Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Sustainable Cities and Society 75 (2021) 103311

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions

Muhammad Adil [a,b], Muhammad Khurram Khan [c,*]

[a] Department of Computer Science, Virtual University of Pakistan, Lahore, Pakistan
[b] Department of Electrical Engineering and Computer Science, Embry Riddle Aeronautical University, Florida, USA.
[c] Center of Excellence in Information Assurance, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

ARTICLE INFO

Keywords:
Emerging IoT applications for COVID-19
Sustainable smart cities
Network architecture security
Security and data preservation challenges

ABSTRACT

COVID-19 is a global infectious disease that can be easily spread by the contiguity of infected people. To prevent from COVID-19 and reduce its impact in sustainable smart cities, the global research communities are working relentlessly by harnessing the emerging technologies to develop the safest diagnosis, evaluation, and treatment procedures, and Internet of Things (IoT) is one of the pioneers among them. IoT can perform a pivotal role to diminish its immense contagious rate by suitable utilization in emerging healthcare IoT applications in sustainable smart cities. Therefore, the focus of this paper is to outline a survey of the emerging healthcare IoT applications practiced in the perspective of COVID-19 pandemic in terms of network architecture security, trustworthiness, authentication, and data preservation followed by identifying existing challenges to set the future research directions. The salient contributions of this work deal with the accomplishment of a detailed and comprehensive literature review of COVID-19 starting from 2019 through 2021 in the context of emerging healthcare IoT technology. In addition, we extend the correlated contributions of this work by highlighting the weak aspects of the existing emerging healthcare IoT applications, security of different network layers and secure communication environment followed by some associated requirements to address these challenges. Moreover, we also identify future research directions in sustainable smart cities for emerging healthcare IoT utilization in the context of COVID-19 with the most productive results and least network implementation costs.

1. Introduction

In the medical sector, the use of the Internet of Things (IoT) has shown an exponential increase in the last decade as they have been used in various healthcare applications to gather, store, process, and transmit data in the networks (Castiglione et al., 2021). In the context of healthcare applications deployment, IoT can strategically enhance the accessibility of patient assessment, disease detection, and treatment accompanied by improved patient experience with lower cost at their doorstep (Hossain, 2015; Sun et al., 2019). The pandemic of COVID-19 has made a massive impact on the global healthcare sectors by introducing new challenges, which can affect the overall healthcare assurance systems by calling additional requirements to follow the patient timeliness of assessment, prescription, and healthcare guidelines (Mbunge, 2020; Otoom et al., 2020; Vedaei et al., 2020).

In the prevailing situation, IoT is expected to play a significant role in the healthcare sector by collecting, processing, and analyzing the key symptoms of COVID-19 patients (Qadri et al., 2020). However, the extensive use of IoT devices in the healthcare sector requires special needs, because the collected data of these devices contain sensitive information related to patients. Therefore, the leakage of patients' private information will cause serious problems to the healthcare industry followed by the patient's trust of willingness to use this emerging technology in their health-related problems (Alam et al., 2018; Farahani et al., 2018). Beside that, network architecture, efficient data collection, new protocols, and security techniques deployment with proper load distribution among the participating network components are major obstacles in IoT applications specifically in healthcare (Balaji et al., 2019; Joyia et al., 2017; Pang, 2013; Rath, 2020). In the context of COVID-19, IoT applications need fast real-time data processing with accurate decision-making processes to increase the fertility of their deployed applications (Ahmed et al., 2020; Mohammed et al., 2020b). However, most of the existing IoT applications in healthcare store data in a centralized location, which increases their sensitivity in terms of

* Corresponding author.
E-mail addresses: muhammad.adil@ieee.org (M. Adil), mkhurram@ksu.edu.sa (M.K. Khan).

https://doi.org/10.1016/j.scs.2021.103311
Received 13 June 2021; Received in revised form 1 August 2021; Accepted 26 August 2021
Available online 11 September 2021

Table 1
Physical layer attacks with preventive techniques.

Hardware/Physical Attacks	Relevant references with proper description of authentication schemes
Hardware Trojan Attacks	Mohammed et al. Mohammed et al. (2020a), proposed a hybrid scheme of power profiling (PP) and network traffic (NT) to address the Hardware Trojan Attacks (HTA) in HC-IoT networks. References Chen et al. (2019); Dong et al. (2019); Venugopalan and Patterson (2018); Venugopalan et al. (2016), present a multi-layer hardware Trojan authentication architecture for IoT devices to guarantee their validity in the network. In Bahaa et al. (2021); Dey et al. (2021); Malaj and Marinova (2020); Wang (2014); Yang et al. (2016), a thorough overview of the HTA is given, which identifies and categorizes current responses to hardware security provocations in order to guide potential analysis.
Hardware Trojan Insertion Attacks	References Wang (2014); Xiao et al. (2016); Yang et al. (2016), addresses numerous Hardware Trojan injection phases of IoT devices during their circuit architecture life-cycle that are detrimental to operating networks.
Side-Channel Attacks	Side-Channel Attacks (SCA) are anti hardware attacks, where the attacker uses criminological techniques correlated to the system application to accumulate genuine data from the deployed network Xiao et al. (2016). References Ahmed et al. (2018); Lo'ai and Somani (2016); Marques et al. (2019), introduces the concept of Side-Channel Attacks in HC-IoT applications to design a secure transmission infrastructure and encryption algorithms.
Hardware Trojan Based Side-Channel Attacks	Ender et al. Ender et al. (2017), presented a framework that reveals how quickly sneaky Trojan hardware can be adopted as an SCA in hardware, which will insert a malicious code in the network to activate SAC. In Ghandali et al. (2020), the writer introduced astonishingly discreet Trojan hardware through cryptographical primitives with established SCA countermeasures. The spiteful design, once activated, demonstrates a useful side-channel leakage leading to powerful SCA.

data dependency on a centralized point, and the relaying point of failure can cause enormous destruction to the system (Singh et al., 2020). Beside that, the number of IoT devices increased in the healthcare applications, after the evolution of COVID-19 to generate a huge amount of data, which pressures the deployed healthcare IoT network in terms of communication metrics e.g. delay, throughput, computation complexity accompanied by an erroneous diagnosis that could harmfully influence the COVID-19 disclosure and service response rate (Gupta et al., 2021).

To resolve the centralized point of management issue in the healthcare IoT network and produce more reliable services in the COVID-19 pandemic, the present centralized point of management such as cloud network architecture needed to be improved (Wu, 2020). Currently, healthcare IoT applications face challenges in the context of network architecture, protocol deployment, and application specifications. After, COVID-19 pandemic, the importance of healthcare IoT networks is much more increased with defined specifications, which open new research areas by highlighting flaws in the aforestated network metrics.

In this paper, we present a thorough outline of the existing literature of the healthcare IoT applications used for COVID-19 in terms of network structure security and data integrity. In the initial part of the paper, we discuss the disruption of COVID-19 throughout the world in the recent past. Furthermore, we extend our study to the applications of IoT in healthcare specifically used for COVID-19 diagnosis, assessment, and prescription, etc. The correlated part of this discussion will evaluate the role of different parts of the network security e.g Transmission Control Protocol (TCP) security and data preservation with different vulnerabilities threats to highlight the existing challenges and set the stage for new effective research in this sector.

Thus, the key contributions of this paper can be summarized as below:

1. First, we will go through the COVID-19 epidemic disruption supported by a thorough study of IoT applications used in the healthcare domain for COVID-19 diagnosis, treatment, assessment, and prescription. Next, we will extend our discussion to different security techniques to identify the associated challenges.
2. Section III overviews the present literature of IoT applications that how rapidly this technology has been evolved in the sustainable smart cities healthcare sector over the last few years to acknowledge the importance of this systematic survey.
3. The utmost contribution of this work is to overview the existing adopted applications of emerging healthcare IoT in the sustainable smart cities in terms of network architecture security, data preservation, network maintenance, traffic management, protocols implementations, etc, from 2019-2021.

   Furthermore, we identify the existing literature's pros and cons with each aspect to classify their requirements with the most prevailing challenges.
4. Finally, we elaborate on the flaws of existing emerging healthcare IoT applications in sustainable smart cities to suggest possible solutions with future research directions. However, the uniqueness of this survey paper from the existing papers is that it covers most of the network structure and data preservation security threats to observe and identify diverse research possibilities in the emerging healthcare IoT sector in the sustainable smart cities from the perspective of the COVID-19 pandemic. Tables 3 and 4, illustrates the comparative investigation of this work with existing survey papers to ensure its contribution.

The remainder of the paper is organized as follows: Section II of the paper estimates the agitation of the COVID-19, which acknowledges the importance of this work in terms of technology utilization. Section III contains the comprehensive analysis of IoT applications in healthcare specifically used in the context of COVID-19. Section IV observes and identifies the existing required challenges in the present literature, while Section V sets the future research directions in the presence of existing literature flaws. Consequently, Section VI compiles and summarizes the paper.

