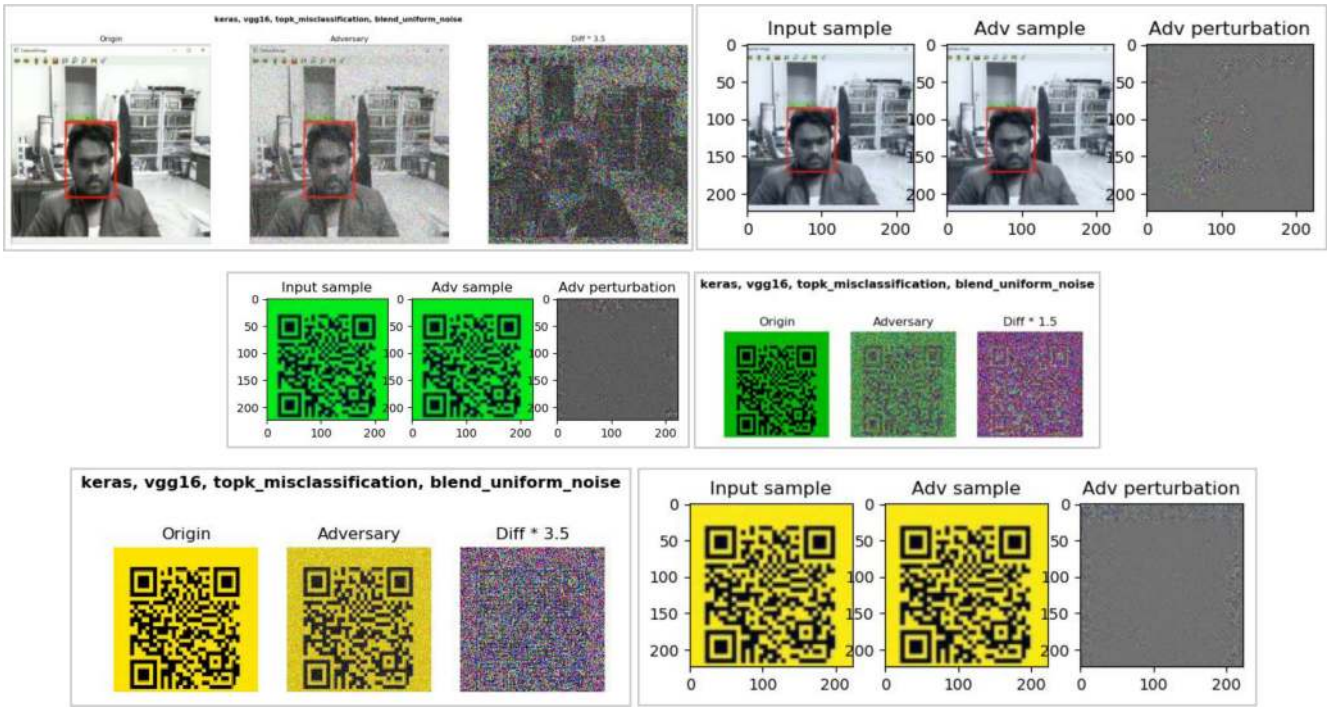


Fig. 6. Illustration of a targeted AE attacking a DL-based QR code generation system to alter COVID-19 test results to a target color, i.e., green, red, or yellow.

causing misclassification. Fig. 5 shows a subset of the implemented AE algorithms for perturbing X-ray images, CT scan images, and images containing individuals wearing face masks in public places.

