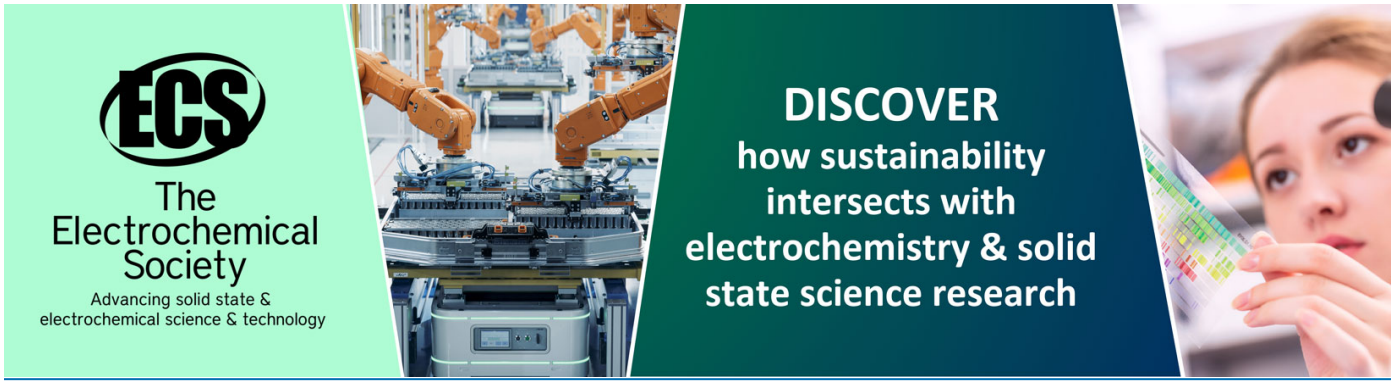
Privacy and security in the use of wearable internet of things for construction safety and health monitoring



Privacy and security in the use of wearable internet of things for construction safety and health monitoring

C Okonkwo[1], I Awolusi,[1] and C Nnaji[2]

[1] School of Civil & Environmental Engineering, and Construction Management, The University of Texas at San Antonio, 501 W César E Chávez Blvd, San Antonio, TX 78207, USA
[2] Department of Construction Science, Texas A&M University, 574 Ross St, College Station, TX 77840, USA

Abstract. Due to the dynamic and complex nature of construction sites, the conventional method of construction safety monitoring which relies mainly on manual observation by inspectors is highly susceptible to human errors, is time-consuming, and is also becoming increasingly difficult to identify all incidents. Wearable Internet of Things (WIoT) in the construction industry creates a lot of opportunities for safety and health management such as identifying real-time locations of workers, body temperature, heart rate, stress level, and breathing rate, which can all be used to ensure that workers are always in safe environments and good health conditions. The use of WIoT for safety and health monitoring however presents research need on the privacy and security of the construction safety and health data collected, transmitted, and processed over the internet. This study examines the concept of privacy and security in WIoT, the security challenges, infrastructure requirements, and legal issues associated with WIoT. A review of privacy and security regulations for safety and health data is also presented in this paper. This study is expected to generate scientific information that can be used to develop an effective privacy and security framework to foster the adoption and implementation of IoT-based wearable sensing devices (WSDs) for safety and health monitoring in construction.

Keywords
Wearable sensing devices, construction safety, Internet of Things (IoT), privacy and security, health monitoring.

1 Introduction

The construction industry is a hazardous industry accounting for more work-related injuries and deaths than any other single industry [1]. The inherent nature of the activities undertaken in the construction work environment exposes construction workers to a considerable amount of safety and health risks. In 2019, the construction industry was responsible for about 20% (1,061) of fatalities in the private industry with the four leading causes of worker fatalities in the construction industry responsible for about 56% of the fatalities—falls, electrocution, struck by an object, and caught-in [2]. Despite the adoption of safety procedures and programs, such as those developed and required by OSHA, the rates of injuries, illnesses, and fatalities in construction have increased steadily over the past five years with one out of five workplace fatalities occurring in the construction industry [3]. It is, therefore, crucial to continuously improve construction safety management to protect the lives and