2. COVID-19 Destruction Evaluation

COVID-19 outbreak seems to be on a path to destruction with devastating global instability followed by the catastrophic ability to change geopolitical and socioeconomic norms. In order to manage the COVID-19 destructive situation, many nations are aggressively undertaking significant financial reforms for the rehabilitation programs to restore the industry sector, business, healthcare, and specifically ground level people (Duong et al., 2020; Golan et al., 2020; Xu et al., 2020). Coronavirus has provoked a drastic and unpredictable transition to the socioeconomic norms since it was first identified in late 2019 (Guan et al., 2020). COVID-19 has catastrophic and far-reaching offshoots on the healthcare systems, countries, businesses, and individual lifestyles throughout the globe. Indeed, no one was prepared for the devastating influence of the COVID-19 outbreak, ranging from companies to an individual lifespan.The destruction of the COVID-19 pandemic was enormous, therefore, the global focus on the virus's widespread mitigation response by suggesting hygienic methodologies, social distancing, quarantine, and lockdown, etc.

However, the pandemic affects each region and corner of the world by infecting people or taking their lives. Besides that, the main focus of this paper is on the existing IoT applications used in connection with COVID-19 as an emerging technology to prevent its spread. Before diving into the IoT applications in COVID-19, first, we would like to have a quick review of the most affected countries of the world in terms

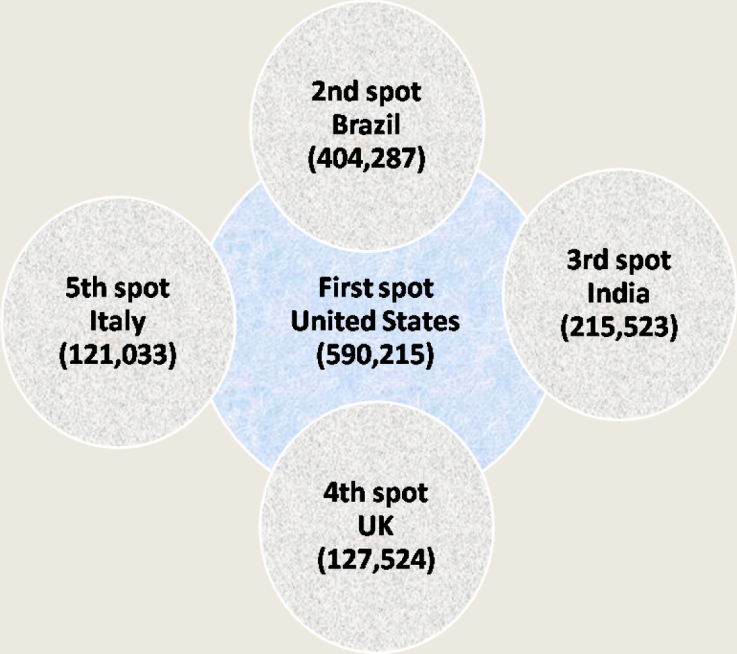

Fig. 1. COVID-19 death statistical analysis.

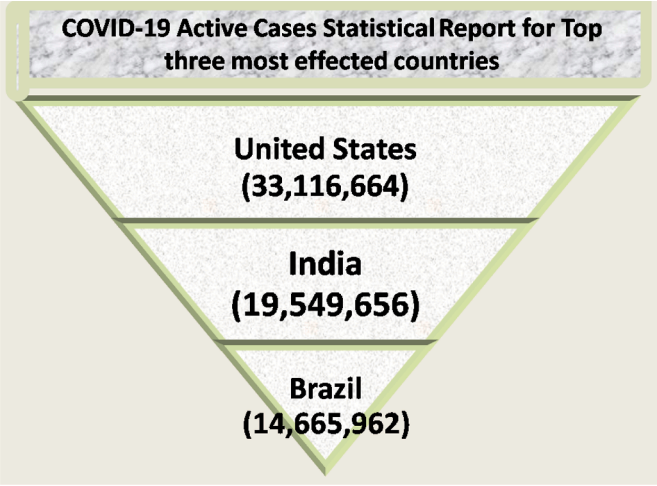

Fig. 2. COVID-19 active cases statistical analysis.

of deaths and active cases to increase the reader's interest in the proposed work followed by the acknowledgment of technology. We follow reference (b23, 2021) worldometer report date (1 May 2021) to share the updated information of the COVID-19 pandemic about the top five most affected countries. Fig. 1, illustrates the list of the countries having the most death cases from COVID-19 pandemic.

Likewise, Fig. 2 of the paper demonstrates the top three countries having the largest number of active cases at the moment.

3. Secure Network Architecture and Authentication Approaches

Healthcare Internet of Things (HC-IoT) systems are made up of a range of modules, including sensors, cluster heads, controls, base stations, and humans such as patients, nurses, physicians, and pharmacists, etc. In the initial phase, we overview a general framework design for analyzing security vulnerabilities by assuming a high-level model of the HC-IoT network used for COVID-19 prevention, assessment, diagnostics, and prescription as an evolving technology. After that, we will utilize a model of defense in resilience, redundancy, and solidifying, to identify the possible threats faced by these networks from cyber-attackers taking into account the effect and probability (Rao and Haq, 2018).

Rahardja et al. (2020) discussed in their research article the main concerns related to security and privacy safeguards for COVID-19 patients while concurrently authenticating sensitive data in the network. The authors developed the COVID Test Certification (CTC) technology to assess and verify the rapid testing outcomes of testing people using a distributed network framework. Furthermore, the proposed model was helpful for the COVID-19 patients to protect their anonymity followed by their fitness after the COVID-19 infection in a secure way. Azrour et al. (2021), suggested an effective and reliable authentication model for remote HC-IoT that makes use of a centralized point such as the cloud to ensure the legitimacy of the patient's wearable devices. The limitation of the proposed model was the centralized point of authentication, which generates network overhead followed by specific applicability of this scheme in a homogeneous IoT network.

Reference Leaby et al. (2021) suggested a reliable cooperative authentication scheme of elliptic curve cryptography (ECC) and Hash Function for HC-IoT applications to overcome the security obstacle in emergency transportation in the context of the COVID-19 virus outbreak. In Masud et al. (2020), the authors suggested a lightweight secret key establishment protocol mutual authentication scheme for HC-IoT applications associated with COVID-19. The proposed model uses Physical Unclonable Functions (PUF) to ensure the network device's validation and authentication before creating a session key, to give access to doctors, patients, and staff. PUF often prevents patient wearable IoT devices from tampering, data copying, and side-channel attacks in an unattended communication atmosphere. Jung and Agulto (2021) suggested a Software-Defined Networking (SDN) interface to monitor and track the information of COVID-19 affected individuals, and provide real-time information disclosure services to the global Centers for Disease Control and Prevention (CDCs). Reference Alam (2020), offers a skeleton for patients with COVID-19 infectious disease, which identifies health infirmities, examinations, and prescriptions electronically. Patients are given access to smart IoT devices by mobile applications like Tawakkalna and Aarogya Setu, etc. Although these applications effectively monitor COVID-19 patients, but the data collected by these devices are communicated through these

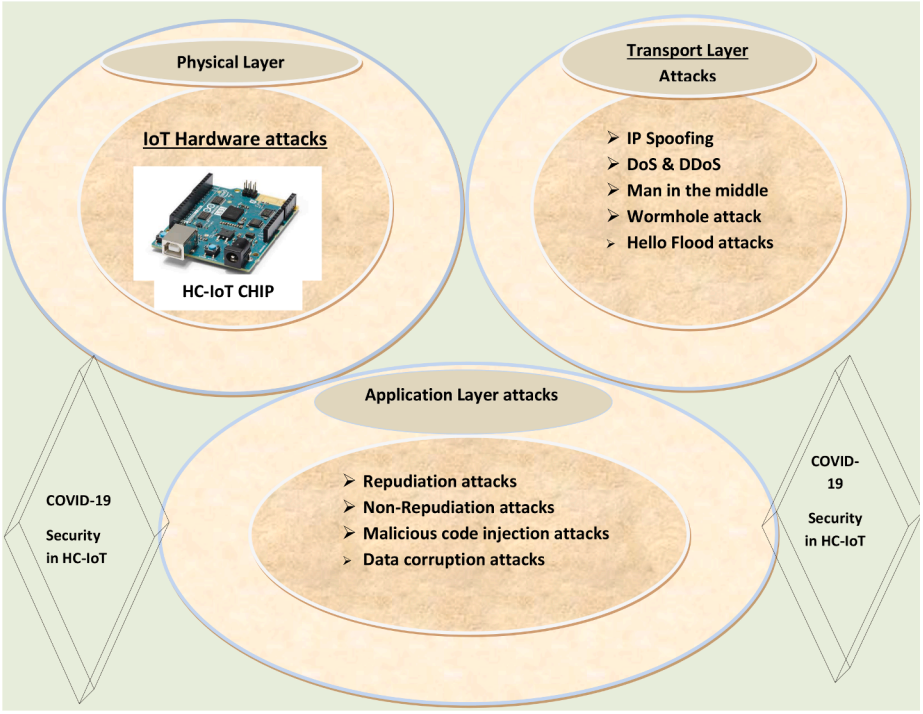

Fig. 3. Different layer security threats to HC-IoT applications.

applications, which makes them susceptible to internal and external attacks.