Fig. 6 shows an example attempt at the implementation of AE in a COVID-19 QR code management system that relies on human face recognition as a noninvasive biometric identifier to obtain each user's immunization certificate. The application uses blockchain to store the QR code status, COVID-19 status (+ve, −ve, or suspect), and off-chain link to the encrypted face image. Every time a user's COVID-19 status is checked, the user has to show his or her face and QR code and share it with the face recognition DL application, which pulls the user's immutable data from the blockchain. In order to attack the application, we have taken a sample user's image and QR code and used them as a backdoor. After successful training, the AE was able to poison the actual DL application and make targeted attacks as shown in Fig. 6. The speech AE algorithm was tested against 80 normal users' coughing sounds, 100 AEs, and 20 COVID-19 patients' coughing sounds. All of the audio samples had a 16-kHz sampling rate. The computer that we used had an NVIDIA GeForce RTX 2080Ti GPU. The average time it took to generate speech AE for a 1-s normal sound file was approximately 55 s.

## IV. Test Results

We have tested the existing adversarial methods in this study, including FGSM, MI-FGSM, Deepfool, L-BFGS, C&W, BIM, Foolbox, PGD, and JSMA [16]. Our goal is to compromise the existing DL algorithms so that each recognition system misclassifies data with the fewest number of perturbations. We assume that evasion, poisoning, extraction, and inference-type attacks are all possible and that the complete knowledge of each DL model is available to generate white-box attacks. We also assume that both the training and test data sets can be poisoned. In the case of nontargeted attacks, our algorithms aim to minimize actual class activation so that any class other than the correct one will be identified. In the case of targeted attacks, our AE algorithms are designed to predict a specific incorrect COVID-19 class, as designing a COVID-19 diagnostic system that classifies a positive sample as negative is far more dangerous than the one that interprets its class as unknown.

Fig. 7 shows two important parameters we observed during AE generation: 1) adversarial loss and 2) the magnitude of distortions. Each AE targeting a COVID-19 application is designed separately, as the underlying DL models are all different. Fig. 7 shows an example of a radiological AE that has been developed to poison X-ray-based and CT-scan-based COVID-19 diagnostic applications. We have looked at these two parameters to obtain the optimal value of perturbations that will yield the best misclassification results.

Fig. 8 shows the perturbation values and adversarial losses for 9000 iterations. This curve provides us with a way to measure the quality of the AE generation process. The white-box AE was tested using Python-based Foolbox to attack PyTorch, Keras ResNet50, and TensorFlow models. Using Foolbox, we can alter the maximum likelihood of the underlying COVID-19 samples. Foolbox API can be configured to use underlying attack models such as FGSM. In the case of radiological DL applications, the attack model continuously monitors the gradients until the actual label is misclassified. In order to mount a black-box attack, we used Clarifai REST API models and manipulated SGD to monitor the scores and decrease classifier

