IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 14, 2020, accepted March 27, 2020, date of publication April 3, 2020, date of current version April 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985313

Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network

PRADIP KUMAR SHARMA[1], (Member, IEEE), JISUN PARK[1], JONG HYUK PARK[2], (Member, IEEE), AND KYUNGEUN CHO[1], (Member, IEEE)

[1]Department of Multimedia Engineering, Dongguk University, Seoul 04620, South Korea
[2]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, South Korea

Corresponding authors: Kyungeun Cho (cke@dongguk.edu) and Jong Hyuk Park (jhpark1@seoultech.ac.kr)

This research was supported by BK21 Plus project of the National Research Foundation of Korea Grant and was supported by the Dongguk University Research Fund of 2019 (S-2019-G0001-00043)

ABSTRACT Recently, wearable technologies have evolved in the most unexpected field like a military force outside of healthcare, fitness, lifestyle and similar areas. The growing need for soldiers' coordination, training and health, the increase in asymmetric warfare, suspected geopolitical conflicts and soldiers' modernization programs, among others, are some of the factors that fuel the growth of the military wearables market. Wearable computation plays an important role in improving the capabilities of the soldier. Further, the 5G network promises a solution to the many network and performance challenges in order to adopt more sophisticated wearable technologies in defense automation. In this paper, we conduct a study to identify the role of wearable computing for the defence automation system. We present the taxonomy of wearable computing in defence automation system and explain the relationship of each attribute. In addition, we identify the raise issues and challenges in communication and cybersecurity when deploying the 5G network in defense automation. Furthermore, we propose the design of the wearable smartwatch architecture as a use case of healthcare transformation in defense automation in the 5G environment.

INDEX TERMS Wearable computing, 5G network, security and privacy, edge computing.

I. INTRODUCTION

In recent years, the adoption of connected smart devices has gained momentum in military organizations. The Internet of Battlefield Things (IoBT) involves the full realization of ubiquitous sensing, communication, and computing. One of the characteristics of IoBT is the interconnection and collaborative decision-making between battlefield resources and combat equipment. In the recent MRFR analysis report, it is predicted that by 2024, the global military IoT market will be 17,720.6 million USD, recording a compound annual growth rate of 10.64% over the forecast period from 2019 to 2024 [1]. Specifically, wearable computing devices are driving military organizations towards defense automation. It helps soldiers, platoon commander and the command controller unit to better understand situational awareness on the battlefield at low cost and to reduce the risk of error. Wearable devices integrated with heterogeneous sensors in a soldier's clothing and body equipment provide the control unit with multidimensional real-time information on the battlefield. According to the end-user and the force group, wearable devices for the military have been classified into land forces, naval forces and airborne forces. To improve the combat capabilities of soldiers, many countries around the world have increased the use of wearable computing devices [2], [3].

On the other hand, edge computing overcomes the limitations of the centralized legacy network architecture. By placing computing and storage resources at the edge of the network, data collection and processing takes place at or near the source or device of the application [4]–[7]. For military organizations, edge computing enables connectivity to wearable computing devices on the battlefield and makes a soldier's life better, safer and increases the accuracy of decision-making. In addition to all this, the scalability, versatility, and reliability of edge computing also make it an attractive proposition for defense automation around the world. Meanwhile, the 5th generation of cellular network technology (5G) is expected to have bandwidth 10 times

The associate editor coordinating the review of this manuscript and approving it for publication was Shiwen Mao.

higher than the current legacy network. 5G is designed not only to improve network performance but above all to link digital systems that need huge amounts of data to function automatically. The most important 5G applications will not be intended for civilian use, but for the military. The 5G military upgrade would also allow drones to independently perform coordinated missions or tasks by increasing the speed of data transfer between operators and combat vehicles. However, even with 5G, sending data over long distances will involve network latency unless the devices connected to 5G have higher computing power. Particularly, the wearable computing devices in the 5G network open up a new paradigm with opportunities and challenges for the realization of defense automation [8]–[10].

This study takes into account the opportunities and challenges of the 5G network in the context of wearable computing towards defense automation. The scientific contributions of this research work are summarized as follows:

- We present the taxonomy of wearable computing in the defense automation system. We discuss each of the attributes of the proposed taxonomy and explain the relationship of wearable computing in defense automation.
- We identify research issues and challenges of wearable computing in the 5G network environment. We present the concerns raised in communication and cybersecurity when deploying the 5G network in defense automation.
- In addition, we also propose the design of the wearable smartwatch architecture as a use case of healthcare transformation in defense automation. The proposed design of a wearable smartwatch using PPG Photoplethysmography) sensor, Inertial sensor, and Physical Unclonable Function (PUF) in the 5G network.

The rest of the paper is structured as follows: Section II discusses the taxonomy of the wearable computing in defence automation system; the issues and challenges of wearable computing in the 5G network environment are discussed in Section III; Section IV the prototype for designing the wearable smartwatch in 5G network; the conclusion of this research is presented in Section V.

II. TAXONOMY OF WEARABLE COMPUTING IN DEFENCE AUTOMATION

Recently, wearable devices have played an important role in improving the capabilities of the soldier. For defence automation, responding properly to the needs of the soldier is crucial and accepted by all military personnel. In this section, we discuss the taxonomy of wearable computing in defense automation and explain the main attributes.

Wearable technologies have been rapidly adopted in the military sector recently, as they help monitor the physical condition of soldiers during missions, improve communication between troops and military posts, and provide a comprehensive knowledge of the situation. Wearable technologies allow a command control unit to track soldiers more accurately, which will make it easier to monitor soldiers' safety during high alert operations and reduce the risk of errors.

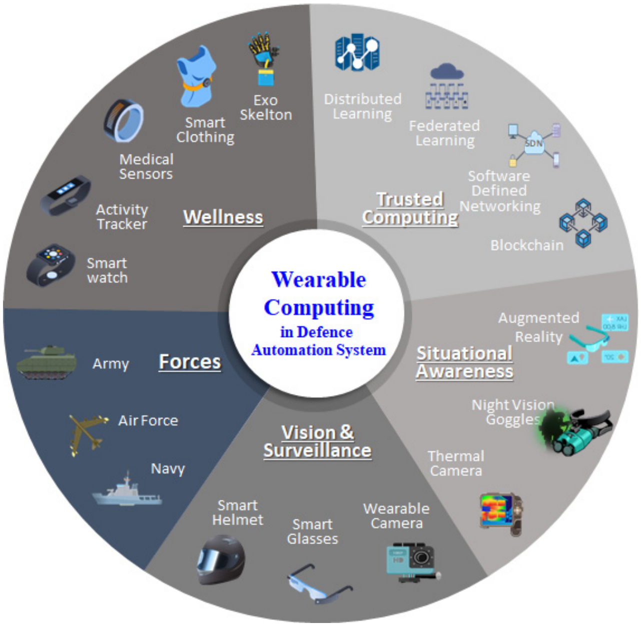


FIGURE 1. Illustrate the taxonomy of wearable computing in defence automation.