health of workers through proactive and active safety measures. The conventional method of construction safety monitoring which relies mainly on manual observation by inspectors is highly susceptible to human error and also time-consuming as it is difficult to manually identify all incidents owing to the intricate nature of construction sites [4]. These problems can be significantly reduced with the application of the Internet of Things (IoT) and wearable technology. IoT is a network of physical objects which are supported by embedded technology for data communication and sensors to interact with both internal and external objects states and the environment [5]. Wearable technology is a category of electronic devices that can be worn as accessories or embedded in clothing, that incorporate computers and sensors, and that can be easily worn on the human body [6]. Wearable sensing devices (WSDs) provide real-time safety and health data for construction safety and health monitoring. Wearable technology has been applied in the medical sector to monitor health conditions and to obtain the vitals of patients [7]. These applications of wearable technology can be extended to the construction industry to measure safety performance [8]. Although IoT-based WSDs could be useful safety and health tools, their application in construction is at the elementary stage when compared to other industries.

Wearable electronics have been described as devices that can be worn by humans to continuously and closely monitor individuals' physiological and physical activities, without interrupting or limiting the user's motions [5, 9]. Wearable devices in the construction industry work by collecting health data from workers for processing or transmitting these data to a central database for processing, to improve the safety and health of construction workers. These devices can be used for the continuous monitoring of a wide range of construction hazards and vital signs which can provide early warning signals to workers with high-risk health issues [8, 10]. The most used wearable sensors include wearable body temperature sensors, pulse, and blood oxygen level sensors, accelerometers for motion sensing, airflow sensors, electrocardiograms, and galvanic skin response sensors [11]. However, the presence of a diverse set of onboard sensors also provides an additional attack surface to applications intending to access personal user information in an unauthorized manner [12].

The wearable device industry is still in the development phase and currently faces challenges such as privacy and security concerns [13]. The fact that these devices transmit huge amounts of data that are in most cases considered private to the individuals presents the need for privacy and security while collecting, transmitting, processing, and storing them. Like other connected devices, IoT-based WSDs also referred to as wearable IoT (WIoT) devices are vulnerable to breaches or attacks which impact not only the functionality of the devices but also the security and privacy of the data collected and transmitted. The benefits and great potential of WIoT for accident prevention in construction can only be achieved if users are confident in the privacy of their personal information and the security of the data collected using these devices [14]. Some researchers have explored the feasibility of WIoT in the construction industry [1, 7, 8, 13, 15, 16, 17]. However, there is need for a privacy and security framework to protect the integrity of the data processed and transmitted through WIoT. This study aims to provide scientific information that can be used to develop an effective privacy and security framework to improve the adoption and implementation of WIoT for safety and health monitoring in construction. To achieve the above-stated objective, this study characterizes the concept of privacy and security concerning the construction industry, identifies the different construction safety and health data that can be monitored with WIoT, and reviews the relevant privacy and security regulations for WIoT.

2 Research Methodology

This study presents a literature review of privacy and security in construction safety and health monitoring using WIoT with the aim of identifying scientific information that could be used to develop an effective framework for privacy and security. The study tries to answer the questions of the requirements of an effective WIoT system, the challenges and risks to be anticipated in a WIoT

system, the various types of safety and health data collected from construction workers, and how the data is managed. To answer these questions, a review of WIoT applications is carried out by querying IEEEXplore, ASCE, and ScienceDirect databases with the aforementioned questions to obtain peer-reviewed journals that are directly related to the study. Articles published earlier than 2005 were not considered for this review to reduce the possibility of having obsolete ideas in this study. Relevant reports were also included from an extensive google search. The review focused mainly on identifying the challenges, security requirements, and legal issues that could be obstacles to the widespread adoption of WIoT in construction safety and health monitoring.

