Securing Military IoT: Context-Aware Biometrics at the Edge

Abdul Baseer Buriro, Attaullah Buriro, Muhammad Ali Jamshed, Wali Ullah Khan, and Muhammad Azfar Yaqub

Abstract

The increasing exploitation of the Internet of Things (IoT) in military settings has revolutionized the development of interconnected defense systems, resulting in the concept of the Internet of Military Things (IoMT). Within this technological ecosystem, wearable devices, especially smartwatches, have emerged as inevitable tools to improve the operational effectiveness and safety of soldiers. This study examines how smartwatches could function as edge devices to verify the identity of soldiers and to monitor their health in real time. By employing biometrics such as gesture recognition (for example, how wearer checks the time or gives a thumbs up) and meticulously analyzing these patterns, soldiers can be securely authenticated, to access sensitive information and IoT systems. Moreover, smartwatches can track biological signals, including Electrocardiogram (ECG) and Electromyographic (EMG) data, to comprehensively assess soldiers' emotional well-being and strategically respond when necessary. The fusion of technology with edge computing and behavioral biometrics in military wearables represents a groundbreaking advancement in modern warfare tactics and equipment.

Introduction

Technological convergence of the Internet of Things (IoT) has radically transformed multiple sectors. This innovation enables seamless device interconnectivity, creating smarter, more responsive systems. In the defense sector, this technological evolution has catalyzed the Internet of Military Things (IoMT)- a specialized technological ecosystem designed for military applications. IoMT comprehensively integrates interconnected devices and sensors to optimize situational awareness, logistics, and real-time decision making [1].

Wearable technologies represent a critical architectural component of IoMT. Smartwatches emerge as sophisticated edge computing nodes, providing soldiers with instantaneous data and health monitoring capabilities. These devices autonomously process local data, enabling rapid decision making without centralized system dependencies. Real-time biometric tracking becomes a strategic advantage in high-stakes military environments, where timely information is critical to mission outcomes [2].

In military operations, robust personnel authentication is critically imperative to prevent unauthorized access to system [4]. Traditional authentication methods, passwords and ID cards, prove fundamentally inadequate in dynamic environments. These approaches are inherently vulnerable, susceptible to compromise and pose significant security risks. Critically, they lack continuous authentication mechanisms, creating potential unauthorized access vulnerabilities.

Behavioral biometrics has emerged as a transformative authentication strategy. Using unique behavioral signatures — walking patterns, gestures, device interactions — soldiers can achieve continuous real-time verification. As demonstrated in Fig. 1, smartwatches enable sophisticated person-specific profiling through arm-movement analysis [3]. This approach dynamically adapts to changing operational conditions, ensures accuracy of authentication under stress. Although behavioral biometrics demonstrate an exceptional smartphone authentication potential [5], military wearable deployment remains an emerging technological frontier.

This article investigates smart wrist wearables as edge authentication devices within the IoMT ecosystem and contributes in the following ways:

- Critically assessing biometric verification methodologies, evaluating accuracy and reliability in military scenarios.
- Analyzing smartwatch capabilities in tracking biometric signals — ECG and EMG — to comprehensively monitor soldier emotional and physical well-being.
- Exploring IoMT infrastructure integration, investigating data security challenges and connectivity solutions.

By synthesizing interdisciplinary research, this review provides a comprehensive technological landscape of smartwatch potential in enhancing the safety, security, and operational effectiveness of military personnel.

Literature Review

In this part of our work we examine the research carried out in the three primary technologies.

Wearable Technology: The New Frontier

The Emerging Realm of Wearable Technology smart wearables such as smartwatches have become indispensable tools in military settings.

Abdul Baseer Buriro is with Sukkur IBA University, Pakistan; Attaullah Buriro and Muhammad Azfar Yaqub (corresponding author) are with Free University of Bozen-Bolzano Italy; Muhammad Ali Jamshed is with University of Glasgow, UK; Wali Ullah Khan is with the University of Luxembourg, Luxembourg.

Digital Object Identifier: 10.1109/IOTM.001.2400147

2576-3180/25/$25.00 © 2025 IEEE

They have been used for monitoring vital signs and movements while delivering real-time information to soldiers and command centers using a variety of built-in sensors. The capability of processing data on the device - termed edge computing enables quick decision making without the dependence on centralized systems. Smartwatches have been used effectively in different fields to recognize activities and verify user identities [3]. They can play a vital role in ensuring security infrastructure and connecting with IoT applications.

