algorithms

MDPI

Systematic Review

Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation

Aswani Devi Aguru [1], Erukala Suresh Babu [1], Soumya Ranjan Nayak [2,*], Abhisek Sethy [3] and Amit Verma [4]

[1] National Institute of Technology Warangal, Warangal 506004, India
[2] Amity School of Engineering and Technology, Amity University Uttar Pradesh, Noida 201313, India
[3] Department of Information Technology, GMR Institute of Technology, Rajam 532127, India
[4] Department of Computer Science Engineering, University Centre for Research Development, Chandigarh University, Mohali 140413, India
* Correspondence: srnayak@amity.edu

Abstract: Internet of Things (IoT) is one of the efflorescing technologies of recent years with splendid real-time applications in the fields of healthcare, agriculture, transportation, industry, and environmental monitoring. In addition to the dominant applications and services of IoT, many challenges exist. As there is a lack of standardization for IoT technologies, the architecture emerged as the foremost challenge. The salient issues in designing an IoT architecture encompass connectivity, data handling, heterogeneity, privacy, scalability, and security. The standard IoT architectures are the ETSI IoT Standard, the ITU-T IoT Reference Model, IoT-A Reference Model, Intel's IoT Architecture, the Three-Layer Architecture, Middle-Based Architecture, Service-Oriented Architecture, Five-Layer Architecture, and IWF Architecture. In this paper, we have reviewed these architectures and concluded that IWF Architecture is most suitable for the effortless development of IoT applications because of its immediacy and depth of insight in dealing with IoT data. We carried out this review concerning smart healthcare as it is among the major industries that have been leaders and forerunners in IoT technologies. Motivated by this, we designed the novel Smart Healthcare Reference Architecture (SHRA) based on IWF Architecture. Finally, present the significance of smart healthcare during the COVID-19 pandemic. We have synthesized our findings in a systematic way for addressing the research questions on IoT challenges. To the best of our knowledge, our paper is the first to provide an exhaustive investigation on IoT architectural challenges with a use case in a smart healthcare system.

Keywords: IoT architectures; IoT challenges; IoT countermeasures; IoT Protocols; IoT applications; smart healthcare; COVID-19 pandemic; Medical 4.0

check for updates

Citation: Aguru, A.D.; Babu, E.S.; Nayak, S.R.; Sethy, A.; Verma, A. Integrated Industrial Reference Architecture for Smart Healthcare in Internet of Things: A Systematic Investigation. *Algorithms* **2022**, *15*, 309. https://doi.org/10.3390/a15090309

Academic Editors: Frank Werner and Pierre Leone

Received: 26 July 2022
Accepted: 17 August 2022
Published: 29 August 2022

1. Introduction

The term "Internet of Things" was first introduced by Kevin Aston in 1996 when he deployed an application in supply chain management using radio frequency identification (RFID) tags [1]. IoT has brought a revolution in making the Internet and other real-world applications smarter. Machine to machine (M2M) communication can be used interchangeably with IoT because things can communicate with other things using the Internet without human intervention. The world has turned its attention towards IoT and its research because there are compelling applications and services. By the end of 2020, there were billions of connected smart devices [2], from which we can conclude that future technologies will be IoT dependent. Some reasons for deploying IoT include dynamic industry control, improvements in the quality of daily life, increments in resource utilization, maintaining a better relationship between humans and nature, universal transportation, global internetworking, enhanced accessibility, and amplified usability. With these extensive advantages, IoT is elevated as another industrial revolution. Smart homes, smart agriculture, smart transportation, smart health (Internet of Medical Things/IoMT), smart industry, and smart supply chains are the acclaimed applications of IoT. Each of these applications has its part in delivering an increased standard of living. Smart healthcare is an actual application of IoT and has advantages over traditional healthcare systems. These applications effectively reduce the costs and risks of medical processes, ensure timely diagnoses, improve healthcare resource utilization, support telemedical services, support self-service medicare, assists with early detection of diseases, and facilitate optimal hospital management.

Besides the splendid applications and services of IoT, many challenges exist. The foremost issue in the real-time deployment of the IoT is its architecture. There is no standard IoT architecture, and organizations such as IBM, Intel, and Cisco designed their reference architectures based on their approaches to developing IoT technologies. Some of the IoT architectural standards include the ETSI IoT Standard, ITU-T IoT Reference Model, IoT-A Reference Model, Intel's IoT Architecture, Three-Layer Architecture, Middle-Based Architecture, Service-Oriented Architecture, and Five-Layer IWF Architecture. IoT Protocols play a vital role in any IoT architecture and are responsible for data exchange among intelligent devices in IoT networks. The IoT architectural standards encounter many challenges, including connectivity, data handling, heterogeneity, interoperability, privacy, scalability, and security. The billions of smart devices, including sensors, RFID tags, etc. [3], need to be connected continuously, which is tough to attain. Data handling issues exits, as vast amounts of data are generated from smart devices [4,5]. Heterogeneity is challenging because communication must be done among devices of heterogeneous manufacturers, heterogeneous protocols, and heterogeneous architecture standards [6]. Interoperability is a significant issue because different technologies are used for communication by IoT devices [7–9]. Privacy must be ensured to build the customers' trust by protecting users' information from exposure in the IoT environment [10]. The scalability of IoT must be ensured for the adaptability of devices to changing needs of the future [11]. The security of IoT has gained researchers' attention. They have worked on security protocols and algorithms, as there are major vulnerabilities in IoT devices [12,13]. Authentication is the major challenge under IoT security that enables access for only the authorized users [14–17]. Figure 1 depicts the histogram on the number of papers published in IoT application domains in the past five years. Statistics have shown that less research is being carried out on the smart healthcare domain, even though it is the signature field in real-time. The works by Maurizio Capra et al. [18] and Rana Alabdan [19] were studied for understanding the various paradigms and protocols in conducting the systematic surveys. Taher M. Ghazal et al. [20] presented a review on machine learning approaches in smart healthcare in regard to IoT smart cities. By building a deep understanding of the presented surveys, we have presented a novel and systematic investigation by employing a qualitative methodology to address research questions on IoT challenges [21]. Throughout this investigation, we have employed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA, (accessed on March 2021) https://prisma-statement.org/) approach. Figure 1 depicts the flow diagram of the identification and finalizing of the resources which are included in our review.