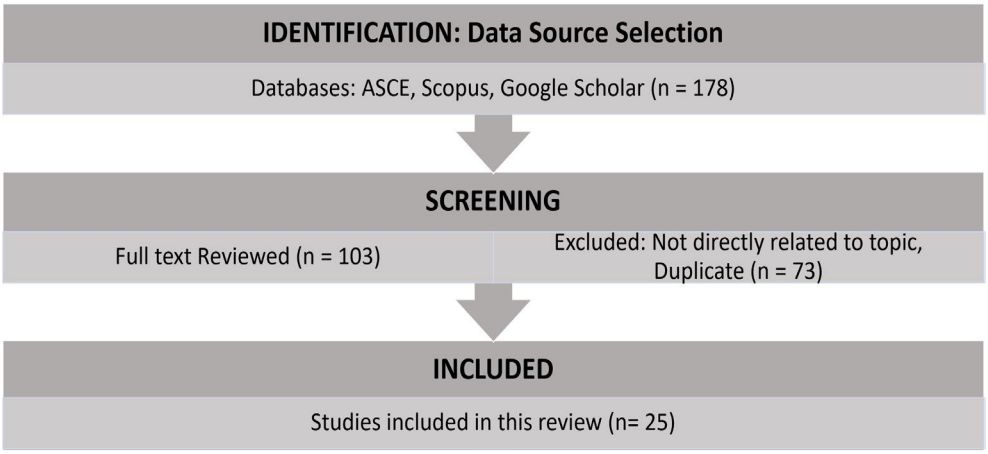


Figure 1. Research process

3 Literature Review

In construction safety and health research, the study of wearable sensing devices (WSDs) and the Internet of Things (IoT) have been attracting huge attention. This is due to the widely reported potential applications of wearable devices for the continuous monitoring of complex safety and health metrics associated with construction activities and conditions in the dynamic and harsh construction work environment [6, 8]. The recent growth in the popularity of interconnected wearable devices with sensing, computing, and communication capability has been very rapid and is paving the way for the widespread use of this class of IoT-based WSDs also referred to as wearable IoT (WIoT) devices. Contemporary mobile and wearable devices, equipped with state-of-the-art sensing and communication capabilities, enable a wide range of unique context-based applications including activity tracking, wellness monitoring, social networking, and home automation [12].

With IoT, digital and physical entities can be linked, using appropriate information and communication technologies, to enable a unique class of applications and services. The concept of IoT provides a solid framework for interconnecting edge computing devices— wearable sensors and smartphones—and cloud computing platforms for seamless interactions [10]. IoT-based WSDs enable the collection, storage, analysis, monitoring, and sharing of a huge amount of data with users and other networked devices. Internet of Things (IoT) refers to the ability of physical devices capable of collecting, processing, and transmitting data to connect with other systems in real-time and exchange data over the Internet [18]. The idea of IoT is to avail inanimate real-world objects with vision, speech, touch, and hearing, to work more effectively in a collaborative and learning environment [19, 20]. As of 2020, there are about 50 billion IoT devices in the world [21]. IoT application in construction creates a lot of opportunities in safety and health management such as identifying real-time locations of workers and obtaining body temperature, heart rate, stress level, and breathing rate, which can all be used to ensure that workers are always in safe environments and good health

conditions. However, these benefits of IoT create the possibility for unauthorized access to the collected data by hackers. Also, access to such health data could unethically influence the decision of employers on employees. Therefore, privacy and security in each architecture layer of IoT are of utmost importance to developers [18].

Privacy and security are crucial parts of any system that involves data management. A review of the Internet of Things by Farooq *et al.* (2015) emphasized the need to address the privacy and security challenges in the use of IoT for its adoption in any industry. The authors concluded that if the challenges of IoT in the areas of confidentiality, privacy, and security are not properly addressed, the technology may not attain universal acceptance despite the numerous possibilities and benefits it offers. Yugha and Chithra (2020) surveyed the various open issues related to security and the use of IoT protocols. The authors discussed the various security attacks on IoT at the different layers of the architecture and identified privacy and security as the most important feature focus for each architecture layer of an IoT system. The study also identified some IoT security requirements like authenticity, availability of services, the privacy of users, integrity, especially during transmission, and confidentiality to avoid leakage of information. In the study of the requirements, challenges, and solutions to IoT security by HaddadPajouh *et al.* (2021), the authors concluded that the lack of a predefined standard for an IoT environment has resulted in different structures of IoT research. The authors classified the IoT system requirements and challenges based on three layers of architecture—perception, network, and application layer. Legislations and standards are necessary for maintaining an effective privacy and security system. According to the United Nations Conference on Trade and Development, only 71% of the countries in the world have data protection and privacy regulation [24]. In the United States, The Health Insurance Portability and Accountability Act (HIPAA) is the major regulatory body. The information provided in this study is expected to foster the development of a comprehensive privacy and security framework for the use of WIoT for construction safety and health monitoring.