This research explores the ways in which these technologies could be adjusted and utilized in the field of IoMT to improve the security and effectiveness of systems. By leveraging the features of smartwatches or similar devices, the goal of this study is to offer creative solutions for verifying soldiers identities, and monitoring their well being in real-time settings. The successful integration of sensors into military contexts, like those seen in the German armed forces further demonstrates the practical advantages and possibilities offered by such technologies [6].

Behavioral Biometrics: Continuous and Adaptive Authentication

In high-pressure military environments, traditional authentication methods, such as passwords or ID cards, may not be sufficient. Behavioral biometrics offers a more secure alternative by leveraging unique patterns in a soldier's behavior. For example, how a soldier checks time, performs specific hand signals, or how they walk, can be used to continuously and adaptively authenticate their identity. This authentication means that only approved personnel can access confidential information and systems, greatly reducing the probability of security breaches [7].

Soldiers' behavior could be analyzed for the development of adaptable authentication schemes using behavioral biometric methods, i.e., gesture recognition [5] and EMG [3] signals. Gesture recognition involves studying how soldiers use their smartwatches by observing actions such as checking the time or making gestures, like clapping or snapping fingers. Through the analysis of these data using advanced machine learning techniques, the aim is to create a real-time authentication system that seamlessly adjusts to the evolving circumstances of soldiers.

In scenarios of operational research, researchers have looked extensively into the use of behavioral biometrics. The study by Zwanenburg et al. [7] discusses the application of biometrics in military operations and highlights the importance of automated recognition based on biological and behavioral characteristics. Another study by Burmaoglu *et al.* [1] stresses the influence of IoMT on improving situational awareness and decision-making on the battlefield. Furthermore, a comprehensive review by El et al. [2] offers valuable insights into the efficacy of behavioral biometrics for user authentication in high-stakes situations.

Using these advancements in technology, we can establish a strong and flexible verification system that prioritizes the safety and effectiveness of military personnel. This method not only boosts security measures but also adjusts to the varied circumstances faced by soldiers, guaranteeing accurate verification even during challenging scenarios [5].

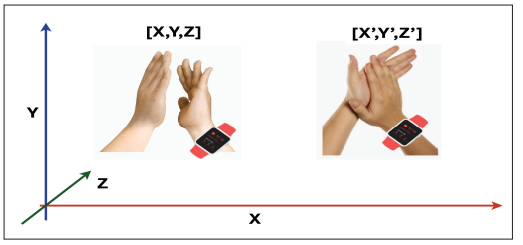

FIGURE 1. Gesture (i.e., clapping) collection, using smartwatch, in 3D space [3].

Edge Computing: Real-Time Processing and Decision Making

Edge computing plays an important role in the IoMT ecosystem by enabling instant data processing at the point of origin. Smart wearables, such as smartwatches can analyze biometric information on-site to offer immediate feedback and responses. It helps in decreasing delays, boosting data protection, and guaranteeing that soldiers receive timely mission-related updates. The fusion of edge computing with advanced technology and behavioral biometrics forms an effective seamless system that adapts to the dynamic nature of battlefield environments.[1]

In military operations, the ability to process data locally on the device, known as edge computing, is crucial. It becomes important to process data directly on the device using edge computing technology instead of relying solely on centralized systems that may be prone to delays and security risks. By exploiting edge computing for smartwatches to analyze signals, i.e., heart rate variability, and EMG data in real-time, it can estimate the physical and emotional state of soldiers [3].

Edge computing also improves the security of the IoMT framework by handling data processing on the device itself instead of transmitting it over networks where interception risks are greater. This localized processing feature ensures that soldiers receive timely and secure information for making swift and well-informed decisions in critical situations.

The integration of behavioral biometrics, edge computing, and wearable technology specifically tailored for Military IoT (MIoT) applications introduce a novel approach that has not been explored in depth. Unlike civilian applications, MIoT solutions demand adaptive authentication, stress detection, and situational awareness in high-risk environments. This study uniquely addresses these demands by combining real-time behavioral biometrics with edge computing capabilities in smartwatches to support secure, continuous soldier authentication and health monitoring. This approach provides a foundation for improved situational awareness and tactical advantage in military operations, representing a significant advancement in IoMT research.

