Special Section: Security, Trust and Privacy Solutions for Intelligent Internet of Vehicular Things

Deep Learning-Based Intrusion Detection System for Internet of Vehicles

Imran Ahmed
Institute of Management Sciences, Hayatabad

Awais Ahmad
Air University of Islamabad

Gwanggil Jeon
Xidian University and Incheon National University

***Abstract*—The growth of the Internet of Things (IoT) has resulted in several revolutionary applications, such as smart cities, cyber-physical systems, and the Internet of vehicles (IoV). Within the IoV infrastructure, vehicles are comprised of various electronic intelligent sensors or devices used to obtain data and communicate the necessary information with their surroundings. One of the major concerns about the implementation of these sensors or devices is data vulnerability; thus, it is necessary to present a solution that provides security, trust, and privacy to communicating entities and to secure vehicle data from malicious entities. In modern vehicles, the controller area network (CAN) is a fundamental scheme for controlling the interaction among different in-vehicle network sensors. However, not enough security features are present that support data encryption, authorization, and authentication mechanisms to secure the network from cyber or malicious intrusions such as denial of service and fuzzy attacks. An intrusion detection system is presented in this work based on the deep learning architecture to protect the CAN bus in vehicles. The VGG architecture is used and trained for different network intrusion patterns in order to detect malicious attacks.**

Digital Object Identifier 10.1109/MCE.2021.3139170
Date of publication 29 December 2021; date of current version 6 December 2022.

The experiments are performed using the CAN-intrusion-dataset. The experimental findings demonstrate that the presented deep learning system significantly reduces the false positive rate (FPR) compared to the conventional machine learning techniques. The overall accuracy of the system is 96% with FPR of 0.6%.

Today, the Internet of Things (IoT) has received prominent attention from researchers. It is a system that consists of different sensors or devices connected to each other or attached to different things allowing the sharing of data and information via the Internet connection. IoT technology gave birth to the concept of the Intelligent Internet of Vehicles (IoV), considered to be more effective and safer for users, as illustrated in Figure 1. Modern smart vehicles consist of a variety of hardware/devices/modules, such as electronic control units (ECUs), telematics control unit (TCU), and other sensors managed by complex software elements. These modules are responsible for controlling the actuators in a vehicle. IoV is an integrated and open network system that connects vehicles, human intelligence, nearby environments, and public internet connections. However, these crucial levels of connectivity have made smart vehicles vulnerable toward different types of cyberattacks. Moreover, it may conflict with various vehicle features, including its intelligence or communication systems, thus; threatening the security, trust, and privacy (STP) of vehicles and putting passengers' lives at risk.

IoV is an extremely relevant target for intruders or attackers to misuse private and massive driving-aid information. Intruders may able to insert and penetrate malicious messages with various internal and external interfaces. These interfaces include physical access to the on-board diagnoses (OBD) system, which controls speed, emissions, distance, and other information in vehicles, short-range wireless access such as Bluetooth, long-range wireless access, such as Wi-Fi mobile network, and TCU, into the CAN traffic. It can help attackers or intruders to insert remote attack surfaces that enable ECU's to compromise by accepting malicious messages. Therefore, it is necessary to discuss solutions that provide STP to communicating entities and to secure vehicle data from mali-cious attacks. Various in-vehicle network protocols are available to manage and control communication between in-vehicle network sensors.[1] Among all, CAN is one of the most popular and broadly adopted protocols in the automobile sector and is recognized as the de-facto model for vehicular networks.[2,3]

Nowadays, researchers utilized various artificial intelligence based techniques and presented intrusion detection systems to classify and detect different kinds of malicious attacks. In the CAN bus protocol, intrusion detection controls communication and transmission traffic between ECUs and classifying any abnormal traffic behavior. In this work, we present an IoT-enabled intrusion detection system that is based on a deep learning architecture. The system can identify two different kinds of CAN attacks, including DoS and Fuzzy. The deep learning structure is based on the VGG-16 architecture. First, the dataset samples are converted into byteplot images (every byte resembles one pixel in a grayscale image). After, that the VGG-16 architecture[4] is trained on CAN-intrusion-dataset.[5] The transfer learning approach is adopted, and bottleneck features (filter activation maps) are extracted using convolutional layers of the VGG-16 architecture. Fully connected layers further utilize the bottleneck features for the detection of different malicious or cyberattacks. The major contribution is provided as follows.