4 Findings and Discussion

4.1 Wearable Internet of Things

This section provides an overview of WIoT architecture and operation mechanism, the common security challenges of an IoT system, and the security requirements necessary to protect the integrity of the data passing through the system

4.1.1 WIoT Architecture

For industrial adaptation, the architecture of IoT can be classified into four layers which include the perception layer, transmission layer, computation layer, and application layer [20, 22, 23]. The perception layer simulates the human sense organs by gathering information from the environment. This layer deals with the sources such as sensors, circuits, and actuators, through which the technology obtains information like temperature, humidity, location, motion, etc., from the environment [18, 19, 20]. The transmission layer sends the information obtained in the perception layer to the computation layer for processing. The connectivity required for this layer can be broadly classified into wired and wireless connectivity. Some of the wireless connectivity include Radio Frequency Identification (RFID), radar, magnetic field, ultra-wideband, Bluetooth, etc., while the wired connectivity includes Universal Serial Bus (USB), Zigbee, Long Range Wide Area Network (LoRaWAN), Integrated Service Digital Network (ISDN), Wi-Fi, and RJ45 connector [18, 20]. The computational layer consists of hardware and software working together to process the information obtained by the perception layer. The output from this layer is sent to the application layer. The final layer is the application layer which is the end-user of the cycle where the information obtained and processed is used for the intended purpose.