We performed the identification of studies via nine kinds of databases in three major stages.

- **Identification of Sources:** We collected 160 sources from various databases. Before the screening process, we removed the duplicate records and irrelevant records.
- **Screening of sources based on objectives:** The screened records from the previous step were sought for retrieval, and the same number of reports were assessed for eligibility. The screening process resulted in the optimal number of records which contributed the best for carrying out the systematic survey.
- **Final resources which we included:** After performing the level-wise screening, the final 136 resources were identified for reference. The number of sources from each databases was tabulated in detail.

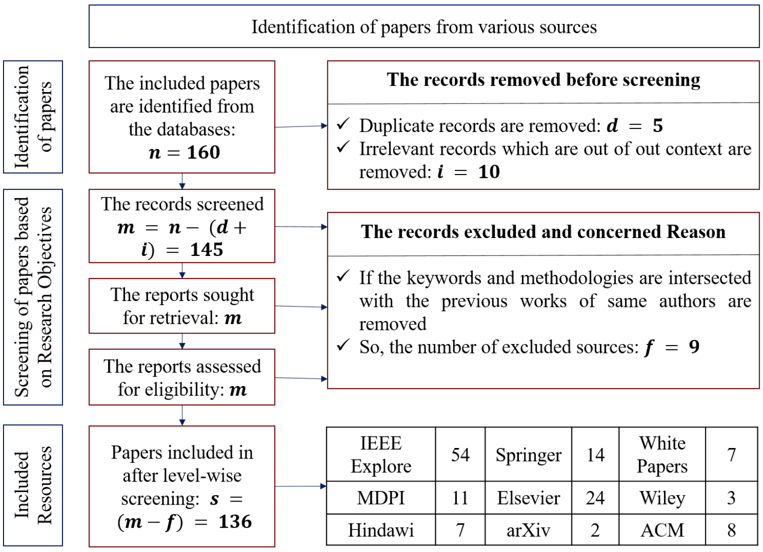

Identification of papers from various sources
Identification of papers
The included papers are identified from the databases: $n = 160$
The records removed before screening
✓ Duplicate records are removed: $d = 5$
✓ Irrelevant records which are out of out context are removed: $i = 10$
Screening of papers based on Research Objectives
The records screened $m = n - (d + i) = 145$
The reports sought for retrieval: m
The reports assessed for eligibility: m
The records excluded and concerned Reason
✓ If the keywords and methodologies are intersected with the previous works of same authors are removed
✓ So, the number of excluded sources: $f = 9$
Included Resources
Papers included in after level-wise screening: $s = (m - f) = 136$
IEEE Explore 54
Springer 14
White Papers 7
MDPI 11
Elsevier 24
Wiley 3
Hindawi 7
arXiv 2
ACM 8

Figure 1. Flow diagram of our systematic investigation using the PRISMA approach.

Before conducting the systematic review, we prepared a research protocol that describes the methodology or approach for carrying out this review. As shown in the Phase 2 in Figure 1, we carried out developed a research protocol that describes the planned method of the review. The IoT protocols, applications, implementation issues, and corresponding countermeasures were reviewed. Thus, the respective papers are included in our review. We included the papers which address various IoT architectures as presented in Section 3. We designed a smart healthcare architecture using one of these standard architectures, called IWF Architecture. Thus, we included the research papers and white papers on IWF Architecture while designing SHRA. To elaborate the responsibilities of all seven layers, the concerned references are included. The existing mechanisms which address the IoT challenges and countermeasures are included. The references regarding the significance of smart healthcare during COVID-19 pandemic are included. The major mechanisms and their improvements in the future are discussed with the respective paper references.

All the included papers/references contribute to our systematic literature survey in an optimal and precise way. Figure 2 presents the number of papers published in significant IoT application domains. Even though there are tremendous industrial architectures for smart healthcare, our proposed SHRA is the simplest architecture that provides the clear flow of IoT data.