In Jan et al. (2021), the writers realized many vulnerability issues in the healthcare IoT applications, as a result of the rash usage of cloud services without proper safeguards in the disastrous COVID-19 scenario. Lucca et al. (2020) suggested a Privacy-preserving touch Tracing scheme leveraging 5G and Blockchain to maximize data protection in HC-IoT application used in the association with the COVID-19 pandemic. Beside that, 5G technology was used as a fundamental part of this system, to allow everyone to search the patient's whereabouts via their cell phones to ensure that whether someone has made contact with a patient diagnosed with coronavirus or not. Data preservation is still the foremost provocation associated with HC-IoT technologies since the usage of criteria of these applications, wearable devices, and functionalities expose them to a variety of risks. Reference (Lucca et al. (2020), presents a systematic literature review to establish a taxonomy of the HC-IoT application criteria to preserve patient privacy in the hospital during the COVID-19 pandemic. Security predicaments related to HC-IoT applications, IoT devices, communication environments, gadgets, and other network components such as the Transmission control protocol (TCP) stack are thoroughly addressed in reference Tyagi (2021).

In Mahajan and Zafar (2021), the authors demonstrated the impact of DDoS attacks during the transmission of data in the network to effectively combat COVID-19. In this analysis, the author compares the efficiency of adaptive hybrid routing protocols for throughput and quality of service (QoS) in the presence and absence of DDoS. References (Adil, 2021; Adil et al., 2021; Manavi et al., 2020; Sharma et al., 2020) discuss the security issues associated with different applications of IoT-powered technologies used in COVID-19 scanning, touch tracking, and surveillance. In Li et al. (2021), the authors provided a thorough overview of the H-IoT applications leveraging machine learning (ML) strategies for large data analysis. Beside that, they also highlighted the strengths and shortcomings of the existing approaches with numerous analyses to illustrate and provide healthcare professionals, government, and relevant organizations an insight into the current developments in ML algorithms for big data analytics in smart healthcare.

Khan et al. (2021a) present a comprehensive survey on the utilization of modern technologies in the COVID-19 pandemic such as artificial intelligence (AI), machine learning (ML), blockchain, cloud, and edge computing. Moreover, they highlighted the existing challenges in these innovative technologies to set a footprint for effective utilization of them followed by concrete future research direction. Consequently, reference (Abir et al., 2020) investigates the use of emerging technologies such as HC-IoT in the sense of COVID-19 by proposing a privacy-first comprehensive paradigm for integrating digital transformation technologies. In addition, this paper thoroughly addresses the advantages and disadvantages of data sources, tools, users, patients, staff, and applications used for coronavirus detection, treatment, and prevention.

Figure 3, summarises the current research to highlight the limitation of each adopted technique to set the road map for new research.

3.1. HC-IoT Physical Layer security

Physical layer or Hardware attacks pretend severe intimidation to H-IoT devices because these types of attacks can either decrease security level or even cancel the security level of legitimate H-IoT devices, due to open area implementation and easy accessibility (Kazemi et al., 2018). Beside that, the physical layer security of the HC-IoT network necessitates particular deliberation, since these devices are subject to a variety of stipulations that must be overcome during the deployment phase i.e. reliable operation, quick access to the patient, low latency, and data preservation followed least implementation costs (Dofe et al., 2016; Kazemi et al., 2019). As a result, high security on board is critical to meeting the above requirements during the construction process of HC-IoT devices. In practice, implanted device architects persist unfamiliar with hardware security standards. Therefore, hardware security professionals are not always capable of designing the whole system by themselves, as this will significantly raise construction costs (Stellios et al., 2018). Indeed, these problems also acknowledge the HC-IoT devices vendors to inspect the security issues, which may have significant implications for the patients, doctors, and staff privacy, etc. Thus, to build a secure HC-IoT networking infrastructure, hardware-level security and threats must be evaluated.

Table 2
Network layer attacks with preventive techniques.

Netework Layer Attacks	Relevant refereneces with proper description of authentication schemes
IP Spoofing Attacks	In reference (Vijayakumar et al., 2020), K-means clustering and Support Vector Machine are used in tandem to overcome the data privacy and authentication problems in H-IoT applications. NAT+ paradigm was suggested by Veeraraghavan et al. Veeraraghavan et al. (2020) to address the IP Spoofing problem in H-IoT applications. In Chen et al. (2020); Khan et al. (2021b); Rohatgi and Goyal (2020); Singh and Pandey (2020), IP spoofing attacks and their fundamental causes in H-IoT applications are thoroughly studied as a key security hazard in cloud computing to draw the concentration of consumers and designers toward this domain.
Hello Flood attacks	Detection, Prevention Low Power and Lossy Network (DPLPLN) authentication technique was presented in Gajbhiye et al. (2020) to develop a secure IoT communication architecture. To assure network traffic validation, the DPLPLN provides security by recognizing the flooding operation or garbage of packets of Denial of Service (DoS) attacks.
Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks	In Hussain et al. (2021); Kamble and Gawade (2020); Khatkar et al. (2020), the writers explore the weak aspect of the H-IoT security to leak integrity, authenticity, availability, and confidentiality of accumulated data in the network. They also present a pinpoints study paradigm, which is helpful for further research to develop new methodologies for discovering and anticipating DDoS and DoS attacks at the network layer. Hussain et al. Hussain et al. (2020), used the ResNet framework to convert the network legitimate traffic into image format and trained the Cable News Network (CNN) to evaluate the proposed model and avoid DoS & DDoS attacks.
Wormhole & Blackhole Attacks	Reference Kaliyaperumal et al. (2020), introduced a Hybrid Rabin Public Key Signature Algorithm for H-IoT applications to overcome wormhole and black hole attacks. In Adil et al. (2020); Ambarkar and Shekokar (2020); Kame and Elhamayed (2020), the authors suggested reliable authentication schemes for H-IoT applications to address wormhole, black hole, and sinkhole attacks.

Table 3
Application layer attacks with preventive techniques.

Hardware/Physical Attacks	Relevant refereneces with proper description of authentication schemes
Non-repudiation Attacks	Reference Kremer et al. (2002), demonstrate the existing classical non-repudiation authentication procedures by highlighting that most of them are befalling within the class of a trusted third party (TTP) authentication model, which is comprehensively discussed in references Coffey et al. (2003); Yaga et al. (2018). Classical non-repudiation security explications are maturing and antiquated in the H-IoT application employed in connections of COVID-19, due to the certification of trustworthiness and third-party interruption in the network. In this context, blockchain-based authentication played a major role to address the possible malicious attacks on H-IoT deployed networks. To address the non-repudiation security threat in H-IoT application, the on-chain and off-chain channels scheme was suggested in reference Xu et al. (2019).
Repudiation Attacks	Reference Awan et al. (2020), suggested a NeuroTrust mutual authentication model that leverages trust parameters to assure dependability, adaptability, and packet authenticity with low network cost to detect rogue devices in the H-IoT network. In Ahanger and Aljumah (2018); Algarni (2019); Sahi et al. (2017), the writers give a thorough sketch of the security and privacy predicaments that must be addressed for the prosperous implementation of H-IoT applications on a viable large scale. Despite that, they also examined the security interests amalgamated with H-IoT applications by analyzing the present literature to get an insight into these security obligations.
Malicious code injection attacks	Reference Ahmed and Ullah (2017), presents the false data injection attack (FDIA) solution by launching an awareness campaign followed by some cryptographic techniques to prevent the foretasted attacks in the healthcare domain. In Aggarwal et al. (2021), the author designs a three-layered blockchain-based Unmanned Aerial Vehicles (UAV) approach to enable privacy protection in the H-IoT applications. The recommended model offers a distributed policies for UAVs that assures the integrity and confidentiality of data during transmission of H-IoT applications from one site to another practicing the proof of work (PoW) consensus technique.
Data corruption attacks	In Alazeb and Panda (2019), the authors present two model-based data preservation scheme for the H-IoT applications by utilizing separate fog modules for heterogeneous, and homogeneous data respectively to assure the legitimacy of transmitted data. The current literature in Abouzakhar et al. (2017); Chaudhry et al. (2021); Roy et al. (2018) fully describes data corruption removal strategies.

The physical layer or hardware attacks and preventive techniques discussed in the literature are summarized in Table 1, with relevant references.

3.2. Network Layer Attacks

Secure communications of the smart healthcare network ameliorate the potency of these applications by getting the trust of patients, treating staff, and pharmacists. In this case, the writers of reference Granjal et al. (2014) assess the use of contemporary condensed security parameters for protocol stack in the scope of smart HC-IoT applications. In Yang and Yang (2021), an applied strategy of immunology analysis, numerical experiment technology, and complex adaptive system theory was proposed to overcome the network layer security dilemma utilizing an artificial privileged system. References Baker et al. (2017); HaddadPajouh et al. (2020a); Somasundaram and Thirugnanam (2020), comprehensively outline the security challenges associated with the HC-IoT network layer to set the expected investigation direction. The declining efficacy of H-IoT services has resulted from data preservation, security, and privacy challenges, which have a negative influence on individuals' sensitive health data. As a result, we broaden our research to include a review of individual network-layer authentication algorithms in the H-IoT area in table 2.

3.3. Application Layer Security in H-IoT

The determination of decent application layer protocols can overwhelm some security provocations and be influential in the secure transmission of low-power lossy networks (LLNs) such as H-IoT networks employed in the circumstances of COVID-19. Despite that, various application-layer protocols had been used in the literature to ensure data preservation in these LLNs with peculiar validation of patient embedded devices (Bhattacharjya et al., 2020; Ghotbou and Khansari, 2021). HaddadPajouh et al. (2020b), introduced AI4SAFE-IoT for secure communication and transmission for H-IoT application layer infrastructure. To defend H-IoT infrastructure, this scheme was constructed in coordination with an artificial intelligence-powered security module to combat cyber threat attribution, threat hunting, and web application firewall, etc. Bansal et al. Bansal (2020), examine and assess numerous

Table 4
Security challenges in the existing literature comparative analysis with our paper.