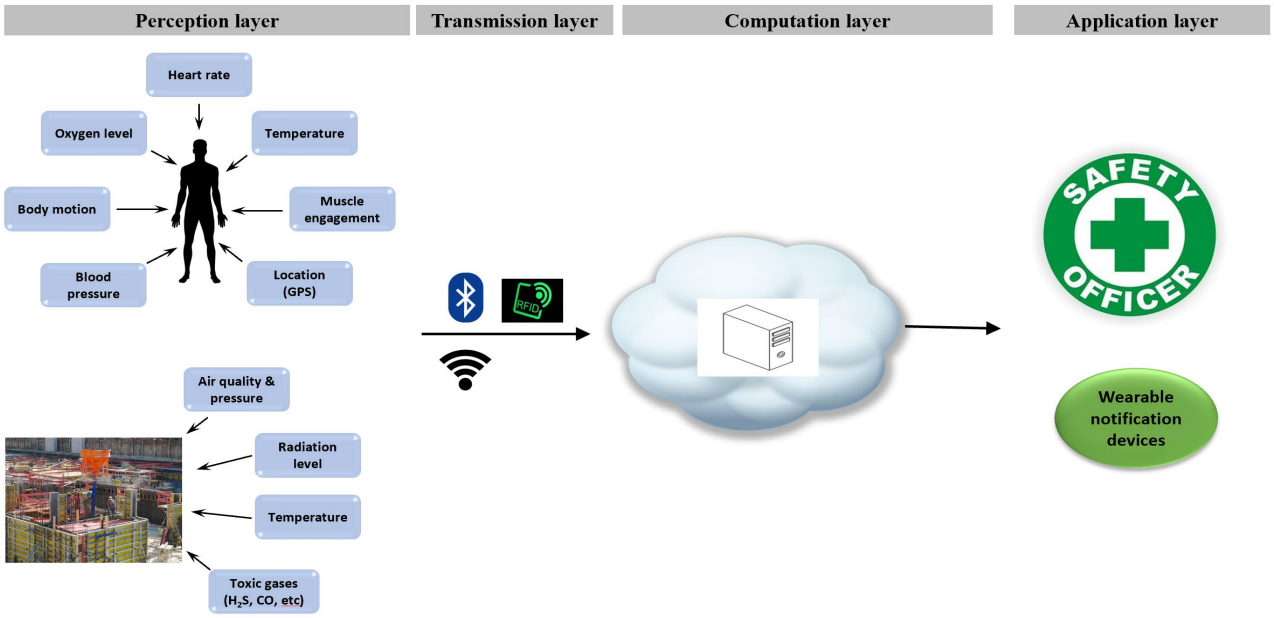


Figure 2. Layers of WIoT

4.1.2 Security Challenges

WIoT in the construction industry is subject to similar security attacks faced by IoT devices in other industries. This section presents a summary of common security attacks on IoT. These attacks occur in the different layers of WIoT architecture from the perception layer through the application layer. Attacks on WIoT sensor nodes could breach security, affect network availability, and compromise authentication, and service integrity [19, 25]. Cloud computing is a network of servers used in IoT for data storage, processing, and sharing. The use of cloud computing, however, presents security vulnerabilities in WIoT such as man-in-the-middle attack which intercepts message transmission between two parties, and malware which is primarily used for system hijacking typically results in data loss [19]. Other security challenges include spoofing attack to gain access to a system by impersonating an authorized device, phishing attack for stealing data like login credentials and card details, and sinkhole attack which tries to reroute network traffic by advertising fake routing update [18]. Table 1 summarizes the common security attacks on IoT technology.

Table 1. Common security attacks on IoT systems

Security attack	Resulting problem
• Sensor node attacks	• Network availability, authentication, service integrity
• Unauthorized RFID access	• Network authentication
• Man-in-the-middle attack	• Unauthorized access to data
• Malware attack	• System hijacking, data loss
• Sleep deprivation attack	• Excessive power consumption and shutdown
• Spoofing attack	• Service denial, bypass access control
• Sinkhole attack	• Data leakage, fake traffic routing
• Phishing attack	• Data leakage

4.1.3 Security Requirements

IoT systems should provide measures to ensure the safety and integrity of the data stored and transmitted through the system. Some of the requirements for an efficient IoT system include authentication, anonymity, encryption, and traffic monitoring [26]. Authentication ensures that only authorized users are granted access to the system. Authentication could be single sign-on, where a user is permitted to sign into a single account, two-way authentication which involves parties testing the validity of each party, or multi-factor authentication which combines different authentication methods [18, 26, 27]. It is a good practice to keep the identity of owners of collected data anonymous to avoid privacy compromise by an unauthorized hand, which can be achieved by de-identification. De-identification is a technique for removing a person's identification information from collected data while preserving as much information as possible [28]. Data transmitted through IoT devices and cloud providers should be securely encrypted to safeguard user privacy and sensitive information. Encryption is the process of encoding information by converting the original form of the information (plaintext) into another form (ciphertext) [26, 29]. Since the application layer works with information it obtains from the transmission and computation layer, the system traffic should be monitored to identify the presence of malware that could corrupt the system. It is a good practice to have an additional layer of protection for anomaly detection [26].

4.2 WIoT Functions for Construction Safety and Health Data Monitoring

The purpose of collecting safety and health data of workers is to monitor and improve workers' safety. Continuous monitoring of workers' activities could help to reduce the number of workplace accidents, as well as injuries, falls, and musculoskeletal problems [30, 31]. This section discusses the different WIoT functions for construction safety and health data monitoring and management.

4.2.1 Physiological Monitoring

Physiological data include cardiac activity, body motion, skin response, eye movement, and muscle engagement [13, 30, 31, 32]. In activity recognition, for instance, real-time body motions of construction workers could be obtained through three common methods which are the kinematic method, computer vision method, and audio method [31]. The kinematic approach identifies different motion patterns of construction workers and equipment with the aid of sensors such as accelerometers and gyroscopes. These sensors are usually contained in portable wearable devices and work by providing information on angular velocity, acceleration, magnetic field, orientation, and speed of rotation of the device [31]. Wearable devices also measure cardiac activity mostly by two methods—photoplethysmography (PPG) and Electrocardiography (ECG). PPG is an indirect method of measuring cardiac activity by flashing a particular wavelength of light from a pulse oximeter sensor when the wearable device meets the skin. The pulse oximeter monitors variations in light absorption when the light illuminates the tissue, and the gadget then uses this information to calculate heart rate [33]. Some of the applications of worker health monitoring include detecting unsafe worker motions, falls, progress monitoring, identifying worker suitable tasks, generating input for simulation models, predicting action patterns for repetitive activities, and identifying areas where improvement is needed [31].