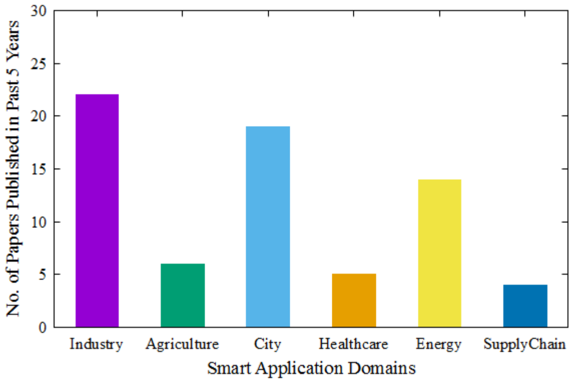


Figure 2. Number of papers published in major IoT application domains.

1.1. Motivation

As mentioned in the introduction, many researchers have presented various surveys on IoT architectures and applications. We present a novel systematic investigation on an integrated industrial reference architecture for smart healthcare in IoT. We achieved novelty in constructing the reference architecture for smart healthcare applications along with the analysis of various standard IoT architectures. To the best of our knowledge, no published review has presented the standard IoT Architectures and the challenges of a smart healthcare system. It is pivotal to review the existing models for designing a reference architecture of an IoT application or service. Among the applications of IoT, smart healthcare gained our attention. Getting medical services is one of the basic needs of humans. However, sometimes, the limitations in outmoded healthcare systems lead to the loss of lives. Motivated by the essence of smart healthcare, we have designed a novel reference architecture for smart healthcare based on a standard IoT architecture.

1.2. Our Contribution

The whole overview of the review is depicted in the form of a road map in Figure 3. This paper presents an integrated industrial reference architecture for smart healthcare systems in the Internet of Things with the following objectives:

1. We reviewed nine standard IoT architectures, key challenges of these IoT Architectures, and various IoT applications.
2. The IoT World Forum (IWF) reference architecture is the most suitable model for the effortless development for any IoT application after performing a comprehensive analysis on these IoT architectures with pros and cons.
3. We have designed a Smart Healthcare Reference Architecture (SHRA) based on IWF Architecture and present a detailed analysis on the substantial challenges of SHRA.
4. Finally, we present the significance of smart healthcare during the COVID-19 pandemic with up-to-date statistical analysis.

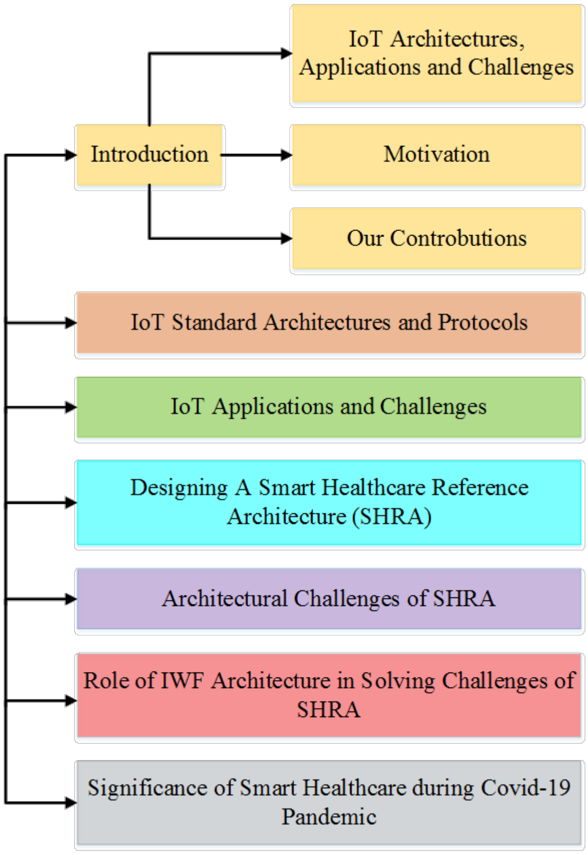

IoT Architectures,
Applications and Challenges
Introduction
Motivation
Our Controbutions
IoT Standard Architectures and Protocols
IoT Applications and Challenges
Designing A Smart Healthcare Reference Architecture (SHRA)
Architectural Challenges of SHRA
Role of IWF Architecture in Solving Challenges of SHRA
Significance of Smart Healthcare during Covid-19 Pandemic

Figure 3. Road-map of the paper.

2. Flow of Systematic Investigation

In this section, we present the detailed flow of our systematic investigation in six phases, as depicted in Figure 4.

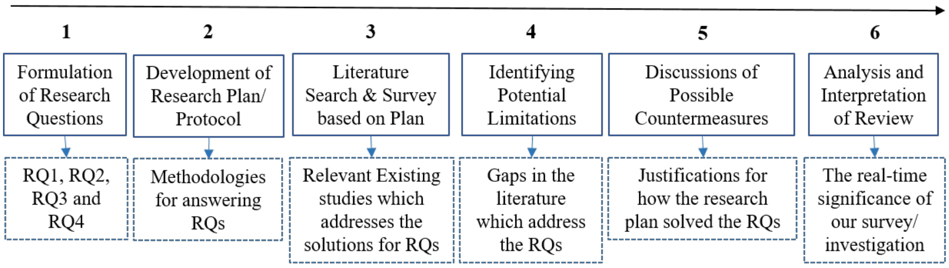

1
2
3
4
5
6
Formulation of Research Questions
Development of Research Plan/ Protocol
Literature Search & Survey based on Plan
Identifying Potential Limitations
Discussions of Possible Countermeasures
Analysis and Interpretation of Review
RQ1, RQ2, RQ3 and RQ4
Methodologies for answering RQs
Relevant Existing studies which addresses the solutions for RQs
Gaps in the literature which address the RQs
Justifications for how the research plan solved the RQs
The real-time significance of our survey/ investigation

Figure 4. Flow of our systematic investigation.