- An IoT-enabled intrusion detection system is introduced. The system uses a deep learning architecture that strengthens the CAN bus protocol and communication between in-vehicle network sensors.
- The system delivers successful intrusion detection results by identifying different types of cyberattacks without any modification in the CAN protocol; hence, it can be implemented in common vehicles.
- Furthermore, the comparison of the system is made with other conventional machine learning techniques. The experimental results exhibit the efficiency of a deep learning system with good accuracy.

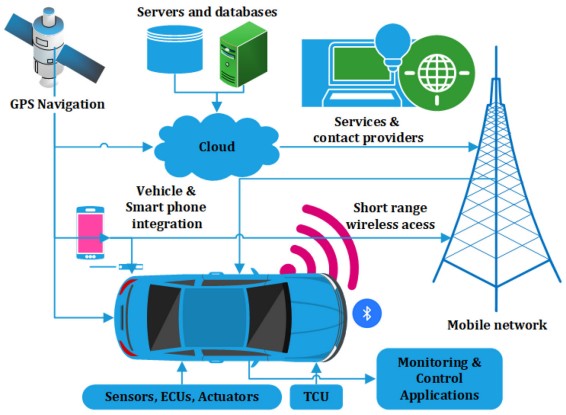

Figure 1. IoT technology in modern smart vehicles.

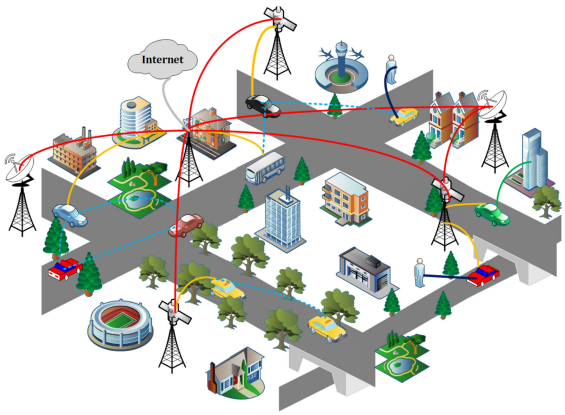

Figure 2. General IoV infrastructure: IoV technology provides a communication network environment. Vehicles communicate with other objects or things via Internet connections. The yellow lines show communication links between base stations and vehicles; the blue lines point V2V communication links; the black lines are used for V2H; the green lines demonstrate V2I communication links.

The rest of this article is organized as follows. The "Related Work" Section reviews different methods used for the detection and classification of cyberattacks. The "Intrusion Detection System for the IoV" Section explains an IoV infrastructure and developed intrusion detection system. The experimental results and performance evaluation of the developed system are illustrated in the "Experimental Results" Section. Finally, the main conclusions of this work with some possible future trends are given in the "Conclusion and Future Work" Section.

RELATED WORK

Intrusion detection has been considered as one of the important topics by researchers in vehicle network communication systems Tian *et al.*[6] presented a machine learning based system that utilized gradient-boosting decision tree, suitable for large data processing, and provided an effective ongoing information security defense system. Kang and Wang[7] suggested a deep neural network for malicious attacks classification, i.e., normal and attack packets in CAN bus, Alshammari *et al.*[8] presented a machine learning technique to classify the malicious attacks in vehicular adhoc networks by applying K-Nearest Neighbour (KNN) and Support Vector Machine (SVM) classifier.

Verma *et al.*[9] investigated various machine learning classification algorithms and presented an intrusion detection system that detects DoS attacks. Li *et al.*[10] provided solutions for CAN bus anomaly detection by using regression learning. Zhang *et al.*[11] also studied deep learning techniques based on gradient descent with momentum and adaptive gain for the intrusion detection system.