4.2.2 Environmental Monitoring

Worksite environmental stress reduces the efficiency and productivity of construction workers, in extreme cases, negatively impacts a worker's health [34]. To ensure a healthful work environment for construction workers that is free from hazardous materials, it is necessary to continually monitor the work environment to take proactive safety measures in protecting the health of workers [13, 34]. With the aid of WSDs, real-time data can be obtained on temperature, air quality, pressure, radiation, carbon monoxide, etc., and processed to determine if the work environment is safe for construction workers.

4.2.3 Proximity Sensing

Proximity sensors are used to detect the presence of an object within a specified range without contact with the object. Proximity sensing aims to warn workers through sound or vibration signals of the presence of an object by identifying the location of the worker relative to the potential danger, mostly heavy construction equipment that could lead to injury or fatality [1]. Motion data (e.g., velocity, acceleration, etc.) and location data (e.g., position, orientation or direction, etc.) can be captured using sensors and technology systems such as radio-frequency identification (RFID), Global positioning systems (GPS), accelerometer, gyroscope, and magnetic field generators [13].

4.2.4 Location Tracking

Dependable and timely information regarding the location of equipment, materials, and workers can assist the management in making the best decision based on current conditions. Tracking technology has been used to discover undetected barriers in blind spots, as well as in worker tracking to manage aspects related to human error like hazard identification. Location data such as position and orientation or direction data can be tracked using technologies including GPS, RFID, and Ultra-wideband (UWB) which have been demonstrated to be useful for precise coordinate location [8].

4.3 Data Privacy and Security Regulations

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that protects sensitive health information from being disclosed without the owner's consent or knowledge [38]. Health data regulations under HIPAA are classified into two categories—privacy rules and security rules. The privacy rule generally aims to protect individuals' identifiable information while the security rule is made up of four major safeguards/standards for managing health data. The four major safeguards include administrative safeguards, physical safeguards, policies and procedures, and organizational safeguards. These four standards are administrative actions and policies expected by HIPAA of any health data collecting entity to prevent, contain, and correct security violations. However, health data collecting entities under HIPAA regulation are permitted to disclose personal identifiable information (PII) without the consent of the individual when needed by the individual, for the public interest, treatment, and healthcare purposes. Other health data regulatory agencies include Health Information Technology for Economic and Clinical Health (HITECH), the International Organization for Standardization (ISO), and the National Institutes of Standards and Technology (NIST).

4.4 Legal Challenges of WIoT

The legal aspect of IoT presents another challenge to WIoT application according to practitioners. In the United States, there is no legal provision for data storage duration, creating a crime-enabling environment for the service providers [35]. The lack of agreement amongst different countries on the regulation of IoT security presents the possibility of breaking the law as different data for the same purpose could be processed in different areas with different legislations and trying to reconcile the various laws could increase the complexity of the process. This lack of common law for IoT infrastructure could be attributed to the rapid development of IoT technology as legal bodies responsible for the regulation struggle to meet up with the legal problems of IoT technology [35, 36, 37]. According to Losavio *et al.* (2018), data complexity, diversity and heterogeneity, size and validation, visualization, and identity management all pose challenges to the grasp of these rising data masses, as well as how legal rules map to technical execution.

5 Conclusion and Further Research

This study presents an inquiry into privacy and security in the use of WIoT for construction safety and health monitoring. WIoT has proven to be effective in other industries like healthcare and

sports/fitness. It is currently being adapted to the construction industry to improve safety and health monitoring. This study evaluated the different layers that make up the architecture of WIoT as well as the security challenges associated with it. These security attacks as presented in this study could lead to data leakage, unauthorized access, authentication problem, and system hijack, which could all compromise the integrity of the collected and stored data. The study also identified the need for global legislation for data management to reduce the complexities in the use of WIoT beyond a local region. The different categories of construction safety and health data based on WIoT functions are also presented in the study together with a review of the privacy and safety regulations guiding the collection and processing of the data. To enhance the use of WIoT in the construction industry, there is a need to address the various security and legal challenges identified in this study, and also ensure that the outlined security requirements for WIoT architecture are met in line with appropriate regulations. This study is limited to the application of WIoT in the construction industry. The information from this study is expected to assist in developing an effective privacy and security framework to strengthen the adoption and implementation of IoT-based WSDs for construction safety and health monitoring. Further research on the perception of construction practitioners on the impact of privacy and security on the adoption of WIoT will help in identifying and addressing some privacy concerns that deter construction workers from WIoT acceptance.