Fig. 1 illustrate the taxonomy of wearable computing in defence automation. We have classified the taxonomy of wearable computing for defence automation into five attributes: forces, wellness, trusted computing, situational awareness and vision & surveillance. We discuss each of the attributes of taxonomy and explain the relationship of wearable computing in the defense automation system as follow:

A. FORCES

Military forces are broadly divided into mainly three groups: army, air force, and navy. In each of these military forces groups, wearable computing-based solutions play an important role in defence automation. In the case of the army, it is possible to identify the enemy through smart glasses that can identify the enemy better than the general field of view when confronting the enemy and the mountainous area. It shares the field of view information acquired through each individual device to successfully accomplish the global mission. For air force, wearable technology makes possible to automatically detect emergency situations during missions such as supersonic flight lights through smart clothes that continuously monitor the pilot's biometric information. In the case of Navy force, Augmented Reality (AR) /Virtual Reality (VR) technology can reduce the cost of training in the real ocean for maritime missions in a virtual marine environment.

B. WELLNESS

Wellness is one of the important parts of a soldier's healthcare to sustain healthy body condition and improve the individual's overall military skills. Wearable devices for wellness are smartwatch, activity tracker, medical sensors, smart clothing,

TABLE 1. **The device of wearable sensors for wellness in military.**

Device type	Device name, Company	features
Smartwatch	MARQ COMMANDER, GARMIN	GPS, thermometer, accelerometer, gyroscope, compass, barometric altimeter and heart rate monitor, etc.
	Traverse Alpha Foliage, SUUNTO	GPS, GLONASS, compass, night vision, Route Preview, step counter, and temperature, etc.
	Pro Trek, Casio	Optical sensor (heart rate), compass (magnetic) sensor, pressure (air pressure, altitude) sensor, accelerometer, and gyrometer, etc.
Smart clothing	DOMINATOR warrior combat suite, Elbit Systems	SmartEye (geo-oriented head-mounted C2 display), Smart WristView (convenient view of operational data in combat situations), SmartSight (day and night weapon sights, projecting see-through AR symbology) and SmartNVG (AR navigation)
Exo skeleton	Onyx Exoskeleton, Lockheed Martin	External skeleton to increase mobility and reduce fatigue of its users

and exo skeleton and so on. Smartwatch has sensors to monitor individual soldier's conditions continuously such as GPS, thermometer, accelerometer, gyroscope, compass, barometric altimeter, and heart rate monitor [11], [12]. An activity tracker can provide a log of behaviors of soldiers such as a passed path or a training record. Medical sensors constantly monitor the soldier's current health and detect risks by monitoring biodata such as temperature and heart rate. Smart clothing includes thin flex batteries and sensors which read body movements to understand current events in the surrounding in the war [13]. Exo skeleton is a wearable device of an external selection that supports and protects the human body [14]. Table 1 presents the products of the wearable device for wellness in the military.

C. TRUSTED COMPUTING

In recent times, wearable computing combines Internet of Things (IoT) and Artificial intelligence (AI) technologies to integrate all information, not just individual information, to better understand global situations to decide better military decisions [15]. As the importance of data sharing increases, information security's also increases because their military information should not be exposed to the enemy. Therefore, trusted computing is the key element of wearable computing in the defence automation system. Trust computing includes distributed learning, federated learning, Software Defined Network (SDN) and blockchain.

By sharing the model among multiple computing nodes in distributed learning, it facilitates the improvement of efficiency and performance [16]–[18]. But, due to the heterogeneous nature of the dataset at the edge network in the battlefield, federated learning complements the bottleneck of distributed learning [19]. On the other hand, the functionality of SDN technology makes the defense network more dynamic, programmable, cost-effective, manageable, and highly adaptive by decoupling the control and data planes [20], [21]. In addition, the blockchain technology features such as distributed, incorruptible, shared, and secure without the need of trusted third party makes the military organization one step forward towards defence automation [22], [23].

D. SITUATIONAL AWARENESS

Situational awareness can be increased through soldiers' visual interface technology using a thermal camera, night vision goggles and AR technology, etc. A thermal camera can detect and track the enemy's movement more easily and the night vision goggle also increases the situational awareness skill at night. Furthermore, AR technology is used for rapid target acquisition by providing graphical expected situation [24]. A combination of these technologies allows soldiers to better understand their surroundings and decide what to do next rapidly.

E. VISION & SURVEILLANCE

Using smart helmets, smart glasses and wearable cameras, soldiers' vision & surveillance skills can be increased. The smart helmet includes bone earphones to transmit sound when a solider receives and speaks order, rather than traditional microphones and earphones [25]. Smart glasses provide an extended view of sight and information using AR. The wearable camera can gather visual information of the enemy or friends easily. Based on these wearable sensors, soldiers can communicate individual situation information in real-time, then cooperate to complete their mission [26]. Table 2 shows wearable devices of vision & surveillance.

III. WEARABLE COMPUTING IN 5G ENVIRONMENT

In the era of Industry 4.0, the 5G network promises a solution to the many network and performance challenges in order to adopt more sophisticated wearable technologies in defense automation. The proper deployment of the 5G network will unlock the possibility of using wearable computing technologies in defense automation and can reach a more granular

TABLE 2. Wearable devices of vision & surveillance in military.

Device type	Device name, Company	features
Smart helmet	Q Warrior, Google & BAE systems	A wearable computer using the Google glass with a helmet-mounted display technology similar to, 3D HUD, that gives a soldier a picture of the entire battlefield
Smart glass	HoloLens 2, Microsoft	An Integrated Visual Augmentation System (IVAS), that offers the capabilities they need to regain and maintain overmatch in multi-domain operations on battlefields.