Scheme name	Authentication Challenges	CIA Challenges	Authorization Challenges	Connectivity Challenges	Interoperability Challenges	Privacy Challenges	Security Challenges
Abir et al. (2020)	Yes	Partial	Yes	No	No	Yes	Yes
Ahmed et al. (2018)	Yes	Yes	No	No	Yes	No	Yes
Marques et al. (2019)	No	Partial	Yes	No	No	Yes	Yes
Somasundaram and Thirugnanam (2020)	Yes	Yes	Yes	No	No	Yes	Yes
Baker et al. (2017)	No	No	Yes	Yes	No	Yes	Yes
our scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes

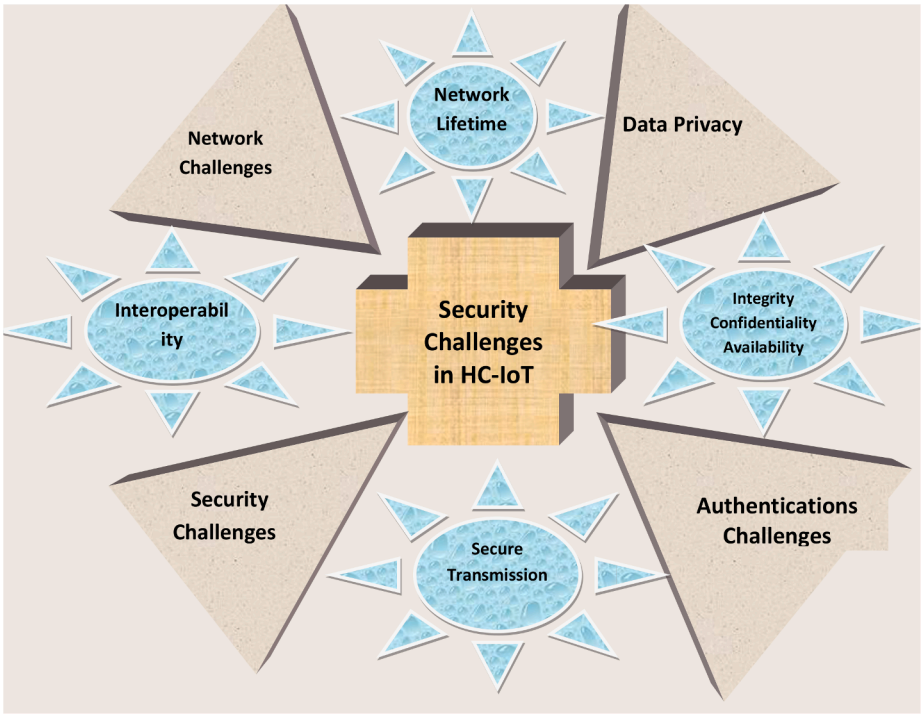

Fig. 4. Different Challenges associated with HC-IoT applications.

security-related application layer protocols in order to validate their durability metrics.

Swamy et al. (2017), overviewed the security intimidations, obligations, and provocations of the H-IoT application layer in their survey report to acknowledge the investigation community's endeavors to build countermeasures strategies to determine these concerns. Reference Coffey et al. (2003); Kremer et al. (2002); Tewari and Gupta (2020); Xu et al. (2019), investigates the cross-layer diverse integration challenges, security difficulties, to set the future research directions, and attempt to discover answers for these challenges. Table 3 of the article extensively assesses many factors that might agitate the application layer security of H-IoT in the circumstances of COVID-19.

4. Network and Security Challenges in H-IoT

H-IoT applications implemented in conjunction with COVID-19 may provide significant advantages to patients, physicians, and other important personnel. However, they do it by carrying certain issues in terms of network deployment, dependability, cybersecurity, and privacy issues, which are the key concerns of customers and healthcare providers. These are creating a significant provocation for the H-IoT applications due to common high-profile cybersecurity assaults. The interconnectedness of patient implanted IoT devices is the source of this risk, because of the wireless communication and open area deployment, which necessitates unique data preservation and security solutions for these networks (Ahad et al., 2019). All of those arguments have a substantial impact on the protection and privacy of H-IoT applications and may result in large losses of data. Fig. 4, of the paper, illuminates the several provocations affiliated with H-IoT applications used in the circumstances of COVID-19.

4.1. Security Challenges in H-IoT

H-IoT applications are comprised of an extensive range of similar or approximately alike devices that yield similar characteristics to collect and process data in the network. Although many healthcare foundations have developed risk assessment guidelines to guarantee data preservation, where numerous H-IoT devices may automatically establish secure connections with other devices to exchange data erratically. Despite the fact that the problem of security in the information technology (IT) industry is not new, the adoption of H-IoT devices has posed an unprecedented culmination, which needs to be addressed at utmost priority to maintain the trust of clients and the healthcare enterprise (Zeadally et al., 2019a). Poorly secured H-IoT devices are one of the most influential channels for cybercriminals to disclose client's data via communication streams that are not effectively secured.

The open operation and interconnected nature of H-IoT devices expose them to multiple security threats, due to an inadequately protected environment, where an attacker can easily compromise the security and resilience of these networks. In addition, the nature and deployment of the H-IoT application acknowledge their challenges in terms of widespread use in an open area, wearable or move-able environment. Aside from the capacity of certain H-IoT gadgets that are mechanically interconnected with other devices in the network, which exhibit that H-IoT clients, enterprises, and developers have alike responsibility to guarantee the security of these networks. As a result, a collaborative strategy is needed to be revealed, which can be an efficient and pleasant answer for those problems that have been identified in the literature.

4.2. Privacy Challenges

The benefit of H-IoT applications can be determined by how effectively these applications can admire the privacy preferences of patients, staff, and even the enterprises. Concerns regarding the privacy issues with possible threats that are associated with H-IoT applications may be key factors to delay the impeccable approval of these applications in any healthcare organization (Mahmoud et al., 2021). Therefore, it is decisive to recognize the privacy rights of clients and staff, because they play a very significant role to maintain patients, staff, and enterprise trust and confidence in the H-IoT network. In this context, the literature demonstrates a lot of efforts of the researcher, which had been done to guarantee the privacy of patient embedded IoT devices to gain the trust of all enterprises, clients, and staff.

In ubiquitous intelligence with integrated artifacts, the sampling process and information dissemination in the H-IoT applications may be done practically everywhere, but privacy is the main problem. Apart from this, the omnipresent accessibility of these devices through the Internet is also an important aspect in comprehending this dilemma, because a novel system is needed to be put in place to obtain the personal information of patients from any location on the planet in a secure communication environment.

4.3. Interoperability Challenges

In the H-IoT applications, patient's values and data are perceived to be hampered by adversaries in an operational network. Despite that, complete interoperability between assigned tasks, services, and IoT devices suitability is not always possible, because patients may not like to share some secret data in the network, which may be a challenging task to manage with proper interoperability. Aside from this, inadequately originated or managed H-IoT devices may have a deleterious consequence on the resource-limited devices during data collection or communication in the network (Jabbar et al., 2017; Ullah et al., 2017).

4.4. Network Connectivity Challenges

H-IoT applications employed in the COVID-19 connection are made up of a family of IoT devices that could be only succeeded if they proffer connectivity to every IoT device participating in the network with the ability to sense, produce, and exchange essential data. In H-IoT, patients implanted or other relevant IoT devices may make an interface using any accessible communication network. However, ensuring connection in H-IoT applications utilized in COVID-19 pandemic has several issues, which includes:

1. Providing an extensive range of connectivity to the large number of IoT devices installed in the H-IoT network.
2. Ensure intradepartmental communication of patients embedded IoT devices.
3. Guarantee uninterrupted connectivity of highly mobile vehicles e.g. ambulances, for patient transport.

4.5. Confidentiality, Integrity and Availability Challenges

H-IoT is a platform of an interlinked patient implanted sensor devices, where each device has given a unique address for identification and authentication in the network. When a communication request is initiated among interlinked H-IoT gadgets, they must often verify each other in terms of authentication validity before providing private data. As a result, they generate the authentication, data integrity, and confidentiality problems in the H-IoT applications employed in the context of COVID-19 (Zeadally et al., 2019b). H-IoT networks consist of thousands of gadgets, which collect massive amounts of data from their deployed area and send it across the network with hop count communication to further processing, therefore, efficient availability and data access are particularly indispensable to the clients and enterprises in these networks (Karthigaiveni and Indrani, 2019). It involves data consumption privileges that might be assigned to various professionals in the context of big H-IoT applications employed in the consolidation of COVID-19. The efficiency and scheduling limits of access control in these networks or applications are a consequential provocation because the computational intensity of these applications is greater than that of the standard Database Management System (DBMS) (Dewangan et al., 2020). Therefore, this argument also necessitates noteworthy consciousness from the research community to compose reliable and computation fewer accessibility schemes for these networks.