Case Studies and Real-World Applications

Figure 2 illustrates the complete process: It shows that smartwatches could be used to collect 3D sensory data generated from different actions (also termed as gestures), or other biometric signals, such as EMG or ECG, from soldiers to analyze this data in real-time. In addition to local decision-making, this data could also be securely transmitted through a Virtual Private Network

Gesture recognition involves studying how soldiers use their smartwatches by observing actions such as checking the time or making gestures, like clapping or snapping fingers.

[1] https://www.nationaldefensemagazine.org/articles/2021/10/7/the-rise-of-edge-computing-in-defense.

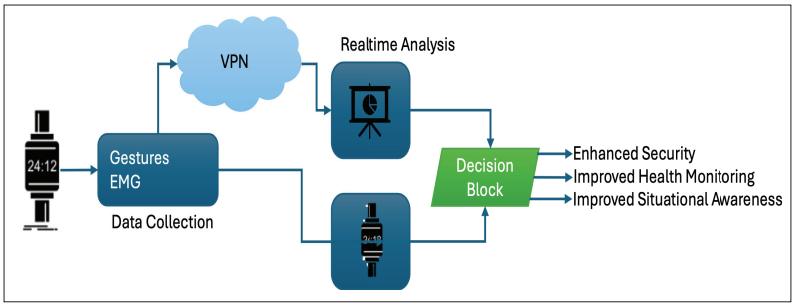

FIGURE 2. Graphical illustration of combining behavioral biometrics with edge computing.

(VPN) to the Command and Control Center to ensure privacy. Real-time analysis helps to make informed decisions, leading to outcomes such as enhanced security, improved health monitoring, and better situational awareness. Essentially, it shows how real-time data processing and secure transmission can be used to achieve significant benefits in various applications.

The integration of smartwatches, behavioral biometrics and edge computing in the IoMT framework could provide promising results in various military applications, such as in verifying the identity of soldiers, continuously monitoring their state of mind to make better decisions and creating better situational awareness. This section highlights some real-world examples and case studies that demonstrate the effectiveness of these technologies.

Case Study 1: Real-Time Soldier Authentication

The studies by Buriro et al. [3, 8] and Guerar et al. [9] indicate that smartwatch users can be verified based on their produced data while participating in various arm movements. In their investigation reported in [3], the study showcases how smartwatch technology could provide continuous authentication for soldiers. By tracking EMG signals and sensory data during activities, such as clapping using smartwatch devices, studies ensure that authorized military personnel can access critical infrastructure securely. The research showed that implementing this security measure could greatly reduce the chances of unauthorized entry and improve the overall safety of the system.

The results of these studies are promising. These studies have proved to be highly effective in authenticating users and maintaining security. They could ensure blocking unauthorized attempts, significantly reducing the risk of security breaches. Furthermore, these techniques could be used to provide continuous authentication of the soldiers and adapt to changing conditions of the soldiers in high-pressure environments [10].

Case Study 2: Health Monitoring and Stress Management

Another interesting application of the use of smartwatches is to track the health and stress levels of soldiers in real-time situations. The smartwatches analyze heart rate variability (HRV) as well as EMG data to give an insight into the physical and emotional conditions of soldiers. HRV is a known factor that indicates stress levels and cardiovascular health in general; monitoring it in real-time can provide crucial information about a soldier's readiness and stress levels [11]. Furthermore, EMG data measures muscle activity that could contribute to assessing physical strain and fatigue in soldiers.

In a study by Jerath et al., the integration of smartwatches with HRV technology was shown to be effective in providing real-time stress feedback and personalized stress management interventions [11]. This capability is particularly beneficial in military settings, where maintaining optimal physical and mental health is crucial for mission success. By continuously monitoring these biometric signals, commanders can make informed decisions about troop deployment and support, thereby improving mission outcomes and soldier well-being.

In addition, the VitalMonitor initiative under the Austrian Defence Research Program showcased the utility of biosensors to monitor real-time physiological stress in military training and operations, as discussed by Almer et al. [12]. By continuously monitoring these biometric signals, commanders can make informed decisions about troop deployment and support, thereby improving mission outcomes and soldier well-being.

These applications show how smartwatches and wearable tech can improve the well-being and effectiveness of personnel. By leveraging biometric information effectively, military leaders can ensure that their troops are in the best possible condition to perform their duties, ultimately contributing to the success of military operations [11].