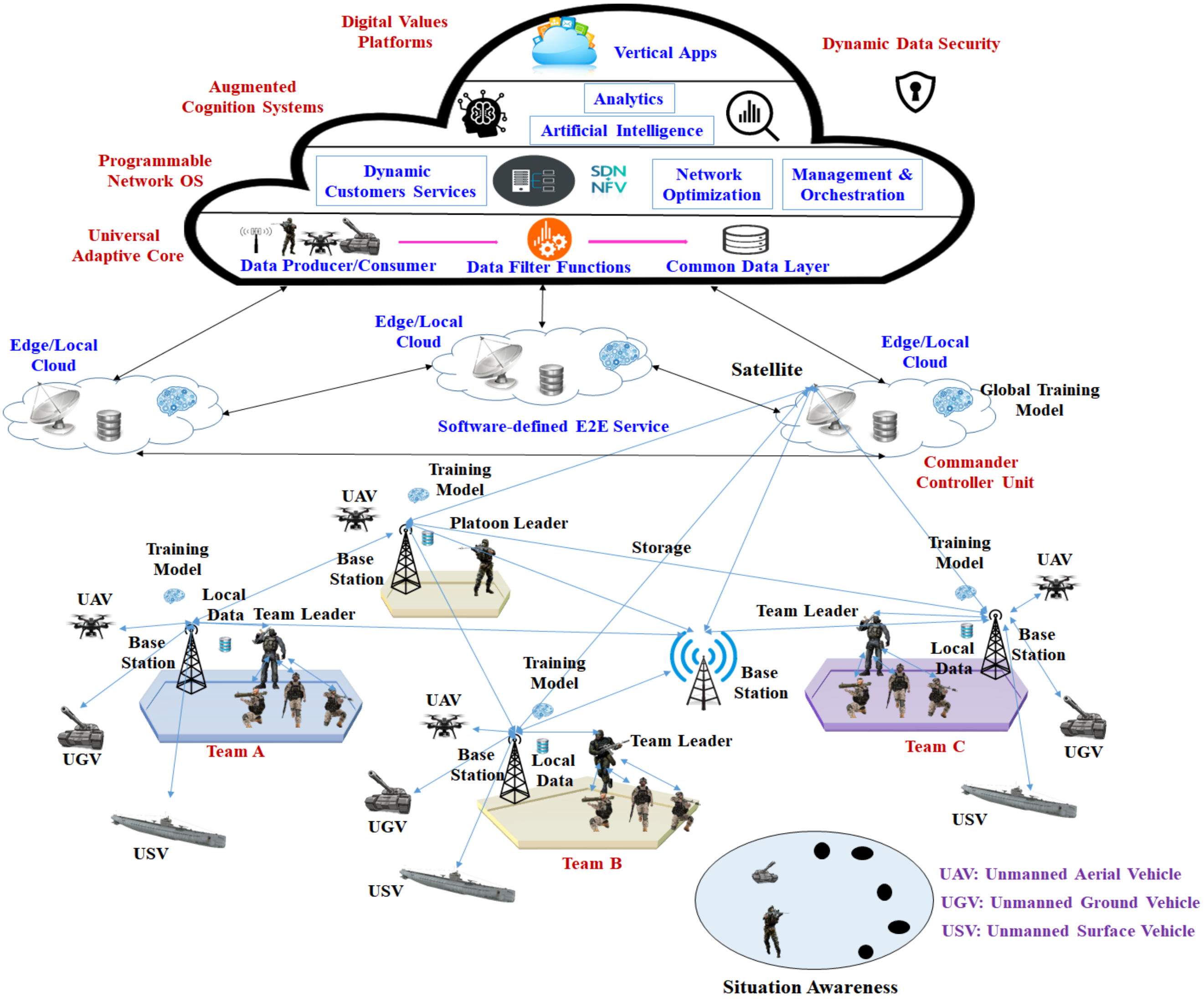


FIGURE 2. Abstract overview of wearable computing 5G network architecture in defence automation.

level on the battlefield. However, the deployment of the 5G network is still in its infancy and is not mature enough for defense automation. In this section, we discuss the problem and challenges of wearable computing in defense automation in the context of the 5G network.

Fig. 2 presents the abstract overview of wearable computing 5G network architecture in defence automation. A 5G network is equipped to provide greater bandwidth capacity, increased throughput, improved reliability, while dramatically reducing latency. In the defence automation, the deployment of the 5G network supports the mobile edge connectivity and the requirements of the Internet of Battle Things (IoBT) such as on-device/edge model training for making a critical decision on the battlefield, flexibility, and availability. Specifically, wearable computing in defence automation classified according to their level of complexity and functional/non-functional requirements. Here we discuss the concerns raised in communication and cybersecurity while deploying the 5G network in defense automation.

A. COMMUNICATION

In defence automation, the main motive is to transmit the soldier activity and situational awareness from the battlefield to make an appropriate decision. Wearable IoBT devices that enable the fleet military to make on the fly communications with soldiers at battle zones and have the potential to dramatically impact the future of the defence industry. Army safety is a top concern in the defence industry, and wearables can play a key role by enhancing communication between commander, platoon, and soldiers. However, in the 5G network, the realization of wearable computing in defence automation raises certain concerns:

1) ENERGY CONSUMPTION

Designing the small size of most wearable devices without degrading the user experience poses a challenge in defense automation. Specifically, in the combat zone, a smart device with a small form factor generally limits the capacity of the battery and requires frequent battery replacements and charging is very difficult. Harvesting energy from ambient sources is an interesting way to alleviate the problem of power constraints. However, in the 5G network, the design of network architecture as optimal as possible in terms of energy consumption to achieve sustainable wearable computing in the defense industry. The power levels and position of massive multiple inputs and multiple output base stations must be optimized to provide maximum user coverage on the battlefield and low power consumption of wearable devices [27]–[29].

2) LICENSED/UNLICENSED WEARABLE COMMUNICATIONS

Generally, the unlicensed technologies used in today's wearable devices that allow direct close proximity communications among multiple devices with less complexity and lower cost. However, most countries prefer to opt for the exclusive use of the spectrum in the defense industry. In the 5G network, the wearable device can communicate directly with base stations/edge nodes in a licensed communication that supports the quality of service and mobility. Licensed communication is generally expensive and complex. In addition, licensed communications can consume more power, which limits the implementation of wearable computing for defense automation in the 5G network [30], [31].

B. CYBERSECURITY

In the cyber world, robust cybersecurity is essential for protecting the information systems of military organizations and the armed forces. It plays a crucial role in national security and provides protection to communication and information systems to enable wearable computing in defense automation. The 5G network offers a larger cyber-attack surface and more devices accessing the network. Defense departments and military organizations should accelerate security strategies to stay protected while deploying wearable computing in defense automation. In this subsection, we discuss the cybersecurity issues and challenges related to the 5G network that we need to address while building a sustainable wearable computing network in defence automation [32]–[36].

1) CHOKEPOINT INSPECTION AND CONTROL

In the 5G network, the network moves away from the centralized hardware-based switching network to a distributed digital routing network defined by software. Compared to the legacy network, the 5G network has pushed network activity outward towards a network of digital routers across the network, which raises the concern of denying the potential for chokepoint inspection and control. In particular, in defense automation, due to resource constraints on wearable devices, cyber hygiene should be practiced on the network. The lack of chokepoint inspection and control raises the concern of the adoption of wearable computing in the 5G network for defence automation. Fig. 3 presents the example of denying the potential for chokepoint inspection and control.