2.1. Formulation of Research Questions

The present survey is intended to address and justifies the following four research questions (RQs).

RQ1: What is the most suitable IoT architecture for designing any IoT application?
RQ2: How can one design a reference architecture for smart healthcare applications using the appropriate standard IoT architecture?
RQ3: What are the challenges in designing and developing any smart healthcare application?
RQ4: What are the approaches for avoiding IoT architectural challenges?

2.2. Development of Research Plan/Protocol

For addressing *RQ1*, the standard IoT architectures needed to be studied while analyzing the advantages and disadvantages each architecture. Among them, the most suitable architecture was selected for designing the smart application. The review protocol for *RQ2* was to define the layered architecture using the selected standard architecture. The functionalities of each layer must be described in detail. *RQ3* can be addressed by identifying the challenges in designing the IoT applications. The countermeasures for the identified challenges were examined during the exploration of *RQ4*.

2.3. Literature Search and Survey Based on Plan

The relevant literature was selected and studied based the research protocol. The existing works in the literature are discussed for each *RQ*. The protocol was designed using the PRISMA approach for identifying and screening the resources. Developing a smart healthcare reference architecture and discussing the challenges and countermeasures in designing such a reference architecture in IoT environments are the significant elements behind the protocol of our review.

2.4. Identifying Potential Limitations

RQ3 identified the limitations in implementing the real-time IoT applications. The existing literature that address each limitation was reviewed. This phase can be called an extension of literature research. The limitations need to be discussed from the set of significant references which were screened using PRISMA method.

2.5. Discussions of Possible Countermeasures

The possible extensions of the existing works are discussed. The countermeasures for the identified limitations are also presented. As a part of our survey based plan or protocol, the white papers from cisco are included for providing the countermeasures for architectural challenges.

2.6. Analysis and Interpretation of Review

The analysis of the existing mechanisms in the literature related to all *RQs* is discussed and interpreted. We also discuss the significance and the applicability of the presented smart heath-care architecture during COVID-19 pandemic. The discussion section provides the pros and cons of considerable mechanism which are mentioned in the literature.

After the six phases from the flow of our systematic investigation, we have also discussed the future applicability of SHRA in brief. Usage of PRISMA approach in conducting the optimal literature search and screening. Based on this step by step systematic investigation, the quality and precise paper references using PRISMA approach lead to quality investigation.

3. IoT Standard Architectures

IoT architectures define the standards and techniques for designing and building IoT ecosystems [22]. The architecture gives a protocol stack and involves how the data are transported, collected, analyzed, and ultimately acted upon. Architectural standards and frameworks have emerged to address the challenge of designing massive-scale IoT networks. In this paper, we present nine architectural standards and describe their layered architectures in detail.

1. ETSI IoT Standard.
2. ITU-T IoT Reference Model.
3. IoT-A Reference Model.
4. Intel's IoT Architecture.
5. Three-Layer Architecture.
6. Middle-Based Architecture.
7. Service-Oriented Architecture.
8. Five-Layer Architecture.
9. Social Internet of Things Representative Architecture.
10. Multi-Internet of Things Architecture.
11. IWF Reference Architecture.

3.1. ESTI M2M Reference Architecture

The European Telecommunications Standards Institute (ETSI) IoT Standard, also known as the ESTI M2M Reference Architecture (as shown in Figure 5), is the high-level functional architecture that consists of Device and Gateway Domain and Network Domain [23]. The lower domain includes the M2M device that runs applications, the M2M gateway, and the M2M Area Network. The upper domain has an Access network, a Core network, M2M Service Capabilities, M2M Applications, a Network Management Functions, and M2M Management Functions. These Two domains can communicate in three ways: direct connectivity, gateway as a network proxy, and multiple gateways as a network proxy. ESTI is the basic standard on which many M2M standards have been built. It gives the requirements, architecture, application programming interface (API), security solutions, and interoperability for M2M and IoT technologies.

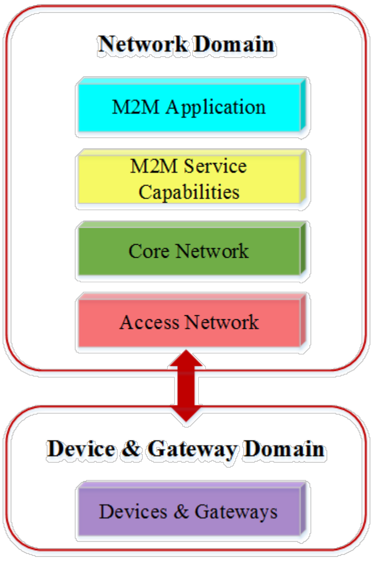


Figure 5. ESTI Reference Architecture.