4.6. Authentication and Authorization Challenges

Authentication and authorization entail allowing access permissions to the network resources to designated individuals according to their tasks. In the case of an H-IoT application, authentication, and authorization relating to a three-phase strategy, which guarantees the confidentiality and legitimacy of the patient's embedded devices. The very first step would have been to determine the security protocols that are nothing but a collection of detailed regulations, while the second phase is about the construction of the access control model and the final one is about the enforcement of these policies (Dhanvijay and Patil, 2019). The goals of authentication, authorization, and access control models are usually apparent, but they bring a lot of security challenges, which need to be regulated for interpretation in the authentication, authorization, and access control model (Safkhani et al., 2020). Despite that, one of the prime duties of authorization is to clarify the practice of interpretation and tie the canyon between high-level security and low-level regulations. Beside that, authorization principles might be used to assess the policies' completeness and coherence in the deployed H-IoT networks.

4.7. Discussion with comparative analysis

The issues identified in this paper are broad, and they are neatly linked to the security of H-IoT applications deployed in the context of COVID-19. To boost the efficiency of these applications while maintaining the confidence of customers and enterprises, the research community must pay close attention to the highlighted problems to devise cost-effective solutions for them. Although the literature comprises several review papers correlated to the security of H-IoT application, however, there no specific papers exist in the past study, which focuses on the security aspect of H-IoT application used in the connection of COVID-19. The reason for this, most of the existing technologies were extended to this specific domain with the crucial requirements of the coronavirus, which creates primary challenges for these networks. In this paper, we outline all the possible challenges associated with these applications and compare them with the existing survey paper to claim the uniqueness and contribution of this work.

4.8. Encryption Weaknesses Challenges

Cryptography contributes to strong privacy and security assurance in

H-IoT applications used in the connection of COVID-19 but they increase the computation and transmission costs. Despite that, patients' embedded IoT devices need plenty of processing energy to produce and disseminate authentication keys in the event of strong encryption and decryption, which will result in a huge rise in the network overhead (Alassaf and Gutub, 2019; Kavitha et al., 2019). Encryption systems might be jeopardized by discovering flaws in the numerical solution of cryptography, which may contribute to cipher violation and data leakage. The way to solve this concern may result in the rendering of public keys, which might be a solicitude since it intensifies the network's computation cost. As a result, when utilizing encryption in the H-IoT application used for COVID-19, the trade-off between privacy and computational complexity must be kept in mind initially.

5. Future Research Directions

IoT must be considered as a fundamental and practical architecture for improved H-IoT applications that could be used in conjunction with COVID-19. Although significant research efforts had been made to address various obstacles, which are still remained open further research such as usability, user interface, data access ubiquitous design, authentication, authorization, cryptography, data preservation, interoperability, QoS, network lifetime, and pervasive customized H-IoT network (Goyal et al., 2021). Presently, H-IoT is liable to gather a massive volume of personal data and transmit it over the Internet without any security assurance. As a result, various ethical and societal concerns might be made regarding openness to patient's personal data privacy. Therefore, it is a notable barrier in the H-IoT applications that are used in the context of the COVID, and demands a necessary redressal to avoid non-authorized interruption (Ray et al., 2019). Aside from this, pervasive monitoring deals with extremely sensitive data of patients, thus, it acknowledges that H-IoT applications must be deployed in a secure environment to ensure the trustworthiness of patient's data.

5.1. Edge architecture in H-IoT

In the future, the research community is suggested to extend their attention toward novel edge architecture that should be managed to fulfill the communication and security commitments associated with IoT applications used for COVID-19. While developing novel edge architecture, the following crucial aspect must be considered: patients embedded IoT devices and network components inside the edge platform must be configured to ensure validation, authentication, and secure communication with minimal network cost (Abbasi et al., 2021; Wang et al., 2021). In order to ensure the aforestated metrics, novel edge layered architecture could be extremely beneficial in the H-IoT application used in the COVID-19 context.

5.2. Cryptography with edge and fog computing

In the future, the importance of lightweight cryptographic authentication and hash authentication model can not be ignored, therefore, we also acknowledge the research community to utilize these types of authentication models in collaboration with edge and fog computing to address the communication and authentication problems in H-IoT applications (Mousavi et al., 2021). Furthermore, we also believe that lightweight authentication did not create network overhead, which is a positive sign for their utilization in healthcare.

5.3. Sensors and actuator Integration in H-IoT

Future H-IoT applications (COVID-19) are expected to include a variety of smart sensors and actuators for various functions. Therefore, centralized traffic administration or authentication models will not provide precise decisions for these devices in an integrated environment. Thus, the requirements for an Inter-integrated circuit (I2C) and Serial Peripheral Interface (SPI) are needed to be focused on the traditional method that might be used for improved edge services employing edge and fog computing (Toledo et al., 2021). Sensors that need an I2C interface with the system might be merged with actuators to make reliable communication infrastructure.

5.4. Dew Computing in H-IoT

Dew computing is indeed a relatively new addition to the current computing framework that addresses the super-user experience and internetwork autonomous technique to provide actual service to patients, doctors, and other relevant staff in the network's utilizing edge and fog computing (Manocha et al., 2021). In addition, the prime goal of dew computing is to explicate the abstract concepts of the cloud-dew drop interaction into the digital realm (Longo et al., 2019). Dew computing makes the applications more translucent and delay-sensitive by utilizing the dew computer, dew-cloud architecture, dew DNS (Domain Name System), etc. Therefore, we also encourage the research community to utilize Dew computing in the H-IoT application used in COVID-19 circumstances to improve their communication and security standards.

5.5. Blockchain based H-IoT

We admit the characteristics of blockchain technology to the research community, which could be used as another alternative redressal technology in the H-IoT domain in the future (Da Xu et al., 2021). It is a perpetual, persistent, and open consensus protocol-based technique, which is effective in the distributed and peer-to-peer communication without the provision of a centralized point of interest. As a result, the "Edge-Block" might be envisioned as a way to allow the current edge H-IoT applications to run autonomously and transparently while executing requests from decentralized patients, doctors, and staff, etc.

5.6. Machine Learning in H-IoT

Network and data security is an important topic that should be thoroughly investigated, particularly in terms of QoS and security. Because the H-IoT is designed in a homogeneous, heterogeneous, self-governing, and very adaptable environment, therefore, they are vulnerable to various cyber-attacks. To ensure the reliability of the network and integrity of the patients, doctors, and staff database, autonomous machine learning methods might be used to address these problems in the H-IoT applications (Cvitić et al., 2021; Majumdar et al., 2021). Thus, we urge the researcher to pay their obeisance to this valuable technology to resolve various H-IoT application problems cost-effectively.

5.7. Digital Twin in H-IoT

We want to elongate the concentration of researchers to a new kind of technology known as the Digital Twin, which is now gaining traction by means of reducing the process of data transfer between the local and distant cloud by offering a localized as well as a virtual duplicate of data encapsulation (Zhao et al., 2021). In the future, it is expected that H-IoT services may be outfitted with digital twin capabilities to provide efficient data dissemination with little network backhaul requirement, therefore, we also confirm the bright future of this technology and ask the researcher to pay attention to the utilization of digital twin in H-IoT and other relevant applications.

5.8. Unified network Integration framework

H-IoT technology's emergence progresses, which opens many research areas and platforms for the research community to devise new

Table 5
Future research direction comparative analysis with existing literature.

Description of future research direction	Abir et al. (2020)	Ahmed et al. (2018)	Marques et al. (2019)	Somasundaram and Thirugnanam (2020)	Baker et al. (2017)	our survey paper
Edge architecture in H-IoT	No	No	No	No	No	Yes
Cryptography with edge and fog computing	Yes	No	No	No	No	Yes
Sensors & actuator Integration in H-IoT	No	No	No	No	No	Yes
Dew Computing in H-IoT	No	No	No	No	No	Yes
Blockchain based H-IoT	Yes	Yes	Yes	Yes	Yes	Yes
Machine Learning in H-IoT	No	No	Yes	No	Yes	Yes
Digital Twin in H-IoT	No	No	No	No	No	Yes
Unified network Integration framework	No	No	Yes	No	No	Yes
Context aware accessibility	No	Yes	Yes	No	No	Yes

schemes. The evolution of this technology results in a quiescent scenario where patient's implanted IoT devices adhere that the other network IoT devices may be un-interoperable to the deployed IoT network (Chatterjee, 2021; Jiang et al., 2021). To resolve the interoperability concerns, a consistent framework for combining all of these concepts should be created for the deployed H-IoT network.

5.9. Context aware accessibility

Edge and Fog computing is intended to provide end-users such as patients, nursing staff, and doctors with relatively close services, it becomes imperative for the assistance provider to add and allow context-awareness features in the H-IoT applications (Kavitha and Ravikumar, 2021). Therefore, we also aspire to draw the researcher's attention toward context-aware features and accessibility with secure and reliable communication.

6. Conclusion

In this study, we have surveyed a detailed assessment of the deployment of emerging healthcare IoT applications in sustainable smart cities in the connection of COVID-19 to highlight the current impediments related to network architecture, data preservation, and security, etc. To do this, we first performed an analysis of the emerging healthcare IoT applications employed in sustainable smart cities in the correlation of COVID-19 from 2019-to-2021. Despite that, we have focused on the current literature in terms of network architecture, authentication, data preservation, and privacy in order to examine the benefits and drawbacks of the existing literature and set the platform for the new research in this domain. Following that, we have performed an in-depth security and privacy study in the context of TCP stack for the emerging healthcare IoT application in sustainable smart cities to identify the limitations of the existing literature. In particular, we have thoroughly examined layered-wise security and privacy threats accompanied by their countermeasures techniques.