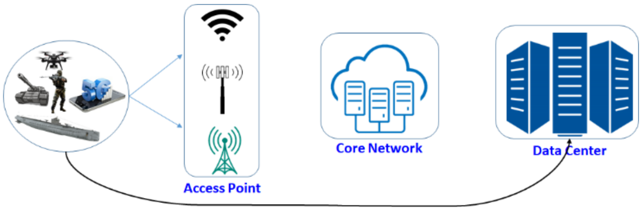


FIGURE 3. Example of denying chokepoint inspection and control.

2) SOFTWARE-DEFINED NETWORK CONTROL

Software virtualization performs high-level network functions in the 5G network, which further complicates its cyber vulnerability. Software vulnerabilities can be easily fixed within the network, but what if the software-defined network controller is compromised. In military organizations, if the attacker takes control of the software that manages the networks, it will be easier for cyber-adversaries to manipulate portable devices to carry out activities aimed at causing damage on the battlefield. Cybersecurity solutions will, therefore, have to be developed to counter them.

3) DYNAMIC CYBER PROTECTION

In defence automation, resource-constrained wearable devices will become new targets for cyber attackers due to the dramatic expansion of bandwidth in the 5G network. While we can configure the network using a dynamic spectrum sharing capability called ''network slices'' based on the category of wearable devices on the battlefield, each network slice will have its own varying degree of cyber risk. Other than relying on a uniform solution with the lowest common denominator, we must provide dynamic cyber protection for

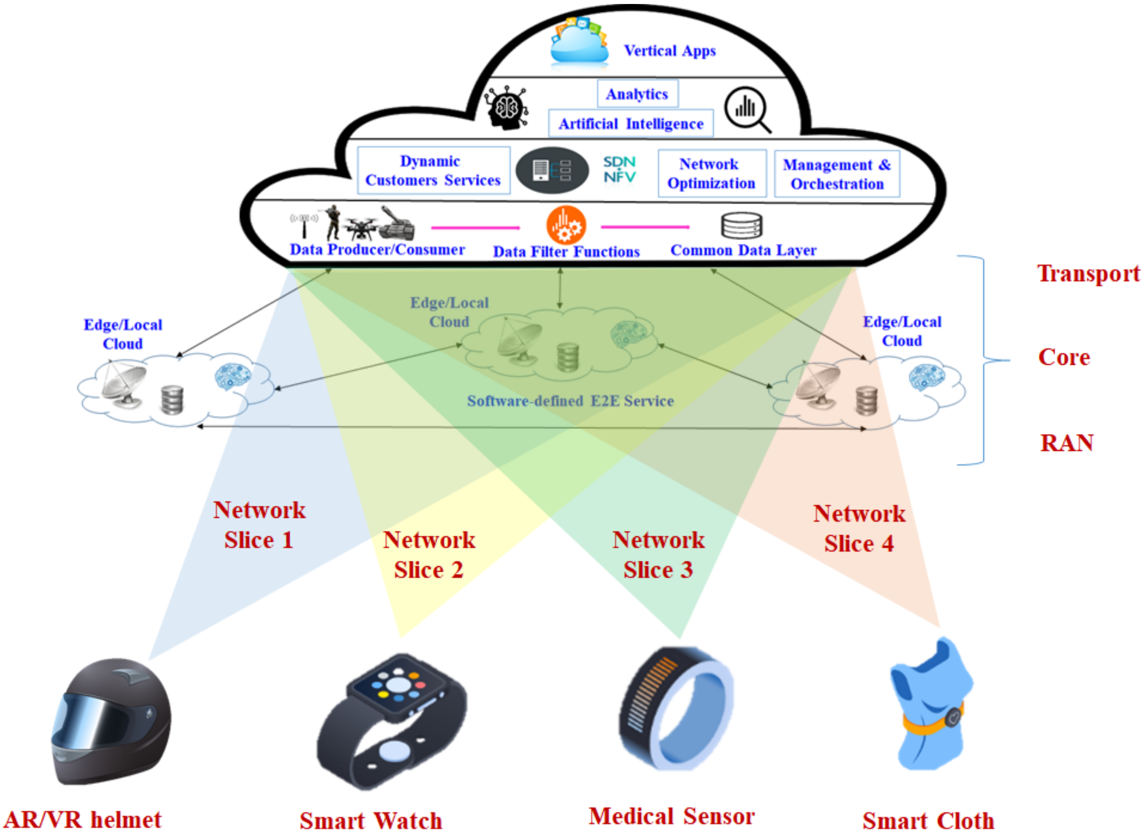


FIGURE 4. Example of dynamic cyber protection.

wearable devices according to their degree of cyber risk. Fig. 4 illustrate the example of dynamic cyber protection.

4) INCREASED BANDWIDTH

The increase in bandwidth in the 5G network will raise another capability concern for wearable computing devices in defence automation. Due to the limited computing power and other resource constraints on wearable devices, security solutions need to be upgraded to deal with these new capabilities with lighter and efficient algorithms. Most of the security solutions for real-time wearable computing devices in defence automation may no longer work in the 5G network.

5) HETEROGENEOUS ACCESS

For military smart devices, wearable sensors are one of the most common smart sensing modules under strict resource constraints that have information resilience, collecting information on the battlefield. In security design consideration, heterogeneous access will be one of the main key characteristics. In the combat zone, multi-network environments are more likely to access the network architecture from different networks are different. Wearable devices will have many choices in how they access networks from the battlefield. In the 5G network, network access policies and security management of wearable devices must be efficient, secure and light enough to meet resource constraints and can build trust relationships between devices and networks. Fig. 5 illustrates the example of heterogeneous access.

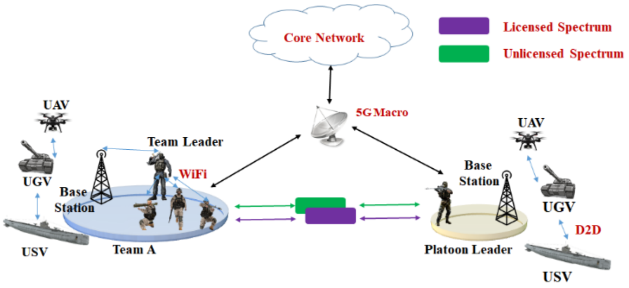


FIGURE 5. Example of heterogeneous access.