Case Study 3: Enhanced Situational Awareness

Smartwatches could also be exploited to improve situational awareness on the battlefield. By integrating with other IoMT gadgets, these devices provide real-time updates or notifications on environmental conditions, enemy movements, and logistical information. This integration allows soldiers to make faster and more informed decisions, giving them a tactical edge in combat situations.

In a recent study by Cho et al. [13], the integration of smartwatches with an aerial reconfigurable intelligent surface (ARIS)-assisted integrated sensing and communication (ISAC) system demonstrated significantly enhanced battlefield awareness. The smartwatches, in conjunction with other IoMT devices, provided real-time data on various battlefield parameters, enabling soldiers to respond quickly to changing conditions [13]. This system exploits deep reinforcement learning to optimize the transmission of beamforming and phase shifts, ensuring reliable communication and accurate sensing in complex environments. The integration of these devices with other IoMT systems allowed seamless data sharing and coordination, enhancing the overall operational efficiency of military units.

The ability to receive real-time logistical information through smartwatches could also prove beneficial. In that case, soldiers equipped with smartwatches could access up-to-date information on supply routes, ammunition levels, and medical support availability. This information is crucial for effectively planning and executing missions, reducing the risk of logistic failure and improving mission outcomes [14].

Figure 3 illustrates a sophisticated system in which data is captured from wearable devices, such as smartwatches, and processed in real-time

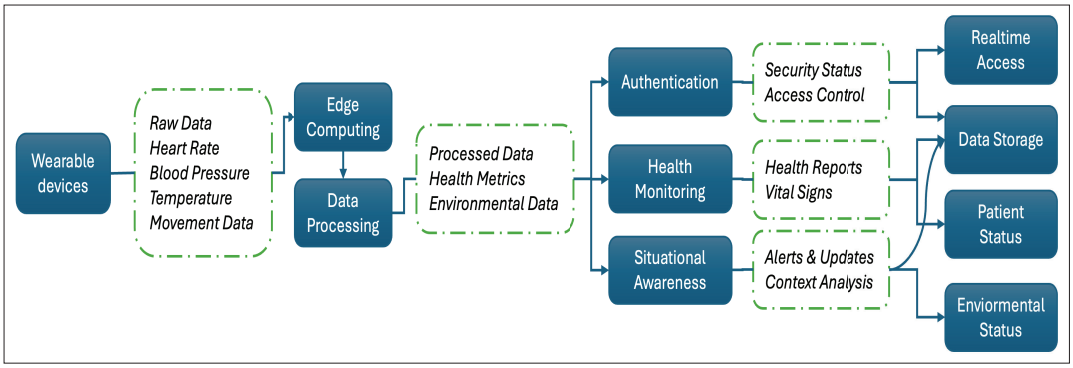

FIGURE 3. Graphical illustration of depicting the functions involved in the process.

The use of edge computing ensures that data processing is efficient and secure, while wearable technology provides a convenient and non-intrusive means of data collection.

using edge computing. Behavioral data undergoes various processing stages, including feature extraction, concatenation, selection, and optimization, all performed on the smartwatch itself. This immediate processing reduces latency and enhances the system's responsiveness. The processed data is then classified to verify the individual's identity and further to determine the individual's mental state (such as stress level), which is communicated to a command and control center for real-time health monitoring. This setup improves situational awareness, making it particularly useful in high-stress environments such as military operations or critical healthcare scenarios.

By integrating behavioral biometrics, edge computing, and wearable technology, the system can continuously monitor health metrics and provide timely insights, leading to improved decision-making and performance. The use of edge computing ensures that data processing is efficient and secure, while wearable technology provides a convenient and non-intrusive means of data collection. This combination of technologies enables advanced tasks such as real-time soldier authentication, stress detection, and situational awareness, ultimately contributing to enhanced security and health monitoring. Overall, the integration of smartwatches with IoMT devices is set to demonstrate significant potential to improve situational awareness on the battlefield. By providing real-time updates and facilitating quick decision-making, these technologies offer a tactical advantage that is essential for modern military operations.

Challenges and Future Directions

In MIoT applications, there are unique demands that go beyond those of civilian IoT deployments. MIoT requires heightened security measures, enhanced data robustness, and resilience to extreme environmental challenges. Unlike civilian applications, MIoT must operate reliably in highly stressful and potentially hostile environments, where data integrity and secure communications are essential for mission success. Military settings impose stringent security protocols, including strong encryption and continuous monitoring to ensure only authorized access. Additionally, MIoT systems must withstand environmental factors such as high temperatures, humidity, physical shocks, and interference. These specialized requirements make MIoT applications fundamentally different from civilian IoT and necessitate solutions that can meet the demanding conditions of military operations.