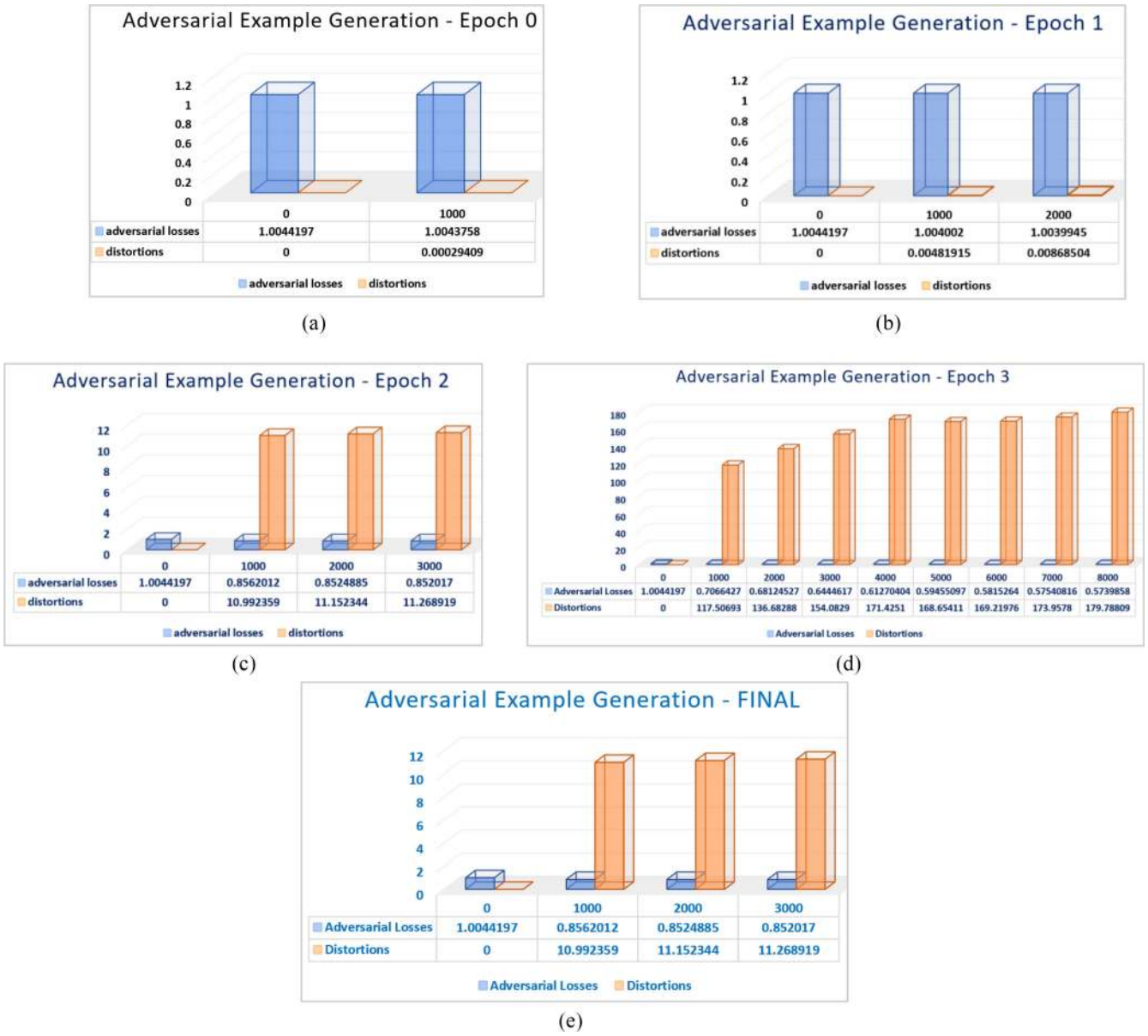


Fig. 7. Test results of AE generation for attacks on radiological media, such as X-ray and CT scan images: batch iterations during (a) epoch 0, (b) epoch 1, (c) epoch 2, (d) epoch 3, and (e) final adversarial loss and distortions values.

performance. In order to test the deepfake AE, we used Google cloud SDK coupled with VNC viewer to visualize the GUI on the NVIDIA Tesla P100 GPU-enabled instance on the cloud. Using Google DL VM, we tested different DL image combinations, such as PyTorch 1.3.0 with fastai m38 and TensorFlow 1.15 m41 with CUDA 10.0. We installed Faceswap and VNC server on the Google DL VM. Additionally, we stole the existing DL models, even those in the black-box mode. The existing DL as a Service (DLaaS) models not only reveal the final label but the confidence values as well. This valuable information is fed into our AE DL model to reverse-engineer and uncover the weights of the intermediate nonlinear layers, as model stealing is much more efficient than training a new adversarial model from scratch. We tested the effects of poisoning the training data set for both targeted and non-targeted attacks (lowering prediction accuracy). We observed the results of different metrics, such as the percentage of the training set that needs to be poisoned or perturbed to attain certain reduction percentages in the recognition rate. We also observed different combinations of accuracy as well as false-positive and false-negative rates with respect to the ratio of the set of original data sets and the set of poisoned data sets.