6) PRIVACY PROTECTION

In the 5G network, we can configure the multiplexing of independent virtualized logical networks on the same physical network infrastructure using network slicing. In military organizations, the network can be configured based on the category of wearable computing devices on the battlefield. However, to offer differentiated quality of service, networks may need to sense the type of service. This raises serious

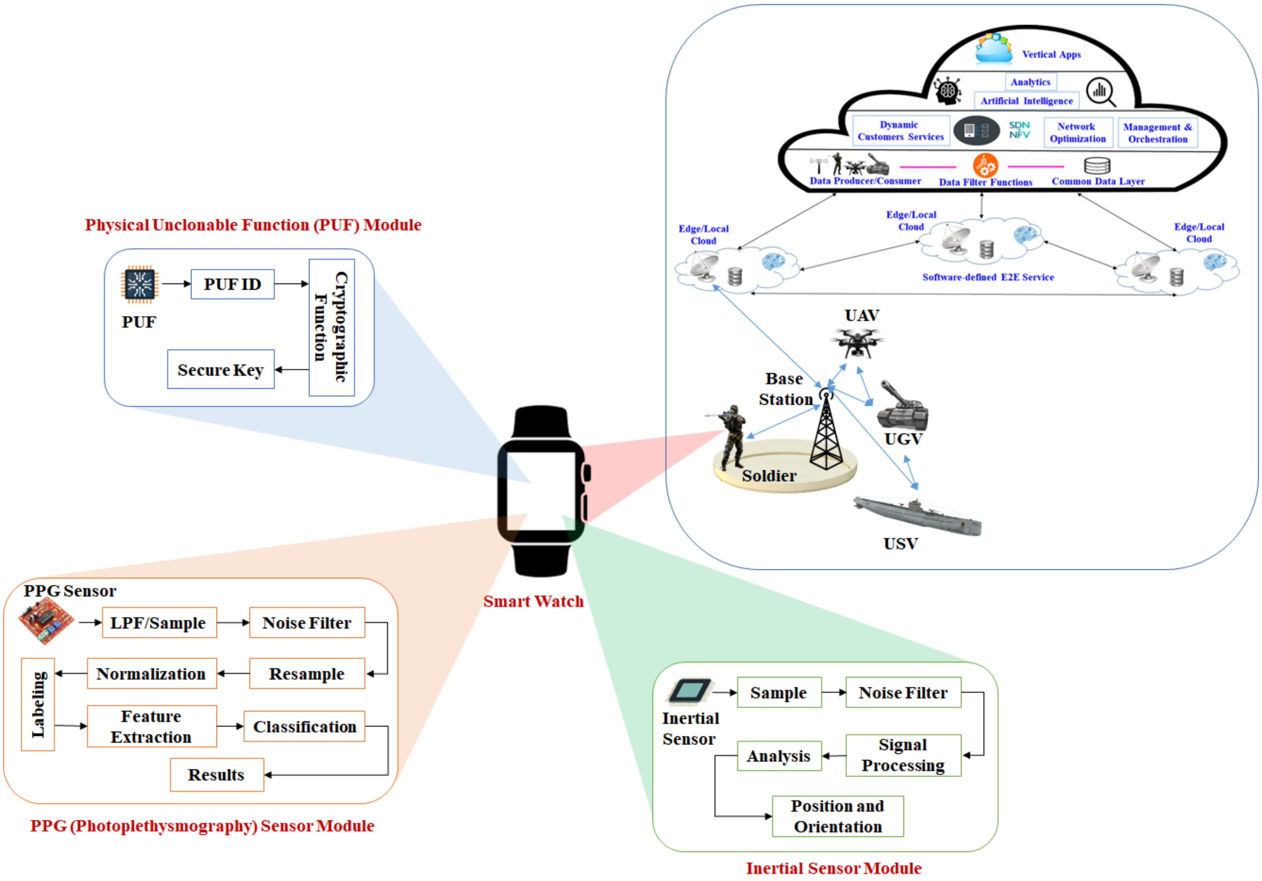


FIGURE 6. Abstract design overview of wearable smartwatch.

concerns about breaches of privacy and has serious consequences in defense automation.

IV. USE CASE OF HEC HEALTHCARE TRANSFORMATION IN DEFENCE AUTOMATION

Human-driven Edge Computing (HEC) is a crucial part of the 5G network for defense automation. It offers a first-rate advantage to communications service providers by seizing new opportunities and challenges for the realization of wearable computing in defense automation. Real-time analytics, high-speed connectivity, and low latency combine to create a sustainable computing system for military organizations in various real-world scenarios. With the 5G network, this is a large set of transformations that we must take into account at the edge in the context of wearable computing adaptation in defense automation. For instance, ultra-low latency techniques, lightweight and secure authentication schemes, data collection and analysis leveraging advanced analysis in defense automation. In this section, we present the design of the wearable smartwatch architecture as a use case of healthcare transformation in defense automation.

In the era of the digital world, national security depends on the strength of military organizations and the safety of soldiers is seen as a vital role. An appropriate tracking system of a soldier's health and position allows to track the soldier's current GPS position and also checks health status such as a soldier's body temperature, heart rate, etc. In the context of the 5G network, the need to design such a system to obtain information on the health status of soldiers and provide them with instant help is crucial for defense automation. In an emergency, due to the lack of medical assistance, soldiers who are the backbone of any armed force usually lose their lives. In addition, in battle zones, soldiers lose contact with the authorities. To address these concerns, we propose a design of a wearable smartwatch using PPG (Photoplethysmography) sensor, Inertial sensor, and Physical Unclonable Function (PUF) in a 5G network, as illustrated in Fig. 6. The design of the wearable smartwatch is consists of three modules: PPG sensor module, Inertial sensor module, and PUF module.

A. PPG SENSOR MODULE

The PPG sensor is designed to measure changes in blood volume. It is a commonly used optical detection method that collects light reflected or transmitted through the skin in order to non-invasively monitor the pulsation of blood flow in subcutaneous blood vessels. The atypical

PPG sensor emits light at the tissue site with one or more LEDs. The measuring photodiode measures the intensity of the non-absorbed light reflected by the tissue. Recently, as an alternative technique for monitoring heart rate, the adaptation of PPG technology has increased [37]–[41]. Specifically, in wearable devices, the PPG sensor is quickly adopted due to the cost-effectiveness and simplicity of its operation. The ability of PPG to measure blood variations in different parts of the body and its potential ability to detect physiological parameters related to the cardiovascular and respiratory systems continued to motivate the scientific community to develop wearable devices based on portable PPG which are more inexpensive and very accurate for monitoring daily routine activities. In recent years, the penetration rate of PPG sensor technology in wearable devices has reached 98% and is expected to reach 100% by 2020 and global net profit is expected to reach the US $ 52.5 billion by 2024 [42], [43]. As illustrated in Fig. 6, the PPG sensor module prototype consists of eight different stages: Low-pass filter (LPF)/Sample, Noise Filter, Resample, Normalization, Labeling, Feature Extraction, Classification, and Results. Initially, the prototype module will collect samples from the PPG sensor. To improve the robustness of detection accuracy and signal quality assessments, the module includes LPF/sample, noise filter, resampling and normalization steps. In the next step, the module will label the collected data and use a lightweight deep learning model for feature extraction and data classification. In the last step, the module will send the classified result data to the local edge node/base station to process further and take the necessary actions from the command control unit at the battlefield.