INTRUSION DETECTION SYSTEM FOR THE IoV

An intrusion detection system is presented in this work for the IoV. It is an immediate connection of the portable Internet in vehicles and IoT. IoV infrastructure or technology, demonstrated in Figure 2 is referred to as effective portable communication systems that allow communication between public networks and vehicles applying vehicle-to-sensor, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-human (V2H) interactions. It helps us to collect and share the information from/on vehicles, streets, roads, highways, traffic control units, and their surroundings. Furthermore, it highlights the sharing, processing, computing, and safe delivery of data on different information platforms.

The IoV supports providing a smart vehicle communication environment for smart cities, but it also suffers from security issues. As each vehicle is equipped with many smart sensors and devices that provide corresponding communication with other objects, including GPS for geographical information, radar for estimating the relevant signals between vehicles, T-box's that controls data

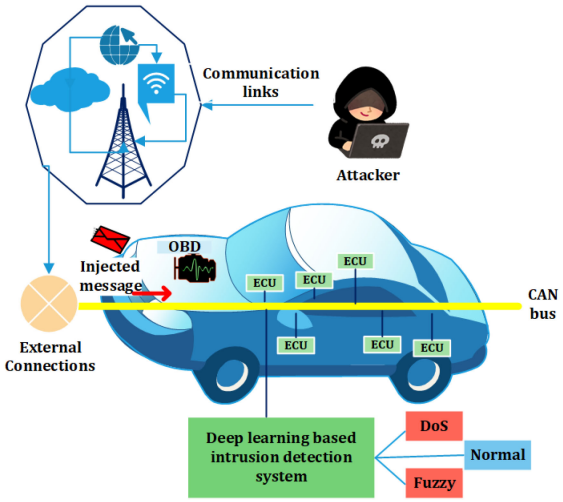

Figure 3. CAN-bus attack scenario, the intruders or attackers sent malicious messages using external communication links. These attack messages are received at OBD port/system. The deep learning-based intrusion detection system detects these attacks and prevents vehicles from false communications.

processing and communication between vehicles other types of equipment. The internal data of the vehicle is transferred through the CAN bus during the communication process.

In Figure 3, as illustrated, a modern vehicle consists of ECUs for information collection; few of them are connected through the CAN bus. These ECUs communicate messages between or within vehicles by utilizing the CAN bus protocol, which is efficient due to its low expense and centralized system for in-vehicular network operations. However, due to low-security features, it usually undergoes through different intruders attacks. The attackers can easily inject malicious data packets (DoS and fuzzy) into CAN message by utilizing communication interfaces. The CAN frame message is comprised of the following seven fields.

- *Start of frame:* First predominant bit notifies a start of communication of CAN message to all nodes.
- *Arbitration field:* Consists of two components; the identifier (describes the ID of the frame, utilized throughout the arbitration process) and remote transmission request (defined according to the type of the CAN frame).
- *Control field:* Indicate two reserved and four bits as data length code.
- *Data field:* Carries the real data message conveyed to other nodes.
- *CRC field:* Assures the efficacy of the message. All connections that accept the information confirm the message, using this field.
- *ACK field:* Acknowledgment bits including ACK and delimiter part. A connection that accepts the actual normal message returns the ACK part. It restores the ACK part, a suspended bit to the dominant bit (i.e., logical 1 to 0).
- *End of frame:* Infers the last head of the CAN message frame.

Deep Learning-Based Intrusion Detection System

As discussed earlier, attackers can easily access the CAN bus due to the in-vehicle network's vulnerability and absence of security features. In this work, we presented a smart intrusion detection system to investigate, classify, or detect two kinds of attacks, i.e., DoS and Fuzzy.

- In DoS attacks, too many requests are transferred to the server of the network. As wireless technologies are used in vehicles, thus, it is obvious to drive a DoS attack. The attacker and intruder can insert higher priority information or messages in a very small time period.
- In fuzzy attacks, the intruder inserts information of randomly spoofed identifiers, including inconsistent data. As an outcome, all network connections or nodes receive many operative messages and may go to the network's malfunction. To inject this kind of attack, the intruder recognizes vehicle messages and decides the targets.