After that, we have analyzed the existing survey papers in this domain to highlight the current issues and conducted a comparison study of our survey paper with them in order to claim the accurate analysis and contribution of our paper, which is demonstrated in Table 4. Finally, we have expanded our research from open problems to potential research directions in the healthcare IoT applications, which are used in sustainable smart cities in the coordination of COVID-19, and compared the statistics of future research paths with current survey studies in Table 5, by demonstrating what sets our article apart from other review studies.

Declaration of Competing Interest

All authors declare that they have no conflict of interest.

Acknowledgment

This work was funded by the Researchers Supporting Project number (RSP-2021/12), King Saud University, Riyadh, Saudi Arabia.

References

Abbasi, M., Mohammadi-Pasand, E., & Khosravi, M. R. (2021). Intelligent workload allocation in iot-fog-cloud architecture towards mobile edge computing. *Computer Communications, 169*, 71–80.

Abir, S. M., Islam, S. N., Anwar, A., Mahmood, A. N., & Oo, A. M. T. (2020). Building resilience against COVID-19 pandemic using artificial intelligence, machine learning, and iot: A survey of recent progress. *IoT, 1*(2), 506–528.

Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017). Internet of things security: A review of risks and threats to healthcare sector. *In 2017 IEEE international conference on internet of things (ithings) and IEEE green computing and communications (greencom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (smartdata) (pp. 373-378)*. IEEE.

Adil, M. (2021). Congestion free opportunistic multipath routing load balancing scheme for internet of things (iot). *Computer Networks, 184*, 107707.

Adil, M., Jan, M. A., Mastorakis, S., Song, H., Jadoon, M. M., Abbas, S., & Farouk, A. (2021). Hash-MAC-DSDV: Mutual authentication for intelligent iot-based cyber-physical systems. *IEEE Internet of Things Journal*.

Adil, M., Khan, R., Almaiah, M. A., Al-Zahrani, M., Zakarya, M., Amjad, M. S., & Ahmed, R. (2020). MAC-AODV based mutual authentication scheme for constraint oriented networks. *IEEE Access, 8*, 44459–44469.

Aggarwal, S., Kumar, N., Alhussein, M., & Muhammad, G. (2021). Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead. *IEEE Network, 35*(1), 20–29.

Ahad, A., Tahir, M., & Yau, K. L. A. (2019). 5g-based smart healthcare network: architecture, taxonomy, challenges and future research directions. *IEEE access, 7*, 100747–100762.

Ahanger, T. A., & Aljumah, A. (2018). Internet of things: A comprehensive study of security issues and defense mechanisms. *IEEE Access, 7*, 11020–11028.

Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). Malicious insiders attack in iot based multi-cloud e-healthcare environment: A systematic literature review. *Multimedia Tools and Applications, 77*(17), 21947–21965.

Ahmed, I., Ahmad, A., & Jeon, G. (2020). An iot based deep learning framework for early assessment of covid-19. *IEEE Internet of Things Journal*.

Ahmed, M., & Ullah, A. S. B. (2017). False data injection attacks in healthcare. *In australasian conference on data mining (pp. 192-202)*. Singapore: Springer.

Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in iot-based personalized healthcare applications. *IEEE Access, 6*, 36611–36631.

Alam, T. (2020). Internet of things and blockchain-based framework for coronavirus (covid-19) disease. *Available at SSRN 3660503*.

Alassaf, N., & Gutub, A. (2019). Simulating light-weight-cryptography implementation for iot healthcare data security applications. *International Journal of E-Health and Medical Communications (IJEHMC), 10*(4), 1–15.

Alazeb, A., & Panda, B. (2019). Ensuring data integrity in fog computing based healthcare systems. in international conference on security. *Privacy and anonymity in computation, communication and storage (pp. 63-77)*. Springer, Cham.

Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access, 7*, 101879–101894.

Ambarkar, S. S., & Shekokar, N. (2020). Toward smart and secure iot based healthcare system. in internet of things. *Smart computing and technology: A roadmap ahead (pp. 283-303)*. Springer, Cham.

Awan, K. A., Din, I. U., Almogren, A., Almajed, H., Mohiuddin, I., & Guizani, M. (2020). Neurotrust-artificial neural network-based intelligent trust management mechanism for large-scale internet of medical things. *IEEE Internet of Things Journal*.

Azrour, M., Mabrouki, J., & Chaganti, R. (2021). New efficient and secured authentication protocol for remote healthcare systems in cloud-iot. *Security and Communication Networks, 2021*.

Bahaa, A., Abdelaziz, A., Sayed, A., Elfangary, L., & Fahmy, H. (2021). Monitoring real time security attacks for iot systems using devsecops: A systematic literature review. *Information, 12*(4), 154.

Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access, 5*, 26521–26544.

Balaji, S., Nathani, K., & Santhakumar, R. (2019). Iot technology, applications and challenges: a contemporary survey. *Wireless personal communications, 108*(1), 363–388.

Bansal, M. (2020). Application layer protocols for internet of healthcare things (ioHT). *In 2020 fourth international conference on inventive systems and control (ICISC) (pp. 369-376)*. IEEE.

Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2020). CoAP–application layer connection-less lightweight protocol for the internet of things (iot) and coAP-IPSEC security with DTLS supporting coAP. *In digital twin technologies and smart cities (pp. 151-175)*. Springer, Cham.

Castiglione, A., Umer, M., Sadiq, S., Obaidat, M. S., & Vijayakumar, P. (2021). The role of internet of things to control the outbreak of COVID-19 pandemic. *IEEE Internet of Things Journal*.

Chatterjee, S. (2021). Antecedence of attitude towards iot usage: A proposed unified model for IT professionals and its validation. *International Journal of Human Capital and Information Technology Professionals (IJHCITP), 12*(2), 13–34.

Chaudhry, J. A., Saleem, K., Alazab, M., Zeeshan, H. M. A., Al-Muhtadi, J., & Rodrigues, J. J. (2021). Data security through zero-knowledge proof and statistical fingerprinting in vehicle-to-healthcare everything (v2HX) communications. *IEEE Transactions on Intelligent Transportation Systems*.

Chen, X., Feng, W., Ma, Y., Ge, N., & Wang, X. (2020). Preventing DRDos attacks in 5g networks: a new source IP address validation approach. *In GLOBECOM 2020-2020 IEEE global communications conference (pp. 1-6)*. IEEE.

Chen, Z., Guo, S., Wang, J., Li, Y., & Lu, Z. (2019). Toward FPGA security in iot: a new detection technique for hardware trojans. *IEEE Internet of Things Journal, 6*(4), 7061–7068.

Coffey, T., Saidha, P., & Burrows, P. (2003). Analysing the security of a nonrepudiation communication protocol with mandatory proof of receipt. *in proc. 1st int. symp. inform. comm. technol. trinity college dublin* (pp. 351–356).

Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of iot devices in smart home. *International Journal of Machine Learning and Cybernetics*, 1–24.

Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into iot for security: A survey. *IEEE Internet of Things Journal*.

Dewangan, K., Mishra, M., & Dewangan, N. K. (2020). A review: a new authentication protocol for real-time healthcare monitoring system. *Irish Journal of Medical Science, 1971-*, 1–6.

Dey, K., Kule, M., & Rahaman, H. (2021). PUF based hardware security: A review. in 2021 international symposium on devices. *Circuits and systems (ISDCS) (pp. 1-6)*. IEEE.

Dhanvijay, M. M., & Patil, S. C. (2019). Internet of things: A survey of enabling technologies in healthcare and its applications. *Computer Networks, 153*, 113–131.

Dofe, J., Frey, J., & Yu, Q. (2016). Hardware security assurance in emerging iot applications. *In 2016 IEEE international symposium on circuits and systems (ISCAS) (pp. 2050-2053)*. IEEE.

Dong, C., He, G., Liu, X., Yang, Y., & Guo, W. (2019). A multi-layer hardware trojan protection framework for iot chips. *IEEE Access, 7*, 23628–23639.

Duong, V., Luo, J., Pham, P., Yang, T., & Wang, Y. (2020). The ivory tower lost: How college students respond differently than the general public to the COVID-19 pandemic. *In 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 126-130)*. IEEE.

Ender, M., Ghandali, S., Moradi, A., & Paar, C. (2017). The first thorough side-channel hardware trojan. *In international conference on the theory and application of cryptology and information security (pp. 755-780)*. Springer, Cham.

Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven iot ehealth: Promises and challenges of iot in medicine and healthcare. *Future Generation Computer Systems, 78*, 659–676.

Gajbhiye, A., Sen, D., Bhatt, A., & Soni, G. (2020). DPLPLN: Detection and prevention from flooding attack in iot. *In 2020 international conference on smart electronics and communication (ICOSEC) (pp. 704-709)*. IEEE.

Ghandali, S., Moos, T., Moradi, A., & Paar, C. (2020). Side-channel hardware trojan for provably-secure SCA-protected implementations. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 28*(6), 1435–1448.

Ghotbou, A., & Khansari, M. (2021). Comparing application layer protocols for video transmission in iot low power lossy networks: an analytic comparison. *Wireless Networks, 27*(1), 269–283.