B. INERTIAL SENSOR MODULE

Inertial sensors are sensors based on inertia and relevant measurement principles which can be applied in various contexts due to the universal presence of movement, vibration, and shock. It is essentially an autonomous system that measures linear and angular movements generally with a triad of gyroscopes and accelerometers. Nowadays, inertial sensors containing many smart devices such as smartphones, Virtual Reality (VR) headsets are known as Inertial Measurement Units (IMUs) [44]–[47]. An accelerometer measures the external specific force acting on the sensor while the gyroscope measures the rate of change in the orientation of the sensor. In defense automation, the use of an inertial sensor in a wearable device such as a smartwatch can be very useful in tracking the position and orientation of the soldier on the battlefield. As illustrated in Fig. 6, the inertial sensor module of the proposed prototype consists of the sample, noise filter, signal processing, analysis, and position and orientation. In the context of the 5G network, for defence automation, the proposed smartwatch prototype with inertial sensor module will be very effective due to its characteristics such as portability, low cost, low energy consumption and high precision.

C. PUF MODULE

In defense automation, due to the resource constraints of wearable devices, secure communications in 5G environments are important and curial part to be taken into account by military organizations. As we discussed in the previous section, with increased bandwidth and low latency, 5G networks are opening up a new paradigm of secure authentication that must be in place while realizing the wearable computing in the automation of defense. Compared to software components where there is only logical existence for the secret key, the secret key in wearable devices must include ROM memory which is vulnerable to cyber-physical attacks. Recently, a symmetric key scheme supported by the hardware, such as PUF has been reported to improve efficiency and provide protection against cyber-physical attacks [48]–[51]. PUF is a digital fingerprint that protects security chips from invasive attacks by generating a unique identifier that cannot be reverse-engineered. It acts as a unidirectional function, of which each different instance provides unique outputs for the same separate input. As shown in Fig. 6, the proposed wearable smartwatch prototype with PUF ID will be used as a unique secret key to supporting cryptographic algorithms to provide secure and tamper-proof communication in the 5G network in defense automation.

V. CONCLUSION

Military operations today have become complex, multifaceted and unpredictable. As the technological capabilities of allies and adversaries advance, military commanders must exert more pressure to anticipate, assess and act in environments that are increasingly stressed and time-limited. Several countries have started to focus on the potential military benefits of wearable computing devices. Defense automation enables today's military agencies to make decisions based on real-time analysis generated by integrating information from a wide range of wearable devices on the battlefield.

This study led to a comprehensive analysis of the role of wearable computing for defense automation in the 5G network environment. We have identified the issues and challenges raised during the deployment of wearable computing devices in the 5G network. We proposed a prototype design of the smartwatch using PPG, inertial sensors to monitor the soldier's activities and state of health. The proposed design also included PUF ID to ensure secure and efficient communication in the 5G network.

Advanced 5G introduces a slew of cybersecurity concerns in wearable computing for defence automation and seen as obstacles in the system design. Organizations and decision-makers should be held accountable for a new cyber due diligence and establish a new cyber regulatory paradigm to reflect the new realities. Ignoring the problems and challenges at the beginning raised by the 5G network in wearable computing for defense automation is not cost-efficient in the long run. Adding functionality later is less efficient and often more costly than including appropriate mechanisms from the beginning. In future work, we will perform the experimental analysis of the design of the proposed prototype to assess the feasibility of the proof of concept

REFERENCES

[1] *Military IoT Market Research Report-Global Forecast Till 2024*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.marketresearchfuture.com/reports/military-iot-market-7546

[2] *Internet of Military Things: Leading Technology Trends Revealed*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.army-technology.com/comment/internet-of-military-things-leading-technology-trends-revealed/

[3] *Global Military Wearables Market Report 2019: Market is Projected to Grow From USD 4.2 Billion in 2019 to USD 6.4 Billion by 2025*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.prnewswire.com/news-releases/global-military-wearables-market-report-2019-market-is-projected-to-grow-from-usd-4-2-billion-in-2019-to-usd-6-4-billion-by-2025–300854336.html

[4] A. Castiglione, K.-K.-R. Choo, M. Nappi, and S. Ricciardi, ‘‘Context aware ubiquitous biometrics in edge of military things,’’ *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 16–20, Nov. 2017.

[5] J. Choi and S. Ahn, ‘‘Scalable service placement in the fog computing environment for the IoT-based smart city,’’ *J. Inf. Process. Syst.*, vol. 15, no. 2, pp. 440–448, 2020.

[6] W. Li, Z. Chen, X. Gao, W. Liu, and J. Wang, ‘‘Multimodel framework for indoor localization under mobile edge computing environment,’’ *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4844–4853, Jun. 2019.

[7] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, and H.-J. Kim, ‘‘An intelligent data gathering schema with data fusion supported for mobile sink in wireless sensor networks,’’ *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 3, Mar. 2019, Art. no. 155014771983958.

[8] *How 5G Could Impact the Military*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.mwrf.com/markets/defense/article/21849618/how-5g-could-impact-the-military

[9] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, ‘‘A survey on 5G usage scenarios and traffic models,’’ *IEEE Commun. Surveys Tuts.*, early access, Feb. 6, 2020, doi: 10.1109/COMST.2020.2971781.

[10] Q. Tang, L. Chang, K. Yang, K. Wang, J. Wang, and P. K. Sharma, ‘‘Task number maximization offloading strategy seamlessly adapted to UAV scenario,’’ *Comput. Commun.*, vol. 151, pp. 19–30, Feb. 2020.

[11] P. S. Sandra, C. M. Sandeep, V. Nair, M. V. Vindhuja, S. S. Nair, and M. P. Raja, ‘‘WSN based industrial parameter monitoring using smartwatch,’’ in *Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT)*, Apr. 2017, pp. 1–6.

[12] S. Li, X. Kang, L. Fang, J. Hu, and H. Yin, ‘‘Pixel-level image fusion: A survey of the state of the art,’’ *Inf. Fusion*, vol. 33, pp. 100–112, Jan. 2017.

[13] S. Scataglini, G. Andreoni, and J. Gallant, ‘‘Smart clothing design issues in military applications,’’ in *Proc. Int. Conf. Appl. Hum. Factors Ergonom.* Cham, Switzerland: Springer, 2018, pp. 158–168.

[14] A. Agrawal, A. N. Dube, D. Kansara, S. Shah, and S. Sheth, ‘‘Exoskeleton: The friend of mankind in context of rehabilitation and enhancement,’’ *Indian J. Sci. Technol.*, vol. 9, no. S1, pp. 1–8, 2016.

[15] V. G. Motti, ‘‘Introduction to wearable computers,’’ in *Wearable Interaction*. Cham, Switzerland: Springer, 2020, pp. 1–39.