6 References

[1] Kanan R, Elhassan O and Bensalem R 2018 An IoT-based autonomous system for workers' safety in construction sites with real-time alarming, monitoring, and positioning strategies. *Automation in Construction*, **88**, 73–86. https://doi.org/10.1016/j.autcon.2017.12.033

[2] Occupational Safety and Health Administration (OSHA) 2021 Commonly Used Statistics, United States Department of Labor. https://www.osha.gov/data/commonstats

[3] Bureau of Labor Statistics (BLS) 2021 National Census of Fatal Occupational Injuries in 2020. *U.S. Bureau of Labor Statistics, U.S. Department of Labor,* https://www.bls.gov/news.release/pdf/cfoi.pdf

[4] Park J, Kim K and Cho Y K 2017 Framework of automated construction safety monitoring using cloud-enabled BIM and BLE mobile tracking sensors. *Journal of Construction Engineering and Management*, **143(2)** 05016019. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001223

[5] Haghi M, Thurow K and Stoll R 2017 Wearable devices in medical internet of things: scientific research and commercially available devices. *Healthcare informatics research* **23(1)**, 4-15

[6] Choi B, Hwang S and Lee, S 2017 What drives construction workers' acceptance of wearable technologies in the workplace?: Indoor localization and wearable health devices for occupational safety and health. *Automation in Construction*, **84**, 31–41. https://doi.org/10.1016/j.autcon.2017.08.005

[7] Ahn, C R, Lee S, Sun C, Jebelli H, Yang K and Choi B 2019 Wearable sensing technology applications in construction safety and health. *Journal of Construction Engineering and Management*, **145(11)**, 03119007. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001708

[8] Awolusi I, Marks E and Hallowell M 2018 Wearable technology for personalized construction safety monitoring and trending: Review of applicable devices. *Automation in Construction*, **85**, 96–106. https://doi.org/10.1016/j.autcon.2017.10.010

[9] Gong Y, Fang Y and Guo Y 2016 Private data analytics on biomedical sensing data via distributed computation. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, **13(3)**, 431–444. http://dx.doi.org/10.1109/TCBB.2016.2515610

[10] Hiremath S, Yang G and Mankodiya K 2014 Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare. *2014 4th International*

Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), 304–307.

[11] Kumari P, López-Benítez M, Lee G M, Kim T S and Minhas A S 2017 Wearable Internet of Things—from human activity tracking to clinical integration. *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2361–2364. https://doi.org/10.1109/EMBC.2017.8037330

[12] Kumari K, Jadliwala M, Maiti A and Manshaei M H 2019 Analyzing defence strategies against mobile information leakages. *Decision and Game Theory for Security - 10th International Conference, GameSec 2019, Proceedings*, 276–296.

[13] Awolusi I, Nnaji C, Marks E and Hallowell M 2019 Enhancing construction safety monitoring through the application of Internet of Things and wearable sensing devices: A review. 530–538. https://doi.org/10.1061/9780784482438.067

[14] Kotz D, Gunter C A, Kumar S and Weiner J P 2016 Privacy and security in mobile health: A research agenda. *Computer*, **49(6)**, 22–30. https://doi.org/10.1109/MC.2016.185

[15] Awolusi I, Nnaji C and Okpala I 2020 Success factors for the implementation of wearable sensing devices for safety and health monitoring in construction. 1213–1222. https://doi.org/10.1061/9780784482865.128

[16] Nnaji C, Okpala I and Awolusi I 2020 Wearable sensing devices. *Professional Safety*, **65(4)**, 16–24.