Golan, M. S., Jernegan, L. H., & Linkov, I. (2020). Trends and applications of resilience analytics in supply chain modeling: systematic literature review in the context of the COVID-19 pandemic. *Environment Systems and Decisions, 40*, 222–243.

Goyal, S., Sharma, N., Bhushan, B., Shankar, A., & Sagayam, M. (2021). Iot enabled technology in secured healthcare: applications, challenges and future directions. *In cognitive internet of medical things for smart healthcare (pp. 25-48)*. Springer, Cham.

Granjal, J., Monteiro, E., & Silva, J. S. (2014). Network-layer security for the internet of things using tinyOS and BLIP. *International Journal of Communication Systems, 27*(10), 1938–1963.

Guan, D., Wang, D., Hallegatte, S., Davis, S. J., Huo, J., Li, S., & Gong, P. (2020). Global supply-chain effects of COVID-19 control measures. *Nature human behaviour*, 1–11.

Gupta, D., Bhatt, S., Gupta, M., & Tosun, A. S. (2021). Future smart connected communities to fight covid-19 outbreak. *Internet of Things, 13*, 100342.

HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020a). AI4SAFE-iot: An AI-powered secure architecture for edge layer of internet of things. *Neural Computing and Applications, 32*(20), 16119–16133.

HaddadPajouh, H., Khayami, R., Dehghantanha, A., Choo, K. K. R., & Parizi, R. M. (2020b). AI4SAFE-iot: An AI-powered secure architecture for edge layer of internet of things. *Neural Computing and Applications, 32*(20), 16119–16133.

Hossain, M. S. (2015). Cloud-supported cyber-physical localization framework for patients monitoring. *IEEE Systems Journal, 11*(1), 118–127.

Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020). Iot dos and DDos attack detection using resnet. *arXiv preprint*.ArXiv:2012.01971

Hussain, F., Abbas, S. G., Shah, G. A., Pires, I. M., Fayyaz, U. U., Shahzad, F., & Zdravevski, E. (2021). A framework for malicious traffic detection in iot healthcare environment. *Sensors, 21*(9), 3025.

Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2017). Semantic interoperability in heterogeneous iot infrastructure for healthcare. *Wireless Communications and Mobile Computing, 2017*.

Jan, M. A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., & Stergiou, N. (2021). *LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics*. IEEE Transactions on Green Communications and Networking.

Jiang, Z., Guo, Y., & Wang, Z. (2021). Digital twin to improve the virtual-real integration of industrial iot. *Journal of Industrial Information Integration, 22*, 100196.

Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IOMT): applications, benefits and future challenges in healthcare domain. *J Commun, 12*(4), 240–247.

Jung, Y., & Agulto, R. (2021). A public platform for virtual iot-based monitoring and tracking of COVID-19. *Electronics, 10*(1), 12.

Kaliyaperumal, D., Dhas, G., Suresh, C., & Sammy, M. (2020). *Secure Health Care Data Transmission and Prevention Based on Hybrid Robin Public Key Signature Algorithm*. Secure Health Care Data Transmission and Prevention Based on Hybrid Robin Public Key Signature Algorithm.

Kamble, P., & Gawade, A. (2020). Automation in healthcare using iot and cryptographic encryption against DOS and MIM attacks. *In advanced computing technologies and applications (pp. 97-105)*. Singapore: Springer.

Kame, S. O. M., & Elhamayed, S. A. (2020). Mitigating the impact of iot routing attacks on power consumption in iot healthcare environment using convolutional neural network. *International Journal of Computer Network & Information Security, 12*(4).

Karthigaiveni, M., & Indrani, B. (2019). An efficient two-factor authentication scheme with key agreement for iot based e-health care application using smart card. *Journal of Ambient Intelligence and Humanized Computing*, 1–12.

Kavitha, D., & Ravikumar, S. (2021). IOT and context-aware learning-based optimal neural network model for real-time health monitoring. *Transactions on Emerging Telecommunications Technologies, 32*(1).E4132

Kavitha, S., Alphonse, P. J. A., & Reddy, Y. V. (2019). An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for iot health care system. *Journal of medical systems, 43*(8), 1–6.

Kazemi, Z., Papadimitriou, A., Hely, D., Fazcli, M., & Beroulle, V. (2018). Hardware security evaluation platform for MCU-based connected devices: application to healthcare iot. *In 2018 IEEE 3rd international verification and security workshop (IVSW) (pp. 87-92)*. IEEE.

Kazemi, Z., Papadimitriou, A., Souvatzoglou, I., Aerabi, E., Ahmed, M. M., Hely, D., & Beroulle, V. (2019). On a low cost fault injection framework for security assessment of cyber-physical systems: Clock glitch attacks. *In 2019 IEEE 4th international verification and security workshop (IVSW) (pp. 7-12)*. IEEE.

Khan, S., Khan, M. K., & Khan, R. (2021a). Harnessing intelligent technologies to curb COVID-19 pandemic: taxonomy and open challenges. *Computing*. https://doi.org/10.1007/s00607-021-00983-1

Khan, S. Z., Mohsin, M., & Iqbal, W. (2021b). On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science, 7*.E507

Khatkar, M., Kumar, K., & Kumar, B. (2020). An overview of distributed denial of service and internet of things in healthcare devices. *In 2020 research, innovation, knowledge management and technology application for business sustainability (INBUSH) (pp. 44-48)*. IEEE.

Kremer, S., Markowitch, O., & Zhou, J. (2002). An intensive survey of fair non-repudiation protocols. *Comput. Commun., 25*(17), 1606–1621.

Leaby, A. K., Yassin, A., Hasson, M., & Rashid, A. (2021). Towards design strong emergency and COVID-19 authentication scheme in VANET. *Indonesian Journal of Electrical Engineering and Computer Science, 21*(3), 1808–1819.

Li, W., Chai, Y., Khan, F., Jan, S. R. U., Verma, S., Menon, V. G., & Li, X. (2021). A comprehensive survey on machine learning-based big data analytics for iot-enabled smart healthcare system. *Mobile Networks and Applications*, 1–19.

Lo'ai, A. T., & Somani, T. F. (2016). More secure internet of things using robust encryption algorithms against side channel attacks. *In 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA) (pp. 1-6)*. IEEE.

Longo, M., Hirsch, M., Mateos, C., & Zunino, A. (2019). Towards integrating mobile devices into dew computing: A model for hour-wise prediction of energy availability. *Information, 10*(3), 86.

Lucca, A. V., Luchtenberg, R., de Paula Conceicao, L. G., Silva, L. A., Ovejero, R. G., Navarro-Cáceres, M., & Leithardt, V. R. Q. (2020). System for control and management of data privacy of patients with COVID-19.

Mahajan, R., & Zafar, S. (2021). DDos attacks impact on data transfer in IOT-MANET-based e-healthcare for tackling COVID-19. *In data analytics and management (pp. 301-309)*. Singapore: Springer.