[16] G. Cicceri, F. De Vita, D. Bruneo, G. Merlino, and A. Puliafito, ‘‘A deep learning approach for pressure ulcer prevention using wearable computing,’’ *Hum.-Centric Comput. Inf. Sci.*, vol. 10, no. 1, p. 5, Dec. 2020.

[17] C. Yin, B. Zhou, Z. Yin, and J. Wang, ‘‘Local privacy protection classification based on human-centric computing,’’ *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, p. 33, Dec. 2019.

[18] W. Li, H. Xu, H. Li, Y. Yang, P. K. Sharma, J. Wang, and S. Singh, ‘‘Complexity and algorithms for superposed data uploading problem in networks with smart devices,’’ *IEEE Internet Things J.*, early access, Oct. 24, 2019, doi: 10.1109/JIOT.2019.2949352.

[19] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, ‘‘Federated learning in mobile edge networks: A comprehensive survey,’’ 2019, *arXiv:1909.11875*. [Online]. Available: http://arxiv.org/abs/1909.11875

[20] N. Ha and N. Kim, ‘‘Efficient flow table management scheme in SDN-based cloud computing networks,’’ *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 1–11, 2018.

[21] B. Xiong, K. Yang, J. Zhao, W. Li, and K. Li, ‘‘Performance evaluation of OpenFlow-based software-defined networks based on queueing model,’’ *Comput. Netw.*, vol. 102, pp. 172–185, Jun. 2016.

[22] Y. Ren, F. Zhu, P. K. Sharma, T. Wang, J. Wang, O. Alfarraj, and A. Tolba, ‘‘Data query mechanism based on hash computing power of blockchain in Internet of Things,’’ *Sensors*, vol. 20, no. 1, p. 207, 2020.

[23] R. D. S. Kulshrestha and I. Navy, ‘‘Military applications of blockchain technology,’’ in *The Age of Blockchain: A Collection of Articles*, vol. 21. New York, NY, USA: IndraStra Global, 2018.

[24] W. Parker, J. Parker, and E. M. Gallo, ‘‘Holographic imageguide display for situational awareness,’’ *Proc. SPIE*, vol. 10197, May 2017, Art. no. 101970U.

[25] W. Von Rosenberg, T. Chanwimalueang, V. Goverdovsky, D. Looney, D. Sharp, and D. P. Mandic, ‘‘Smart helmet: Wearable multichannel ECG and EEG,’’ *IEEE J. Transl. Eng. Health Med.*, vol. 4, pp. 1–11, 2016.

[26] H. Shi, H. Zhao, Y. Liu, W. Gao, and S.-C. Dou, ‘‘Systematic analysis of a military wearable device based on a multi-level fusion framework: Research directions,’’ *Sensors*, vol. 19, no. 12, p. 2651, 2019.

[27] H. Sun, Z. Zhang, R. Q. Hu, and Y. Qian, ‘‘Challenges and enabling technologies in 5G wearable communications,’’ 2017, *arXiv:1708.05410v1*. [Online]. Available: https://arxiv.org/abs/1708.05410v1

[28] J. Park, G. Bhat, A. Nk, C. S. Geyik, U. Y. Ogras, and H. G. Lee, ‘‘Energy per operation optimization for energy-harvesting wearable IoT devices,’’ *Sensors*, vol. 20, no. 3, p. 764, 2020.

[29] M. Matalatala, M. Deruyck, S. Shikhantsov, E. Tanghe, D. Plets, S. Goudos, K. E. Psannis, L. Martens, and W. Joseph, ‘‘Multi-objective optimization of massive MIMO 5G wireless networks towards power consumption, uplink and downlink exposure,’’ *Appl. Sci.*, vol. 9, no. 22, p. 4974, 2019.

[30] J. Wang, W. Wu, Z. Liao, A. K. Sangaiah, and R. S. Sherratt, ‘‘An energy-efficient off-loading scheme for low latency in collaborative edge computing,’’ *IEEE Access*, vol. 7, pp. 149182–149190, 2019.

[31] Y. Mehmood, N. Haider, M. Imran, A. Timm-Giel, and M. Guizani, ‘‘M2M communications in 5G: State-of-the-art architecture, recent advances, and research challenges,’’ *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 194–201, 2017.

[32] *Why 5G Requires New Approaches to Cybersecurity*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

[33] *5G Security: Forward Thinking*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf

[34] *A Guide to 5G Network Security*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.ericsson.com/en/security/a-guide-to-5g-network-security

[35] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, ‘‘Secure D2D communication for 5G IoT network based on lightweight cryptography,’’ *Appl. Sci.*, vol. 10, no. 1, p. 217, 2020.

[36] P. K. Sharma, J. H. Ryu, K. Y. Park, J. H. Park, and J. H. Park, ‘‘Li-Fi based on security cloud framework for future IT environment,’’ *Human-centric Comput. Inf. Sci.*, vol. 8, no. 1, p. 23, Dec. 2018.

[37] C.-C. Chang, C.-T. Wu, B. I. Choi, and T.-J. Fang, ‘‘MW-PPG sensor: An on-chip spectrometer approach,’’ *Sensors*, vol. 19, no. 17, p. 3698, 2019.

[38] M. Ghamari, ‘‘A review on wearable photoplethysmography sensors and their potential future applications in health care,’’ *Int. J. Biosensors Bioelectron.*, vol. 4, no. 4, p. 195, 2018.

[39] F. Riaz, M. A. Azad, J. Arshad, M. Imran, A. Hassan, and S. Rehman, ‘‘Pervasive blood pressure monitoring using photoplethysmogram (PPG) sensor,’’ *Future Gener. Comput. Syst.*, vol. 98, pp. 120–130, Sep. 2019.

[40] D. U. Uguz, B. Venema, S. Leonhardt, and D. Teichmann, ‘‘Multifunctional photoplethysmography sensor design for respiratory and cardiovascular diagnosis,’’ in *World Congress on Medical Physics and Biomedical Engineering*. Singapore: Springer, 2019, pp. 905–909.

[41] A. Chandrasekhar, M. Yavarimanesh, K. Natarajan, J.-O. Hahn, and R. Mukkamala, ‘‘PPG sensor contact pressure should be taken into account for cuff-less blood pressure measurement,’’ *IEEE Trans. Biomed. Eng.*, early access, Feb. 28, 2020, doi: 10.1109/TBME.2020.2976989.