Additionally, we tested for DL inference poisoning. We leveraged another type of attack that has been found to be very efficient on the existing black-box DL models, backdoor attacks. The backdoor provides access to the training phase of the model and allows us to update the model. In order to create a backdoor, we first trained our model with a poisoned set of targeted training data sets. We applied this AE to an existing one-shot learning-based facial recognition model. Our developed algorithm learns both the target regions as well as target styles of the noise that will be added to the original test image. A similar procedure is

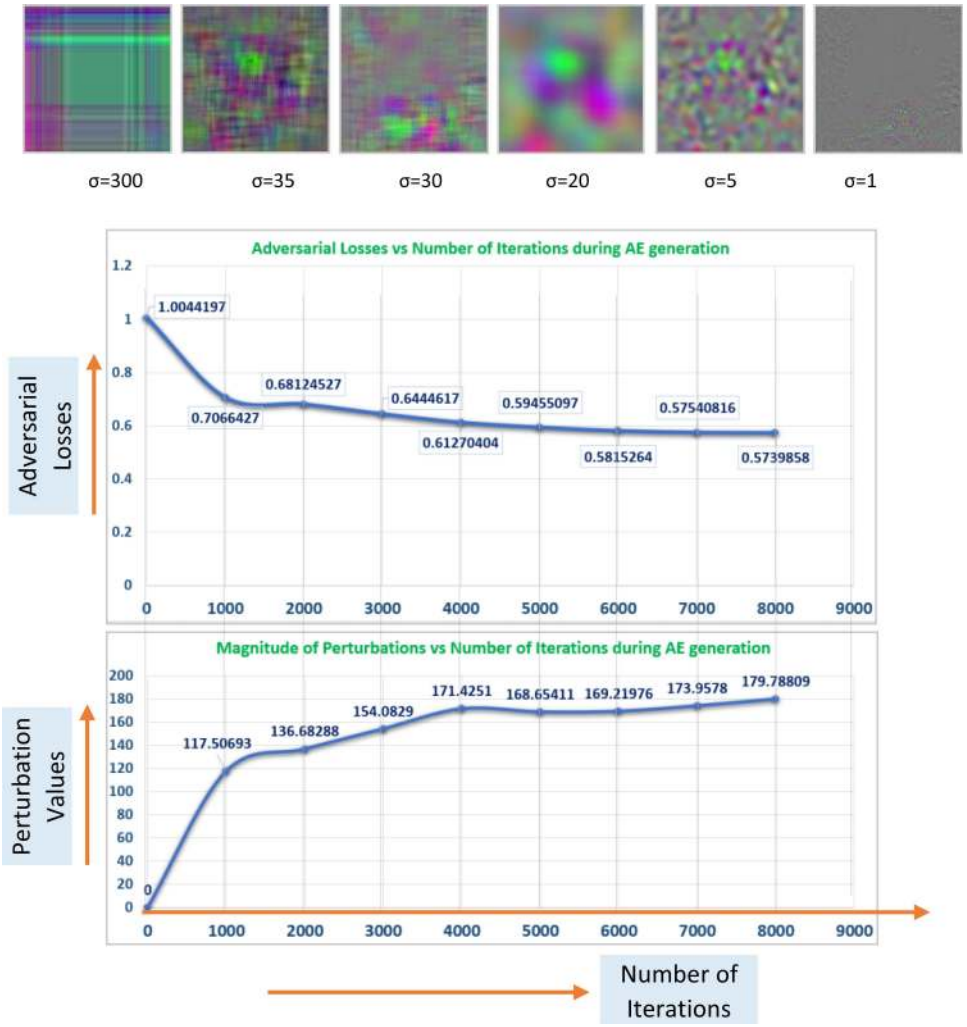


Fig. 8. Test results of AE generation: effect of $\sigma$ values.

performed for other types of media such as audio. During the adversarial learning phase, the algorithm learns about misclassification rates, the average number of changed features, adversarial strength, content preservation, stealthiness scores, and smoothness enhancements.