The use of smartwatches together with behavioral biometrics and edge computing not only brings notable benefits but also certain challenges that need to be addressed. In this section, we discuss the technical, logistical, and security challenges.

Technical Challenges

One of the technical challenges involves ensuring that behavioral biometric systems are accurate and reliable in constantly evolving and active military settings. Factors such as changes in conditions and stress levels as well as fluctuations in environmental elements, can influence the effectiveness of biometric sensors and algorithms. For example, changes in temperature, variations in humidity levels, and physical activity can impact the quality of collected data, potentially resulting in inaccuracies.

Emotional states, such as stress levels, could play a significant role in the performance of biometric systems. High-stress situations, common in military operations, can alter a soldier's physiological and behavioral responses, potentially impacting the accuracy of biometric authentication. Environmental factors like noise and movement can introduce challenges, making it difficult to maintain consistent biometric readings.

Edge devices face resource constraints, including limited computational power, memory, and battery life, which challenge running complex biometric algorithms. These limitations affect both the performance and the feasibility of deploying advanced biometric systems in wearables. To address these constraints, optimizing algorithms for low-resource environments and adopting efficient power management techniques are essential for sustaining biometric functionality in remote or high-stress settings.

Real-time processing and low latency are crucial in military contexts, where immediate authentication is required. High latency can compromise system responsiveness, particularly in context-aware applications. Addressing latency issues involves prioritizing lightweight processing and optimizing communication protocols.

In summary, ensuring the reliability of behavioral biometric systems in military settings requires robust algorithms and innovative approaches to handle resource constraints, environmental variability, and latency requirements. These approaches enable secure, real-time performance in dynamic and challenging military environments.

Logistical Challenges

Deploying and maintaining wearable devices in Military Internet of Things (MIoT) presents sig-

Ensuring that wearable devices are protected against cyberattacks and unauthorized access is critical. The decentralized setup of edge computing systems makes them vulnerable to security risks such as data breaches, distributed denial of service attacks, and unauthorized entry.

nificant logistical challenges. Ensuring that devices are adequately powered, securely connected, and properly maintained requires careful planning and coordination. For example, continuous device operation necessitates reliable power sources, which can be challenging to manage in remote or hostile environments.

Secure connectivity is a critical concern for wearable devices. These devices must maintain robust and secure communication links to transmit data without interruption. This requires implementing advanced encryption methods and secure communication protocols to protect sensitive information from potential cyber threats. The integration of wearable devices with existing military communication infrastructure also requires careful planning to ensure compatibility and reliability.

Proper maintenance of wearable devices is crucial to ensure their functionality and longevity. Regular maintenance checks and updates are necessary to keep the devices in optimal working condition. This includes both hardware and software maintenance, such as sensor calibration and firmware updates.

Additionally, training soldiers to effectively use and trust these technologies is essential for successful implementation. Soldiers must be familiar with the operation and capabilities of wearable devices to fully leverage their benefits. Training programs should focus on both the technical aspects of device usage and practical applications in military scenarios. The VitalMonitor project, part of the Austrian Defence Research Program, demonstrated the effectiveness of comprehensive training programs in enhancing the adoption and utilization of wearable biosensors in military settings.

By addressing these logistical challenges, military organizations can ensure the successful deployment and maintenance of wearable devices, ultimately enhancing the operational efficiency and effectiveness of their personnel.

Security Challenges

Edge computing improves data security by handling information locally, but this approach also introduces new security risks. Ensuring that wearable devices are protected against cyberattacks and unauthorized access is critical. The decentralized setup of edge computing systems makes them vulnerable to security risks such as data breaches, distributed denial of service attacks, and unauthorized entry. Developing advanced encryption methods and secure communication protocols is essential to mitigate these risks. For instance, the implementation of Zero Trust Security principles in edge computing environments [15] has been proposed as a way to enhance security. This approach involves continuous verification of user identities and strict access controls, ensuring that only authorized personnel can access sensitive data and systems. In addition, secure network segmentation and continuous monitoring systems can help detect and respond to potential threats in real-time.