[42] *Measuring Heart Rates With Light Technology Applications Expands in Wearables and Potentially Home Healthcare Applications, Says LED Inside*. Accessed: Mar. 13, 2020. [Online]. Available: https://www.ledinside.com/intelligence/2016/5/measuring_heart_rates_with_light_technology_applications_expands_in_wearables_and_potentially_home_healthcare_applications_says

[43] *Global Smart Wearable Device Market to Grow at a CAGR of over 16% through 2016-2024 Research Nester*. Accessed: Mar. 13, 2020. [Online]. Available: https://medium.com/@Mresearchnester/global-smart-wearable-device-market-to-grow-at-a-cagr-of-over-16-through-2016-2024-research-nester-3d4178d05a99

[44] M. Kok, J. D. Hol, and T. B. Schön, ''Using inertial sensors for position and orientation estimation,'' 2017, *arXiv:1704.06053*. [Online]. Available: http://arxiv.org/abs/1704.06053

[45] R. H. Rogne, T. H. Bryne, T. I. Fossen, and T. A. Johansen, ''On the usage of low-cost MEMS sensors, strapdown inertial navigation, and nonlinear estimation techniques in dynamic positioning,'' *IEEE J. Ocean. Eng.*, early access, Feb. 18, 2020, doi: 10.1109/JOE.2020.2967094.

[46] Y. Wu, H.-B. Zhu, Q.-X. Du, and S.-M. Tang, ''A survey of the research status of pedestrian dead reckoning systems based on inertial sensors,'' *Int. J. Automat. Comput.*, vol. 16, no. 1, pp. 65–83, Feb. 2019.

[47] J. Collin, P. Davidson, M. Kirkko-Jaakkola, and H. Leppäkoski, ''Inertial sensors and their applications,'' in *Handbook of Signal Processing Systems*. Cham, Switzerland: Springer, 2019, pp. 51–85.

[48] M. Pérez-Jiménez, B. Sánchez, A. Migliorini, and R. Alcarria, ''Protecting private communications in cyber-physical systems through physical unclonable functions,'' *Electronics*, vol. 8, no. 4, p. 390, 2019.

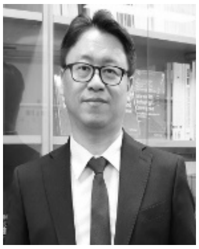
[49] H. Al-Aqrabi, A. P. Johnson, R. Hill, P. Lane, and L. Liu, ''A multi-layer security model for 5G-enabled industrial Internet of Things,'' in *Proc. Int. Conf. Smart City Inform.* Singapore: Springer, 2019, pp. 279–292.

[50] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, ''A survey on hardware-based security mechanisms for Internet of Things,'' 2019, *arXiv:1907.12525*. [Online]. Available: http://arxiv.org/abs/1907.12525

[51] H. Zhuang, X. Xi, N. Sun, and M. Orshansky, ''A strong subthreshold current array PUF resilient to machine learning attacks,'' *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 1, pp. 135–144, Jan. 2020.

PRADIP KUMAR SHARMA (Member, IEEE) received the Ph.D. degree in CSE from the Seoul National University of Science and Technology, South Korea, in August 2019. He is currently with the Department of Multimedia Engineering, Dongguk University, South Korea. He has published many technical research articles in leading journals of the IEEE, Elsevier, Springer, and MDPI. His some research findings are published in most-cited journals. His current research interests are focused in the areas of cybersecurity, blockchain, edge computing, SDN, SNS, and the IoT security. He has also been invited to serve as the Technical Programme Committee Member and the chair of several reputed international conferences such as the IEEE ICC 2019, the IEEE MENACOMM 2019, and 3ICT 2019. He received a top 1% reviewer of computer science by Publons Peer Review Awards, Clarivate Analytics, in 2018 and 2019. He has been serving as a guest editor for international journals of certain publishers such as Springer, MDPI, and JIPS. He is currently an Associate Editor of *Human-Centric Computing and Information Sciences* (HCIS) and the *Journal of Information Processing Systems* (JIPS). He has been an Expert Reviewer of the IEEE TRANSACTIONS, Elsevier, Springer, and MDPI journals and magazines.

JISUN PARK received the B.Eng. degree in multimedia engineering from the Institute of Computer Science, Dongguk University, Seoul, South Korea, in 2016, and the M.Eng. degree in multimedia engineering from Dongguk University, in 2018, where she is currently pursuing the Dr.Eng. degree with the Department of Multimedia Engineering. Her current interests are focused on 3-D reconstruction, artificial intelligence, and deep learning.



JONG HYUK PARK (Member, IEEE) received the Ph.D. degree from the Graduate School of Information Security, Korea University, South Korea, and the Ph.D. degree from the Graduate School of Human Sciences, Waseda University, Japan. From December 2002 to July 2007, he was a Research Scientist of the Research and Development Institute, Hanwha S&C Company, Ltd., South Korea. From September 2007 to August 2009, he was a Professor at the Department of Computer Science and Engineering, Kyungnam University, South Korea. He is currently a Professor with the Department of Computer Science and Engineering and the Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), South Korea. He has published about 200 research articles in international journals and conferences. His research interests include the IoT, human-centric ubiquitous computing, information security, digital forensics, vehicular cloud computing, and multimedia computing. He is a member of the IEEE Computer Society, KIPS, and KMMS. He got the Best Paper Award from ISA 2008 and ITCS 2011 conferences and the Outstanding Leadership Award from the IEEE HPCC 2009, ICA3PP 2010, IEE ISPA 2011, PDCAT 2011, and the IEEE AINA 2015. Furthermore, he got the Outstanding Research Award from the SeoulTech, in 2014. He has been serving as a chair and a program committee or an organizing committee chair of many international conferences and workshops. He is a Steering Chair of international conferences such as MUE, FutureTech, CSA, CUTE, UCAWSN, and World IT Congress-Jeju. He is an Associate Editor/Editor of 14 international journals including JoS, JNCA, SCN, and CJ. In addition, he has been serving as a guest editor for international journals of some publishers such as Springer, Elsevier, John Wiley, Oxford University Press, Emerald, Inderscience, and MDPI. He is the Editor-in-Chief of *Human-Centric Computing and Information Sciences* (HCIS) (Springer), the *Journal of Information Processing Systems* (JIPS) (KIPS), and the *Journal of Convergence* (JoC) (KIPS CSWRG).

KYUNGEUN CHO (Member, IEEE) received the B.Eng. degree in computer science, and the M.Eng. and Dr.Eng. degrees in computer engineering from Dongguk University, Seoul, South Korea, in 1993, 1995, and 2001, respectively. From 1997 to 1998, she was a Research Assistant at the Institute for Social Medicine, Regensburg University, Germany, and a Visiting Researcher at the FORWISS Institute, TU-Munchen University, Germany. She has been a Full Professor with the Department of Multimedia Engineering, Dongguk University, Seoul, since September 2003. She has led a number of projects on robotics and game engines and has also published many technical articles in her research areas. Her current research interests are focused in the areas of artificial intelligence of robots and virtual characters, and real-time computer graphics technologies.