Due to the widespread availability of COVID-19 data sets—such as the CORD data set from the Allen Institute for AI—and the fact that some data sets include both COVID-19 patients' public data and their attributes, we could poison data as well as launch classified inference attacks. We could inject fake audio, images, and other types of media into the training data set so that the learned classifier is misconfigured. Our developed algorithm adjusts the hyperparameters of the added noise threshold as shown in Figs. 7 and 8 that would fool humans as well as DL-based defense mechanisms. Due to the very specific nature of COVID-19 patients' data sets, which may include CT scan images, we only need to add random small white noise patches in order to change the state of the lung, e.g., dark black regions made to look whiter or white regions made to look blackish, depending on the target of the attack.

## V. Conclusion

The present study examined nine COVID-19 DL applications that allow for the rapid diagnosis of the pathogen. These six modalities of DL-based COVID-19 diagnosis have been widely used by researchers. However, researchers have discovered different types of attacks on these nine types of DL applications. We tested these six applications from opensource libraries and carefully observed the models in order to design AEs for each type and identify the vulnerabilities of these models. In this article, we have presented our findings, which show promising results. We have found that the existing DL applications are vulnerable to AE attacks, requiring further research, attention, and implementation of appropriate defense mechanisms, safeguards, and controls before these applications are used in real-life healthcare [17] facilities.

In the future, we will target to improve the efficiency of DL poisoning. We also plan to target more types of AE applications used in the COVID-19 diagnostic domain. In this research, we only studied and presented on the generation of AE and deployment results. Although we tested only a few machine learning algorithms and their vulnerabilities, we will

expand our horizons by targeting remaining popular frameworks, such as XGBoost, CatBoost, GPy, and others. In the future, we will study the detection and defense mechanisms used in the COVID-19 DL poisoning process. In particular, we will investigate the use of blockchain to mitigate AE attacks on COVID-19 applications. Another key area that we will explore is transferable AE, in order to suggest better defense mechanisms against inference and model poisoning. We did not explore the AEs targeting COVID-19-related specific objectives such as fooling DL algorithms through physical or real-life object perturbations. Our algorithms must be tested against real-world attacks, as these require a larger number of perturbations that will be visible to human subjects. We will also research additional attack vector dimensions, such as pose, facial expression, changing target region, distance and elevation from the camera, and others within the poisoned data set, in order to examine how adversarial loss in a targeted deep neural network can work against adversarial defense mechanisms. Since medical IoT devices are frequently targeted by malware, we intend to study the use of static and dynamic malware in the form of perturbations and noise vectors to generate AEs. We will use industry-standard tools, such as IBM ART, to evaluate and defend our algorithms against adversarial threats.

## REFERENCES


[1] M. A. Rahman *et al.*, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[2] M. S. Hossain, G. Muhammad, and N. Guizani, "Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics," *IEEE Netw.*, vol. 34, no. 4, pp. 126–132, Jul./Aug. 2020.

[3] M. A. Rahman, M. S. Hossain, N. A. Alrajeh, and N. Guizani, "B5G and explainable deep learning assisted healthcare vertical at the edge: COVID-I9 perspective," *IEEE Netw.*, vol. 34, no. 4, pp. 98–105, Jul./Aug. 2020.

[4] K. Ren, T. Zheng, Z. Qin, and X. Liu, "Adversarial attacks and defenses in deep learning," *Engineering*, vol. 6, no. 3, pp. 346–360, 2020, doi: 10.1016/j.eng.2019.12.012.

[5] A. Agarwal, R. Singh, M. Vatsa, and N. Ratha, "Are image-agnostic universal adversarial perturbations for face recognition difficult to detect?" in *Proc. IEEE 9th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, Redondo Beach, CA, USA, 2018, pp. 1–7, doi: 10.1109/BTAS.2018.8698548.