Adaptive security measures, such as randomized defense mechanisms, have been explored to protect edge data centers. These mechanisms involve dynamically changing security configurations to make it more difficult for attackers to exploit vulnerabilities. By employing stochastic game theory, researchers can develop optimal security deployment strategies to enhance the resilience of edge computing systems against cyberattacks. Furthermore, the integration of edge security gateways and firewall systems provides perimeter protection for edge settings. These systems can filter and monitor incoming and outgoing traffic, preventing unauthorized access and ensuring data integrity [15]. Cloud-based security services and threat intelligence platforms can also be leveraged to improve threat detection and response capabilities, providing an additional layer of security for edge computing environments [15]. By addressing these security challenges, researchers can develop robust and secure edge computing solutions that protect wearable devices and their sensitive data.

Securing Military Internet of Things (MIoT) systems against cyber threats is essential due to the decentralized and often remote nature of edge computing environments. Adaptive security measures, such as Zero Trust architectures, have become crucial for MIoT, emphasizing strict access controls and continuous verification of user identities. Techniques like secure network segmentation and continuous monitoring provide additional protection, enabling real-time threat detection and response. Stochastic defense mechanisms, such as randomized security configurations, can further enhance resilience by preventing attackers from exploiting predictable patterns. These approaches address the unique security challenges in MIoT and help safeguard sensitive data, ensuring reliable operation in potentially hostile environments.

Conclusions

This research presents a novel approach to securing MIoT environments by integrating behavioral biometrics, edge computing, and wearable technology for military applications. Using smartwatches as edge devices this study addresses critical security and operational requirements unique to military contexts. The approach aims at enhancing security, situational awareness, and enables quick decision-making, providing a tactical advantage for modern military operations.

The combination of these technologies offers a secure and effective solution for contemporary warfare scenarios. Using smartwatches to collect and process biometric data for authentication and emotion detection locally on smartwatch, we can achieve remarkable levels of security and operational effectiveness.

In future studies, we will:

- Understand how wearable devices integrate with MIoT systems
- Conduct experimental evaluations to ensure accuracy of behavioral biometrics,
- Develop more secure edge computing solutions.

We believe that connecting devices with MIoT systems can significantly improve operational efficiency and situational awareness. We will explore wearable technologies like Augmented Reality (AR) glasses and smart textiles to expand IoMT functionalities. AR glasses can provide soldiers with real-time information overlays, enhancing battlefield awareness and decision-making. By advancing these research domains, future IoMT systems may become more reliable, productive, and adaptable, ultimately contributing to military personnel safety and efficiency.

References

[1] S. Burmaoglu *et al.*, "Defense 4.0: Internet of Things in Military," *Emerging Technologies for Economic Development*, 2019, pp. 303–20.

[2] A. A. El-Saleh *et al.*, "The Internet of Medical Things (IoMT): Opportunities and Challenges," *Wireless Networks*, 2024, pp. 1–18.

[3] A. Buriro *et al.*, "Wearable Wisdom: A Bimodal Behavioral Biometric Scheme for Smartwatch User Authentication," *IEEE Access*, 2024.

[4] K. Sahu *et al.*, "Military Computing Security: Insights and Implications," *J. Institution of Engineers (India): Series B*, 2024, pp. 1–25.

[5] A. Buriro, Behavioral Biometrics for Smartphone User Authentication, Ph.D. Thesis, University of Trento, 2017.

[6] L. Scheit, "Optimizing the Introduction of Wearable Sensors Into the German Armed Forces for Military Medical Applications," *Military Medicine*, vol. 186, no. 9–10, 2021, pp. 962–68.

[7] M. Zwanenburg, "Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law," International Law Studies, vol. 97, no. 1, 2021, p. 49.

[8] A. Buriro *et al.*, "Airsign: A Gesture-Based Smartwatch User Authentication," *2018 Int'l. Carnahan Conf. Security Technology (ICCST)*, 2018, pp. 1–5.

[9] M. Guerar *et al.*, "Circlepin: A Novel Authentication Mechanism for Smartwatches to Prevent Unauthorized Access to IoT Devices," *ACM Trans. Cyber-Physical Systems*, vol. 4, no. 3, 2020, pp. 1–19.

[10] I. Deutschmann *et al.*, "Continuous Authentication Using Behavioral Biometrics," *IT Professional*, vol. 15, no. 4, 2013, pp. 12–15.