To detect these attacks, a deep learning-based architecture is used, as demonstrated in Figure 3. The deep learning architecture detects attacks when received on the OBD port. Our deep learning system is based on the VGG-16 architecture, as shown in Figure 4. We first converted the message samples into a byteplot grayscale image,[12] utilized for the automatic classification of visual patterns. These images are variable resolution images with a

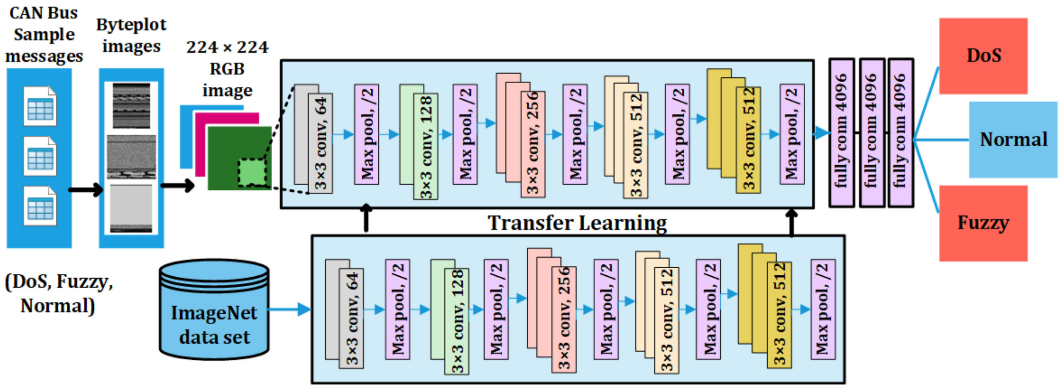

Figure 4. Deep learning-based intrusion detection system.

single channel, while the VGG-16 architecture accepts a fixed image with three channels input, i.e., red, green, blue (RGB). Thus, the grayscale images are converted into RGB with a fixed resolution of 224×224 pixels. The binary data are represented as grayscale images; every byte resembles one pixel color of the image interpreted as a grayscale. For black and white colors, 0 and 255 are used, whereas other values are utilized for intermediate colors of gray. These shades manifest visual patterns utilized to interpret binary data displayed as grayscale graphical depictions. It assists in identifying different data regions and, therefore, helps us to detect attacks or analytical tasks. Furthermore, as suggested by Krizhevsky *et al.*,[13] we subtracted the mean RGB measured on the ImageNet dataset. These RGB pixel values are utilized as input features. We trained the VGG-16 architecture[4] by transferring the pretrained the VGG-16 architecture's convolutional layers to the newly trained layers. The parameters of assigned convolutional layers are implemented to obtain the bottleneck features. Finally, the fully connected layers are used for the detection of different attack messages. To overcome the spatial dimension, the max-pooling layers are added at the end of convolutional layers. The features for input are given as

$$V_i^{(M)} = B_i^{(M)} + \sum_{k=1}^{n_1^{(M-1)}} \varphi_{i,k}^{M} \times h_k^{M-1}. \quad (1)$$

In the abovementioned equation, $V\vec{i}^{(M)}$ represents an output layer; the base value is represented with $Bi^{(M)}$, $\varphi_{i,k}^{M}$ indicates the filter mapping of the *k*th feature value, while h_k determines the $M-1$ output layer. We then applied the fully connected layers to classify different types of sample messages. Finally, the loss function is defined as a type of content loss[4] given as

$$L^{\phi_{i,j}}(\hat{y}, y) = \frac{1}{W_{i,j}, H_{i,j}} \sum_{x=1}^{W_{i,j}} \sum_{y=1}^{H_{i,j}} (\phi_i(y)_{x,y} - \phi_j(\hat{y})_{x,y})^2. \quad (2)$$

In the abovementioned equation, $\phi_{i,j}$ shows the feature map received after activation from the *j*th convolution and before the *i*th max-pooling layer. The loss function of the VGG architecture is the Euclidean distance between the feature maps of an output image $\phi_i(y)$ and the actual image $\phi_j(\hat{y})$. The corresponding dimensions of feature maps' are represented with $W_{i,j}$ and $H_{i,j}$.