[6] G. Goswami, A. Agarwal, N. Ratha, R. Singh, and M. Vatsa, "Detecting and mitigating adversarial perturbations for robust face recognition," *Int. J. Comput. Vis.*, vol. 127, nos. 6–7, pp. 719–742, 2019, doi: 10.1007/s11263-019-01160-w.

[7] X. Ma *et al.*, "Understanding adversarial attacks on deep learning based medical image analysis systems," *Pattern Recognit.*, to be published, doi: 10.1016/j.patcog.2020.107332,

[8] Z. Yahya, M. Hassan, S. Younis, and M. Shafique, "Probabilistic analysis of targeted attacks using transform-domain adversarial examples," *IEEE Access*, vol. 8, pp. 33855–33869, 2020.

[9] W. Zhang, "Generating adversarial examples in one shot with image-to-image translation GAN," *IEEE Access*, vol. 7, pp. 151103–151119, 2019.

[10] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 10, no. 1, pp. 1–13, 2020, doi: 10.1002/widm.1340.

[11] Z. Xu, F. Yu, and X. Chen, "LanCe: A comprehensive and lightweight CNN defense methodology against physical adversarial attacks on embedded multimedia applications," in *Proc. 25th Asia South Pac. Des. Autom. Conf. (ASP-DAC)*, Beijing, China, 2020, pp. 470–475, doi: 10.1109/ASP-DAC47756.2020.9045584.

[12] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "Securing CNN model and biometric template using blockchain," in *Proc. 10th Int. Conf. Biometrics Theory Appl. Syst. (BTAS)*, 2019, pp. 1–6.

[13] J. Jia, A. Salem, M. Backes, Y. Zhang, and N. Z. Gong, "MemGuard: Defending against black-box membership inference attacks via adversarial examples," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2019, pp. 259–274, doi: 10.1145/3319535.3363201.

[14] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[15] K. Kakizaki and K. Yoshida, "Adversarial image translation: Unrestricted adversarial examples in face recognition systems," in *Proc. CEUR Workshop*, vol. 2560, 2020, pp. 6–13. [Online]. Available: http://ceur-ws.org/Vol-2560/

[16] J. Fei, Z. Xia, P. Yu, and F. Xiao, "Adversarial attacks on fingerprint liveness detection," *EURASIP J. Image Video Process.*, vol. 2020, no. 1, pp. 1–11, 2020, doi: 10.1186/s13640-020-0490-z.

[17] M. S. Hossain and G. Muhammad, "Emotion-aware connected healthcare big data towards 5G," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, Aug. 2018.



**Md. Abdur Rahman** (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2010.

He is an Associate Professor with the Department of Cyber Security and Forensic Computing and the Director of the Scientific Research and Graduate Studies, University of Prince Muqrin, Madinah Al Munawwarah, Saudi Arabia. He has authored more than 120 publications. He has one U.S. patent granted and several are pending.

Dr. Rahman has received more than 18 million SAR as research grant.

**M. Shamim Hossain** (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2009.

He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He has authored and coauthored more than 275 publications. His research interests include cloud networking, smart environment (smart city and smart health), AI, deep learning, edge computing, Internet of Things, multimedia for healthcare, and multimedia big data.

Prof. Hossain is on the Editorial Board of the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE MULTIMEDIA, IEEE NETWORK, IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, and the *Journal of Network and Computer Applications*. He is a Senior Member of ACM.

**Nabil A. Alrajeh** received the Ph.D. degree in biomedical informatics engineering from Vanderbilt University, Nashville, TN, USA, in 2001.

He is currently a Professor of health informatics with the Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh, Saudi Arabia, and the Rector with Prince Mugrin Bin Abdulaziz University, Madinah Al Munawwarah, Saudi Arabia.

**Fawaz Alsolami** received the Ph.D. degree in computer science from the King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, in 2016.

He is an Assistant Professor with the Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include artificial intelligence, deep learning, and data science.