[17] Okpala I, Parajuli A, Nnaji C and Awolusi I 2020 Assessing the feasibility of integrating the Internet of Things into safety management systems: A Focus on Wearable Sensing Devices. 236–245. https://doi.org/10.1061/9780784482865.026

[18] Yugha R and Chithra S 2020 A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*, **169**, 102763. https://doi.org/10.1016/j.jnca.2020.102763

[19] Farooq M, Waseem M, Mazhar S, Khairi A and Kamal T 2015 A Review on Internet of Things (IoT). *International Journal of Computer Applications*, **113**, 1–7. https://doi.org/10.5120/19787-1571

[20] Trappey A J C, Trappey C V, Hareesh , G U, Chuang A C and Sun J J 2017 A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0. *Advanced Engineering Informatics*, **33**, 208–229. https://doi.org/10.1016/j.aei.2016.11.007

[21] Evans D 2021 The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper,* **1(2011)**, 1-11.

[22] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M and Ayyash M 2015 Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, **17(4),** 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[23] Bhosale H and Gadekar D 2014 A review paper on big data and hadoop. *International Journal of Scientific and Research Publications*, **4(10)**, 1–7.

[24] UNCTA 2021 *Data Protection and Privacy Legislation Worldwide | UNCTAD*. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[25] Wang Y, Attebury G and Ramamurthy B 2006 A survey of security issues in wireless sensor networks. *IEEE Communications Surveys Tutorials*, **8(2)**, 2–23. https://doi.org/10.1109/COMST.2006.315852

[26] HaddadPajouh H, Dehghantanha A M, Parizi R, Aledhari M and Karimipour H 2021 A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, **14**, 100129. https://doi.org/10.1016/j.iot.2019.100129

[27] Hathaliya J J and Tanwar S 2020 An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, **153**, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

[28] Agrawal, P, and Narayanan, P J 2011 Person de-identification in videos. *IEEE Transactions on Circuits and Systems for Video Technology*, **21(3)**, 299–310. https://doi.org/10.1109/TCSVT.2011.2105551
[29] Hajar M S, Al-Kadri M O and Kalutarage H K 2021 A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Computers & Security*, **104**, 102211. https://doi.org/10.1016/j.cose.2021.102211
[30] Nath N D, Chaspari T and Behzadan A H 2018 Automated ergonomic risk monitoring using body-mounted sensors and machine learning. *Advanced Engineering Informatics*, **38**, 514–526. https://doi.org/10.1016/j.aei.2018.08.020
[31] Sherafat B, Ahn C R, Akhavian R, Behzadan A H, Golparvar-Fard M, Kim H, Lee Y C, Rashidi A and Azar E R 2020 Automated methods for activity recognition of construction workers and equipment: State-of-the-Art review. *Journal of Construction Engineering and Management*, **146(6)**, 03120002. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001843
[32] Shen X, Awolusi I and Marks E 2017 Construction equipment operator physiological data assessment and tracking. *Practice Periodical on Structural Design and Construction*, **22(4)**, 04017006.
[33] Haahr R G, Duun S B, Toft M H, Belhage B, Larsen J, Birkelund K and Thomsen E V 2012 An electronic patch for wearable health monitoring by reflectance pulse oximetry. *IEEE Transactions on Biomedical Circuits and Systems*, **6(1)**, 45–53. https://doi.org/10.1109/TBCAS.2011.2164247
[34] Kiani A, Salman A and Riaz Z 2014 Real-time environmental monitoring, visualization, and notification system for construction H&S management. *Journal of Information Technology in Construction*, **19**, 72–91.
[35] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E and Markakis E K 2020 A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open Issues. *IEEE Communications Surveys Tutorials*, **22(2)**, 1191–1221. https://doi.org/10.1109/COMST.2019.2962586
[36] Losavio M M, Chow K P, Koltay A and James J 2018 The Internet of Things and the smart city: Legal challenges with digital forensics, privacy, and security. *Security and Privacy*, **1(3)**, e23. https://doi.org/10.1002/spy2.23
[37] Okpala I, Nnaji C and Awolusi I 2019 Emerging construction technologies: State of standard and regulation implementation. *Computing in civil engineering 2019: Data, sensing, and analytics* (pp. 153-161). Reston, VA: American Society of Civil Engineers.

[38] Health Information Technology (HIT) 2019 HPAA Basics Available from: https://www.healthit.gov/topic/privacy-security-and-hipaa/hipaa-basics

7 Acknowledgment

This project was funded by The University of Texas at San Antonio, Office of the Vice President for Research, Economic Development, and Knowledge Enterprise.