EXPERIMENTAL RESULTS

This section elaborates on the experiments and performance evaluation of the abovementioned presented intrusion detection system. During this analysis, CAN-intrusion-dataset is used. We used three different kinds of CAN message samples, i.e., DoS, fuzzy, and attack free states (normal), from the dataset. The details of the dataset are provided in Table 1.

The dataset is randomly splitted at the ratio of 70% and 30% for training and testing. The system achieves good results, with an overall detection accuracy of 95% for DoS, fuzzy, and 96% for attack free state samples, as shown in Figure 5. The precision, recall, and F1-score of the system for different kinds of attacks and normal samples are also shown in Figure 5. The system's accuracy shows that the developed intrusion detection

Table 1. Dataset description.

S.No	Attack type	No. of messages
1	DoS attack	656,579
2	Fuzzy attack	591,990
3	Attack free state	2,369,868

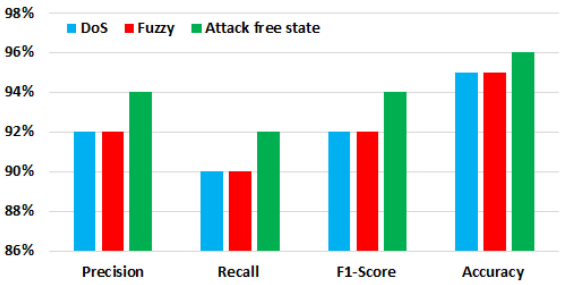

Figure 5. Evaluation results of the deep learning system.

system effectively identifies two different kinds of attacks in sample messages.

We also show the false positive rate (FPR) of the deep learning system in Table 2. It can be observed that the FPR of the deep learning system is 0.6%. The model results are also compared with other machine learning algorithms, as demonstrated in Table 2. It can be observed that the presented deep learning model achieves excellent results.

From the comparison results of Figure 6, it is observed that the presented deep learning system results are good as compared to other algorithms with a true positive rate (TPR) of 96%.

CONCLUSION AND FUTURE WORK

In this article, a deep learning-based intrusion detection system is presented for the IoV. The system's major goal is to provide a solution that affords STP to communicate entities and secure vehicle data from malicious attacks. The system utilized the VGG-16 architecture for the detection of different cyberattacks, i.e., DoS and fuzzy attacks in the CAN bus. For training and testing purposes, we used a CAN-intrusion-dataset, collected at the OBD port of the vehicles through different external communication links. The architecture is trained for the attack patterns to detect malicious attacks. The experiments reveal that the presented intrusion detection system significantly reduces FPR.

Table 2. Comparison results.

S. No.	Method	FPR	TPR
1	KNN	5%	93%
2	Random forest	5%	93%
3	Gradient boosting	4%	93%
4	AdaBoost	5%	94%
5	SVM	4%	95%
6	VGG-16	0.6%	96%

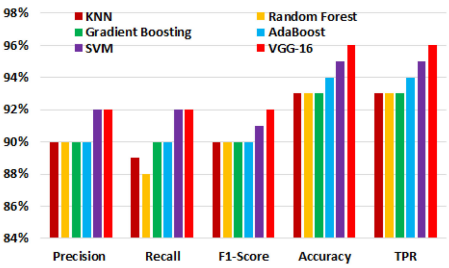

Figure 6. Results of the deep learning system with other algorithms.

The results are also compared with other conventional algorithms; among all, the deep learning system shows high-accuracy results. The overall accuracy is 96% with an FPR of 0.6%. In the future, this work might be extended for other deep learning architectures to enhance in-vehicle intrusion detection system performance and deliver high-quality solutions for its security.

REFERENCES

1. P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, K.-K. R. Choo, and Y. Park, "On the design of mutual authentication and key agreement protocol in Internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, Feb. 2021, doi: 10.1109/TVT.2021.3050614.
2. P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020, doi: 10.1109/ACCESS.2020.2981397.
3. A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, May 2020, doi: 10.1109/TVT.2020.2981934.

4. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.
5. H. Lee, S. H. Jeong, and H. K. Kim, "Otids: A novel intrusion detection system for in-vehicle network by using remote frame," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust*, 2017, pp. 57–5709, doi: 10.1109/PST.2017.00017.
6. D. Tian *et al.*, "An intrusion detection system based on machine learning for can-bus," in *Proc. Int. Conf. Ind. Netw. Intell. Syst.*, 2017, pp. 285–294, doi: 10.1007/978-3-319-74176-5_25.
7. M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, 2016, Art. no. e0155781, doi: 10.1371/journal.pone.0155781.
8. A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wireless Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018, doi: 10.4236/wet.2018.94007.
9. A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2287–2310, 2020, doi: 10.1007/s11277-019-06986-8.
10. H. Li, L. Zhao, M. Juliato, S. Ahmed, M. R. Sastry, and L. L. Yang, "Poster: Intrusion detection system for in-vehicle networks using sensor correlation and integration," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 2531–2533, doi: 10.1145/3133956.3138843.
11. J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, 2019, Art. no. 101974, doi: 10.1016/j.adhoc.2019.101974.
12. G. Conti, E. Dean, M. Sinda, and B. Sangster, "Visual reverse engineering of binary and data files," in *Int. Workshop on Visualization for Comput. Secur.* Berlin, Germany: Springer, 2008, pp. 1–17, doi: 10.1007/978-3-540-85933-8_1.
13. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017, doi: 10.1145/3065386.

Imran Ahmed is currently an associate professor with the Institute of Management Sciences, Hayatabad, Peshawar, Pakistan. He has several research interests such as deep learning, machine learning, data science, computer vision, feature extraction, digital image and signal processing, medical image processing, bio-metrics, pattern recognition, and data mining. He has attended several national and international conferences in these areas. Ahmed received the B.Sc. degree in computer science and mathematics from Edwardes College Peshawar, Peshawar, Pakistan, the M.Sc. degree in computer science from the University of Peshawar, Peshawar, the M.S.-IT degree in computer vision from the Institute of Management Sciences, Hayatabad, Peshawar, and the Ph.D. degree with a computer science major from the University of Southampton, Southampton, U.K. He has been a Reviewer in journals such as the *IEEE Transactions on Industrial Electronics, IEEE Access, Journal of Ambient Intelligence*, Elsevier, etc. Contact him at imran.ahmed@imsciences.edu.pk.

Gwanggil Jeon is currently a professor at Xidian University, Xi'an, China, and Incheon National University, Incheon, South Korea. From September 2009 to August 2011, he was a postdoctoral fellow with the School of Information Technology and Engineering, University of Ottawa, Ottawa, ON, Canada. From September 2011 to February 2012, he was an assistant professor with the Graduate School of Science and Technology, Niigata University, Niigata, Japan. From 2019 to 2020, he was a prestigious visiting professor with Dipartimento di Informatica, Università degli Studi di Milano Statale, Milan, Italy. Jeon received the B.S., M.S., and Ph.D. (*summa cum laude*) degrees from the Department of Electronics and Computer Engineering, Hanyang University, Seoul, South Korea, in 2003, 2005, and 2008, respectively. He was the recipient of the IEEE Chester Sall Award in 2007, the ETRI Journal Paper Award in 2008, and Industry-Academic Merit Award by Ministry of SMEs and Startups of Korea Minister in 2020. Contact him at gjeon@incheon.ac.kr.

Awais Ahmad is currently an assistant professor with the Department of Computer Science, Air University, Islamabad, Pakistan. Previously, he was a postdoctoral researcher at University degli Studi di Milano, Milan, Italy. Prior to his postdoctorate, he was an assistant professor with the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea. In 2014, he was also a visiting researcher at INTEL-NTU, National Taiwan University, Taipei, Taiwan, where he was working on Wukong Project (Smart Home). Ahmed received the Ph.D. degree in computer science and engineering from Kyungpook National University, Daegu, South Korea. Contact him at aahmad.marwat@gmail.com.