[11] R. Jerath *et al.*, "The Future of Stress Management: Integration of Smartwatches and HRV Technology," *Sensors*, vol. 23, no. 17, 2023, p. 7314.

[12] A. Almer *et al.*, "Multisensory Wearable Vital Monitoring System for Military Training, Exercise and Deployment," *Advances in Neuroergonomics and Cognitive Engineering: Proc.e AHFE 2021 Virtual Conf. Neuroergonomics and Cognitive Engineering, Industrial Cognitive Ergonomics and Engineering Psychology, and Cognitive Computing and Internet of Things*, July 25–29, 2021, USA, Springer, 2021, pp. 497–505.

[13] H. Cho *et al.*, "Enhancing Battlefield Awareness: An Aerial RIS-Assisted ISAC System with Deep Reinforcement Learning," arXiv preprint arXiv:2405.20168, 2024.

[14] A. Sharma and S. Aggarwal, "Real-Time Health Monitoring System of Soldiers Using IoT," *Advanced Computational Paradigms and Hybrid Intelligent Computing: Proc. ICACCP 2021*, Springer, 2022, pp. 285–96.

[15] F. Ashfaq *et al.*, "Enhancing Zero Trust Security in Edge Computing Environments: Challenges and Solutions," *World Conf. Information Systems and Technologies*, Springer, 2024, pp. 433–44.

Biograpgihies

Abdul Baseer Buriro (abdul.baseer@iba-suk.edu.pk) is an Assistant Professor at Sukkur IBA University, Pakistan. He earned his Ph.D. in Electrical and Electronic Engineering from the University of Canterbury, Christchurch, New Zealand, in 2019. His research focuses on signal processing, machine learning, and deep learning, with a particular emphasis on Electroencephalogram (EEG) signals. He is a dedicated educator and researcher, regularly publishing in and reviewing for leading international journals.

Attaullah Buriro (aburiro@unibz.it) is currently holding the post of Assistant Professor at the Free University of Bolzano, Italy. Prior to that he held a postdoctoral researcher position at the Free University of Bolzano (Sep. 2019–Aug. 2020) and DISI Security Lab, University of Trento (Mar. 2017–Aug. 30 2019). He earned his Ph.D. degree in Information and Communication Technology (security and privacy) from the University of Trento, Italy, in February 2017. His research interests include biometrics, access control, the Internet of Things (IoT), Computer Vision, machine learning, artificial intelligence, and data mining. He has developed several secure, user-friendly, and implicit behavioral biometric-based authentication solutions for smartwatches, smartphones, and critical infrastructures.

Muhammad Ali Jamshed [SM] (muhammadali.jamshed@glasgow.ac.uk) received a Ph.D. degree from the University of Surrey, Guildford, U.K, in 2021. He is with University of Glasgow, since 2021. He is endorsed by Royal Academy of Engineering under exceptional talent category and was nominated for Departmental Prize for Excellence in Research in 2019 and 2020 at the University of Surrey. He is a Fellow of Royal Society of Arts, a Fellow of Higher Education Academy UK, a Member of the EURASIP Academy, and an Editor of *IEEE Wireless Communication Letters* and an Associate Editor of *IEEE Sensor Journal*, *IEEE Internet of Things Magazine*, and *IEEE Communication Standard Magazine*. His research interests are energy efficient IoT networks, AI for wireless communication, EMF exposure measurements, and backscatter communications.

Wali Ullah Khan [M] (waliullah.khan@uni.lu) received a Ph.D. degree in information and communication engineering from Shandong University, China, in 2020. He is currently working with the SIGCOM Research Group at SnT, University of Luxembourg. His research interests include wireless communications, integrated terrestrial non-terrestrial networks, 6G technologies.

Muhammad Azfar Yaqub [M] (myaqub@unibz.it) is currently an Assistant Professor with the Faculty of Engineering, Free University of Bozen-Bolzano, Italy, where he teaches data science and machine learning. Previously, he was the Department of Electrical Engineering, COMSATS University Islamabad, Pakistan. He was awarded his Ph.D. in Computer Science and engineering at the Kyungpook National University, South Korea in 2019 after achieving his MSc (cum laude) in Engineering and Computer Science from the Lancaster University, UK in 2010. His research interests include artificial intelligence theories and applications, particularly e-health, intelligent networks, and intelligent systems. He serves as TPC/reviewer for serveral journals and conferences.