Mahmoud, H. H. H., Amer, A. A., & Ismail, T. (2021). 6g: A comprehensive survey on technologies, applications, challenges, and research problems. *Transactions on Emerging Telecommunications Technologies*.E4233
Majumdar, S., Subhani, M. M., Roullier, B., Anjum, A., & Zhu, R. (2021). Congestion prediction for smart sustainable cities using iot and machine learning approaches. *Sustainable Cities and Society, 64*, 102500.
Malaj, E. G., & Marinova, G. I. (2020). Review on hardware solutions for cybersecurity of communication systems. *In 2020 28th national conference with international participation (TELECOM) (pp. 129-132)*. IEEE.
Manavi, S. Y., Nekkanti, V., Choudhary, R. S., & Jayapandian, N. (2020). Review on emerging internet of things technologies to fight the COVID-19. *In 2020 fifth international conference on research in computational intelligence and communication networks (ICRCICN) (pp. 202-208)*. IEEE.
Manocha, A., Bhatia, M., & Kumar, G. (2021). Dew computing-inspired health-meteorological factor analysis for early prediction of bronchial asthma. *Journal of Network and Computer Applications, 179*, 102995.
Marques, G., Pitarma, R., M. Garcia, N., & Pombo, N. (2019). Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review. *Electronics, 8*(10), 1081.
Masud, M., Gaba, G. S., Alqahtani, S., Muhammad, G., Gupta, B. B., Kumar, P., & Ghoneim, A. (2020). A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. *IEEE Internet of Things Journal*.
Mbunge, E. (2020). Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14*(6), 1631–1636.
Mohammed, H., Hasan, S. R., & Awwad, F. (2020a). Fusion-on-field security and privacy preservation for iot edge devices: Concurrent defense against multiple types of hardware trojan attacks. *IEEE Access, 8*, 36847–36862.
Mohammed, M. N., Syamsudin, H., Al-Zubaidi, S., AKS, R. R., & Yusuf, E. (2020b). Novel COVID-19 detection and diagnosis system using IOT based smart helmet. *International Journal of Psychosocial Rehabilitation, 24*(7), 2296–2303.
Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Improving the security of internet of things using cryptographic algorithms: A case of smart irrigation systems. *Journal of Ambient Intelligence and Humanized Computing, 12*(2), 2033–2051.
Otoom, M., Otoum, N., Alzubaidi, M. A., Etoom, Y., & Banihani, R. (2020). An iot-based framework for early identification and monitoring of COVID-19 cases. *Biomedical Signal Processing and Control, 62*, 102149.
Pang, Z. (2013). *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being*. Doctoral dissertation, KTH Royal Institute of Technology.
Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials, 22*(2), 1121–1167.
Rahardja, U., Bist, A. S., Hardini, M., Aini, Q., & Harahap, E. P. (2020). Authentication of covid-19 patient certification with blockchain protocol. *Int. J. Adv. Sci Technol, 29*(8s), 4015–4024.
Rao, T. A., & Haq, E. U. (2018). Security challenges facing iot layers and its protective measures. *International Journal of Computer Applications, 179*(27), 31–35.
Rath, M. (2020). Big data and iot-allied challenges associated with healthcare applications in smart and automated systems. *In data analytics in medicine: Concepts, methodologies, tools, and applications (pp. 1401-1414)*. IGI Global.
Ray, P. P., Dash, D., & De, D. (2019). Edge computing for internet of things: A survey, e-healthcare case study and future direction. *Journal of Network and Computer Applications, 140*, 1–22.
Rohatgi, V., & Goyal, S. (2020). A detailed survey for detection and mitigation techniques against ARP spoofing. *In 2020 fourth international conference on i-SMAC (iot in social, mobile, analytics and cloud)(i-SMAC) (pp. 352-356)*. IEEE.
Roy, S., Das, A. K., Chatterjee, S., Kumar, N., Chattopadhyay, S., & Rodrigues, J. J. (2018). Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. *IEEE Transactions on Industrial Informatics, 15*(1), 457–468.
Safkhani, M., Bagheri, N., Kumari, S., Tavakoli, H., Kumar, S., & Chen, J. (2020). RESEAP: An ECC-based authentication and key agreement scheme for iot applications. *IEEE Access, 8*, 200851–200862.
Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., & Yaseen, A. (2017). Privacy preservation in e-healthcare environments: State of the art and future directions. *Ieee Access, 6*, 464–478.
Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat COVID-19 pandemic. *Research on Biomedical Engineering*, 1–8.
Singh, V., Chandna, H., Kumar, A., Kumar, S., Upadhyay, N., & Utkarsh, K. (2020). Iot-q-band: A low cost internet of things based wearable band to detect and track absconding COVID-19 quarantine subjects. *EAI Endorsed Transactions on Internet of Things, 6*(21).
Singh, V., & Pandey, S. K. (2020). Revisiting cloud security threats: IP spoofing. *In soft computing: Theories and applications (pp. 225-236)*. Singapore: Springer.
Somasundaram, R., & Thirugnanam, M. (2020). Review of security challenges in healthcare internet of things. *Wireless Networks*, 1–7.
Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials, 20*(4), 3453–3495.
Sun, Y., Lo, F. P. W., & Lo, B. (2019). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access, 7*, 183339–183355.
Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017). Security threats in the application layer in IOT applications. *In 2017 international conference on i-SMAC (iot in social, mobile, analytics and cloud)(i-SMAC) (pp. 477-480)*. IEEE.
Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in internet-of-things (iots) framework. *Future generation computer systems, 108*, 909–920.
Toledo, P., Rubino, R., Musolino, F., & Crovetti, P. (2021). Re-thinking analog integrated circuits in digital terms: A new design concept for the iot era. *IEEE Transactions on Circuits and Systems II: Express Briefs, 68*(3), 816–822.
Tyagi, A. (2021). Healthcare-internet of things and its components: Technologies, benefits, algorithms, security, and challenges. *In optimizing health monitoring systems with wireless technology (pp. 258-277)*. IGI Global.
Ullah, F., Habib, M. A., Farhan, M., Khalid, S., Durrani, M. Y., & Jabbar, S. (2017). Semantic interoperability for big-data in heterogeneous iot infrastructure for healthcare. *Sustainable cities and society, 34*, 90–96.
Vedaei, S. S., Fotovvat, A., Mohebbian, M. R., Rahman, G. M., Wahid, K. A., Babyn, P., & Sami, R. (2020). COVID-SAFE: An iot-based system for automated health monitoring and surveillance in post-pandemic life. *IEEE Access, 8*, 188538–188551.
Veeraraghavan, P., Hanna, D., & Pardede, E. (2020). NAT++: an efficient micro-nat architecture for solving ip-spoofing attacks in a corporate network. *Electronics, 9*(9), 1510.
Venugopalan, V., & Patterson, C. D. (2018). Surveying the hardware trojan threat landscape for the internet-of-things. *Journal of Hardware and Systems Security, 2*(2), 131–141.
Venugopalan, V., Patterson, C. D., & Shila, D. M. (2016). Detecting and thwarting hardware trojan attacks in cyber-physical systems. *In 2016 IEEE conference on communications and network security (CNS) (pp. 421-425)*. IEEE.
Vijayakumar, K., Rai, A., Kumar, G. S., Angel, T. S., & Snehalatha, N. (2020). A two-way approach for detection and prevention of IP spoofing attacks. *In AIP conference proceedings (vol. 2277, no. 1, p. 020002)*. AIP Publishing LLC.
Wang, T., Mei, Y., Liu, X., Wang, J., Dai, H. N., & Wang, Z. (2021). Edge-based auditing method for data security in resource-constrained internet of things. *Journal of Systems Architecture, 114*, 101971.
Wang, X. (2014). *Hardware trojan attacks: Threat analysis and low-cost countermeasures through golden-free detection and secure design*. Doctoral dissertation, Case Western Reserve University.
Worldometers (2021). https://www.worldometers.info/coronavirus/countries-where-coronavirus-has-spread/.
Wu, Y. (2020). Cloud-edge orchestration for the internet-of-things: Architecture and ai-powered data processing. *IEEE Internet of Things Journal*.
Xiao, K., Forte, D., Jin, Y., Karri, R., Bhunia, S., & Tehranipoor, M. (2016). Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES), 22*(1), 1–23.
Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial iot. *IEEE Transactions on Industrial Informatics, 15*(6), 3632–3641.
Xu, Z., Elomri, A., Kerbache, L., & El Omri, A. (2020). Impacts of COVID-19 on global supply chains: facts and perspectives. *IEEE Engineering Management Review, 48*(3), 153–166.
Yaga, D. J., Mell, P. M., Roby, N., & Scarfone, K. (2018). Blockchain technology overview. *NIST Interagency/Internal Report (NISTIR) - 8202*, 1–59.
Yang, B., & Yang, M. (2021). Data-driven network layer security detection model and simulation for the internet of things based on an artificial immune system. *Neural Computing and Applications, 33*(2), 655–666.
Yang, K., Hicks, M., Dong, Q., Austin, T., & Sylvester, D. (2016). A2: Analog malicious hardware. *In 2016 IEEE symposium on security and privacy (SP) (pp. 18-37)*. IEEE.
Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019a). Smart healthcare: Challenges and potential solutions using internet of things (iot) and big data analytics. *PSU research review*.
Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019b). Smart healthcare: Challenges and potential solutions using internet of things (iot) and big data analytics. *PSU research review*.
Zhao, Z., Shen, L., Yang, C., Wu, W., Zhang, M., & Huang, G. Q. (2021). Iot and digital twin enabled smart tracking for safety management. *Computers & Operations Research, 128*, 105183.

Muhammad Adil received his Associate Engineer degree in Electronics form the school of Electronic associated with civil aviation Pakistan in 2010. Mr. Adil received his Bachelor of Science in Computer Science (4 years programs) and Master of Science in Computer Sciences (2 years program) with specialization in Computer Networks from Virtual University of Lahore, Pakistan in 2016 and 2019, respectively. He has CCNA and CCNP certification. He is currently a PhD Candidate. His research area includes different routing protocols, Security, and Load Balancing in WSN, IoT, and ad hoc networks. Moreover, Mr. Adil is also interested in Dynamic Wireless Charging of Electric Vehicles connected in network topological infrastructure with Machine learning techniques. He has many publications in prestigious journals such as IEEE Access, IEEE Sensors, Computer Networks Elsevier, CMC-Computer Material & Continua and MDPI Sensor etc. In addition, he is IEEE Student member. He is reviewing for prestigious journals, such as IEEE Access, IEEE Sensors, IEEE Systems, IEEE Internet of Things, IEEE Transaction of Industrial Informatics, IEEE Transactions on Cognitive Communications and Networking, MDPI Sensors and Computer Networks Elsevier Journals, Telecommunication System, and IEEE Wireless Communication Letters.

Muhammad Khurram Khan is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia. He is founder and CEO of the 'Global Foundation for Cyber Studies and Research' (http://www.gfcyber.org), an independent and non-partisan cybersecurity think-tank in Washington D.C, USA. He is the Editor-in-Chief of 'Telecommunication Systems' published by Springer-Nature with its recent impact factor of 2.314 (JCR 2021). He is also the Editor-in-Chief of Cyber Insights Magazine (http://www.cyber-insights.org). He is on the editorial board of several journals including, IEEE Communications Surveys & Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, Journal of Network & Computer Applications (Elsevier), IEEE Access, IEEE Consumer Electronics Magazine, PLOS ONE, and Electronic Commerce Research, etc. He has published more than 400 papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has edited 10 books/proceedings published by Springer-Verlag, Taylor & Francis and IEEE. His research areas of interest are Cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a fellow of the IET (UK), a fellow of the BCS (UK), and a fellow of the FTRA (Korea). His detailed profile can be visited at http://www.professorkhurram.com