3.1.1. Advantages of ESTI M2M Reference Architecture

- ESTI is involved in standardizing the technologies at the radio and service layers.
- Context information management enables the exchange of data together with its context.
- Fixed and mobile networks are supported with easy maintenance.

3.1.2. Disadvantages of ESTI M2M Reference Architecture

- Limited flexibility for developing a reference architecture for any smart application.
- Security and ownership of data are not figured out.
- This model does not support interoperability across many application domains.
- It is designed and optimized for networks with fewer smart devices.
- The step-by-step flow of IoT data is a big concern in the ESTI M2M model.

3.2. ITU-T Reference Architecture

International Telecommunication Union—Telecommunication (ITU-T) Reference architecture (as shown in Figure 6) presents a broader representation of all upper layers and capability levels [24]. The abbreviations mentioned in the above figure are elaborated as follows:
DC: Device Capabilities
GC: Gateway Capabilities
NC: Network Capabilities
TC: Transport Capabilities
GSC: Generic Support Capabilities
SSC: Specific Support Capabilities
IOTA: IoT Applications
GMC: Generic Management Capabilities
SMC: Specific Management Capabilities
GSEC: Generic Security Capabilities
SSEC: Specific Security Capabilities

DC deals with sensing and actuating, ad hoc networking, and communication with upper layers. GC deals with multiple interface support, protocol conversion, application logic, and the execution environment. NC deals with connectivity and mobile management and AAA (authentication, authorization, and accounting). TC deals with transport services for data and control information. GSC deals with data processing and storage. SSC deals with support functions of various IoT applications. IOTA deals with applications written by the developer and executed by the user. GMC deals with device management, such as activation and deactivation, firmware and software upgrades, network topology, and congestion management. SMC deals with application-specific requirements. GSEC deals with authorization, authentication, integrity, data confidentiality, and privacy protection. SSEC deals with application-specific requirements.

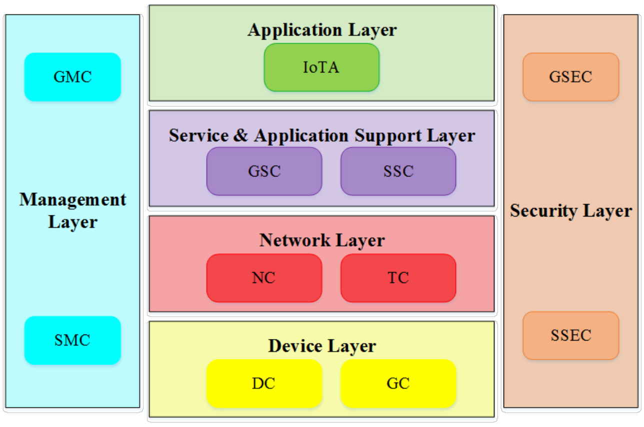


Figure 6. ITU-T Reference Architecture.

3.2.1. Advantages of ITU-T Reference Architecture

- The IoT reference model defined by ITU-T focuses on the capabilities view of IoT infrastructure.
- It can easily collaborate with other IoT reference architectures.
- This architecture supports smart ports for any smart application, improving their operations and services.

3.2.2. Disadvantages of ITU-T Reference Architecture

- Data processing and management support are limited for any smart application.
- This architecture defines the capability exposure of each layer rather than the flow of IoT data from the device layer to the application layer.

3.3. IoT-A Architectural Reference Model

IoT comprises heterogeneous things and technologies, so a significant issue arises regarding architectural standardization. To address this challenge, the European Lighthouse Integrated Project was proposed in 2016, named IoT-A (as shown in Figure 7), which includes the creation of architectural reference models along with the composition of key building blocks [25]. IoT-A uses an experimental paradigm that combines a top-down approach for forming architectural principles and prototype-based design guidelines for exploring the technical consequences of previously chosen architectural designs that support interoperability.

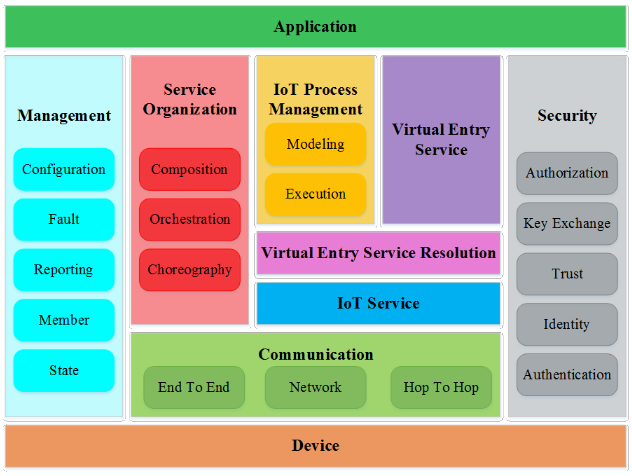


Figure 7. IoT-A Architecture.

3.3.1. Advantages of IoT-A Reference Architecture

- This model can be concretely related to the other standard IoT architectures.
- It promotes the overall understanding of IoT domains.
- A reference architecture can be drawn based on IoT-A architecture using its building blocks.

3.3.2. Disadvantages of IoT-A Reference Architecture

- It is a bit harder to understand the processes and responsibilities of each layer.
- Limited adaptability, and it is difficult to understand a complex functional view along with a security and privacy perspective.
- Designing a reference architecture from the IoT-A model must consider the domain, information, and communication models.

3.4. Intel's IoT Architecture

Intel has defined an IoT architecture named the System Architecture Specification [26]. This model (as shown in Figure 8) has three components: things, network, and cloud, providing device and data security. Moreover, it is designed to facilitate more intelligent IoT and transfer the computation to the edge for faster data accumulation and analysis responses.

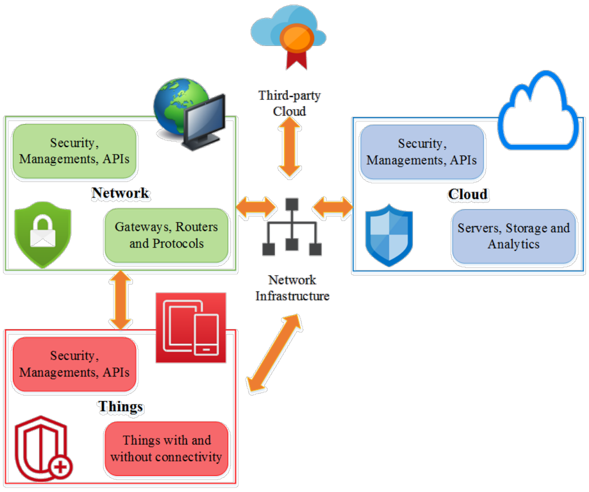

Third-party Cloud
Security, Managements, APIs
Network
Gateways, Routers and Protocols
Security, Managements, APIs
Cloud
Servers, Storage and Analytics
Network Infrastructure
Security, Managements, APIs
Things
Things with and without connectivity

Figure 8. IoT architecture by Intel.

Advantages of Intel's IoT Architecture

- It supports enterprises to move towards the edge. This facilitates bulk data capturing, faster analysis, and high-speed processing.
- Strategic decision-making is enabled in the IoT-A reference model.
- It delivers more significant support for big data processing and analytics.

3.5. Three-Layer Architecture

This IoT architecture is helpful for beginners in IoT [27,28]. The 3-layer model (as shown in Figure 9a) consists of the perception layer, a network layer, and an application layer. The perception layer collects data through physical devices such as sensors, actuators, and other edge devices. The network layer obtains the data from the perception layer for storage and distribution. The application layer enables communication with the user for accessing application-specific resources.

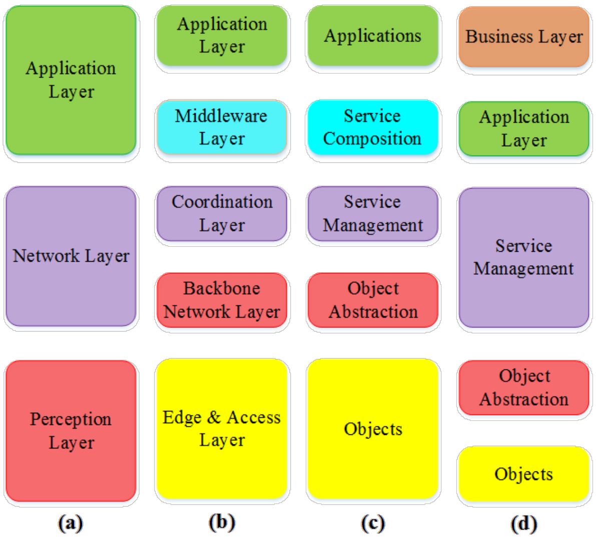


Figure 9. (**a**) Three-Layer Architecture. (**b**) Middle-Ware-Based Architecture. (**c**) Service-Oriented Architecture Based Model. (**d**) Five-Layer Architecture.

3.5.1. Advantages of Three-Layer Architecture

- Simple architecture and easy-to-understand flow of IoT data.
- Any real-time application can be used in this basic architecture.

3.5.2. Disadvantages of Three-Layer Architecture

- Three-layer architecture presents the abstract view of the IoT operational stack, so it cannot deliver detailed architecture for designing a reference architecture.
- It provides the outline of IoT and does not give practical insight into researching the IoT.

3.6. Middle-Ware Based Architecture

In the Middle-Ware-Based Architecture (as shown in Figure 9b), there are edge technologies, an access layer, a alone application system, a backbone network layer, a coordination layer, a middle-ware layer, and an application layer [29–31]. The middle-ware acts as a mediator between the network technologies cluster and the application layer. Middle-ware enables the flow of real-time information access within and among systems in the IoT network.

3.6.1. Advantages of Middle-Ware Based Architecture

- The functional components of IoT middle-ware architecture enable interoperation and context detection.

- Effective device discovery and management with platform portability.
- Enhanced security and privacy.
- Managing high data volumes.

3.6.2. Disadvantages of Middle-Ware Based Architecture

- There is no generic middle-ware that can be applied for multiple smart applications.
- Scalability is not achieved in this model.

3.7. Service-Oriented Architecture

A service-oriented architecture (SOA) includes objects, object abstraction, service management, service composition, and an application layer. This model (as shown in Figure 9c) focuses on software functionality that can be reused for different tasks [32–35]. Applications use services available in the network with adequate resources and services. Applications in SOA are built based on services.

3.7.1. Advantages of Service-Oriented Architecture

- SOA can be used to create a reference based on system services.
- This architecture reduces the product development time by neglecting the unnecessary details.

3.7.2. Disadvantages of Service-Oriented Architecture

- SOA needs higher bandwidth for data transmission in IoT applications.
- The model will be overloaded with extra computation if multiple services are used.

3.8. Five-Layer Architecture

In the 5-layer model (as shown in Figure 9d), there are objects, object abstraction, service management, application layer, and business layer. The object layer holds the physical devices for data collection [36,37]. The object abstraction layer fulfills the transmission and communication responsibilities, and the service management layer is responsible for device management and information analytics. The application layer manages application processes based on the services available in the network. It comprises clouds and servers. The business layer defines how the applications must be delivered for improved user experience in terms of business models.

3.8.1. Advantages Five-Layer Architecture

- It extends three-layer architecture and delivers a detailed perspective about IoT technologies.
- This architecture is most suitable for edge technologies and broad application areas.

3.8.2. Disadvantages of Five-Layer Architecture

- This model cannot provide deep insight into data ingestion and aggregation of IoT data.

3.9. Social Internet of Things Representative Architecture (SIoT-RA)

SIoT-RA establishes the social relationships with things through social computing and social networking paradigms. Trust, device discovery, and scalability issues of IoT are addressed using this representative architecture (Figure 10). The autonomous connections can be built among things and humans using the bidirectional navigation links. The unique ID for IoT object, meta-information, security controls, service discovery, relationship management, and service composition are the major components of the SIoT representative architecture. Luigi Atzori et al. [38] presented a review on architectures, concepts, and network characterizations of social Internet of Things. The authors have outlined the real-time scenarios when IoT meets the social networking.

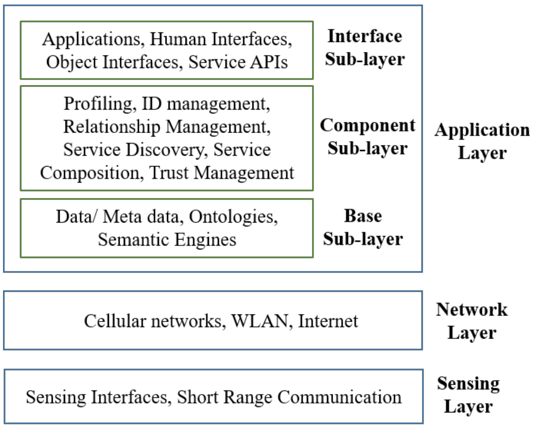

Applications, Human Interfaces, Object Interfaces, Service APIs
Interface Sub-layer
Profiling, ID management, Relationship Management, Service Discovery, Service Composition, Trust Management
Component Sub-layer
Application Layer
Data/ Meta data, Ontologies, Semantic Engines
Base Sub-layer
Cellular networks, WLAN, Internet
Network Layer
Sensing Interfaces, Short Range Communication
Sensing Layer

Figure 10. Social Internet of Things Representative Architecture for the IoT server.

3.9.1. Advantages of SIoT-RA

- Easy integration of WSNs and short range communication technologies such as NFC, Ultra-Wide Band, and RFID.
- A separate layer is dedicated for data transport functionalities.
- Component sub-layer enables the interoperabiltiy and service discovery features.

3.9.2. Disadvantages of SIoT-RA

- The relationship management is only enabled for the servers, but not for objects and gateways.
- Efficiency of resource discovery will be decreased if the number of interactions among the objects is increased.
- Higher complexity.

3.10. Multi-Internet of Things Architecture

MIoT architecture is the recent extension of the Social IoT paradigm, where multiple IoT can be communicated and interact through specific objects called cross-objects or cross nodes (c-nodes) (as shown in (Figure 11)). The inner nodes (i-nodes) are the nodes within the IoT network [39–41]. This deals with semantic-based and data-driven aspects of IoT systems rather that technical issues. The complexity of SIoT can be reduced using MIoT paradigm while joining multiple social IoT networks. SIoT is a specific case of MIoT, in which the relationships are defined at an early stage.

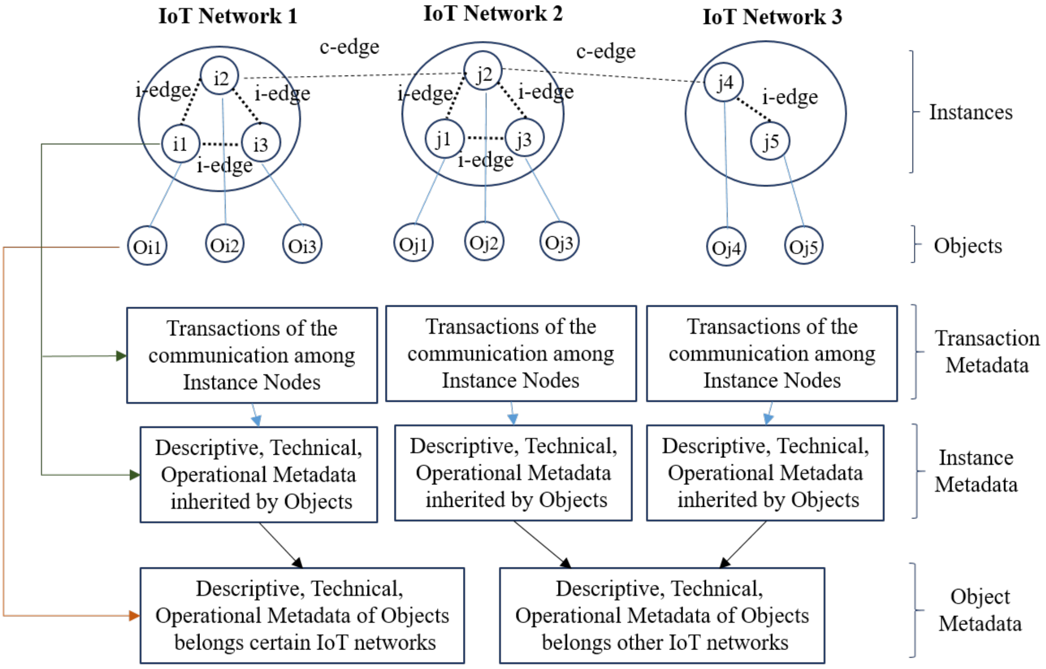

IoT Network 1
IoT Network 2
IoT Network 3
c-edge
c-edge
i-edge
i-edge
i-edge
i2
i1
i3
j2
j1
j3
j4
j5
Oi1
Oi2
Oi3
Oj1
Oj2
Oj3
Oj4
Oj5
Instances
Objects
Transactions of the communication among Instance Nodes
Descriptive, Technical, Operational Metadata inherited by Objects
Descriptive, Technical, Operational Metadata of Objects belongs certain IoT networks
Descriptive, Technical, Operational Metadata of Objects belongs other IoT networks
Transaction Metadata
Instance Metadata
Object Metadata

Figure 11. Multi-IoT Architecture.

3.10.1. Advantages of MIoT

- Reduced complexity in managing multiple IoT systems with social networking paradigms.
- Complex IoT networks can be handled with reliability.

3.10.2. Disadvantages MIoT

- Cannot support cleaning and preprocessing of IoT data at edge.
- Data integration is not addressed in this architecture.

3.11. IWF Reference Architecture

The IoT World Forum (IWF) Reference Architecture (as shown in Figure 12), released in October 2014 contains seven layers from edge level to a central cloud [42]. The IWF model is mainly concerned with developing the applications, middle-ware, and support functions of enterprise-based IoT. The characteristic of the IWF reference model is it simplifies, clarifies, identifies, standardizes, and organizes the IoT functionalities. This reference model defines the integration of traditional IT and OT parts. Table 1. depicts the IWF layers and their respective responsibilities.

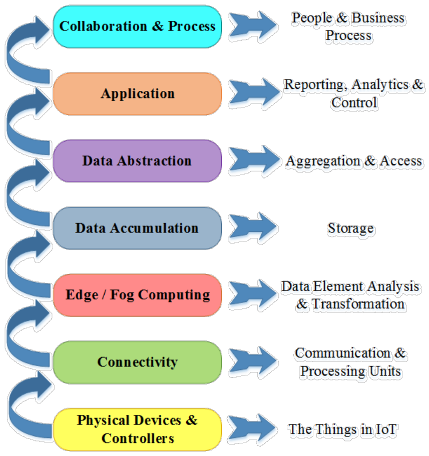

Collaboration & Process
People & Business Process
Application
Reporting, Analytics & Control
Data Abstraction
Aggregation & Access
Data Accumulation
Storage
Edge / Fog Computing
Data Element Analysis & Transformation
Connectivity
Communication & Processing Units
Physical Devices & Controllers
The Things in IoT

Figure 12. IWF 7-layered reference architecture.

Table 1. Layers and respective responsibilities of the IWF Architecture.

Layer	Responsibility
1–Edge Devices/Controllers	Physical devices like sensors, actuators, RFID tags
2–Connectivity	Sum of all hardware and protocols
3–Edge/Fog Computing	Data handling and network security such as the end to end data encryption, Data filtering, Data scrubbing, Event generation
4–Data Accumulation	Data in motion becomes Data at Rest, creation of database records, allowing data query, accumulation, and filtering strategies for data optimization
5–Data abstraction	Ensures quality and completeness of data, Extract, Transform, Load (ETL) functions, Data Processing, Data Comparison and reconciliation, and many types of data manipulations
6–Applications	Data interpretation, Reporting, Analytics and System Control
7–Users/Collaboration	User interaction is coordinated with all functions of the system

Advantages of IWF Reference Model over Other Architectures

- The IoT system topology is depicted clearly in the IWF model.
- It boosts the operational efficiency of the IoT ecosystem by effective decision-making on resource and service management.
- All seven layers of the IWF model are responsible for the optimal flow of IoT data, so this architecture minimizes the cost and downtime by enabling preventive maintenance.
- The business layer of the IWF model is responsible for collaboration and business process handling. This improves the IoT products and services through user or customer satisfaction. This model opens up new business opportunities.
- Realizing the scalability is easy with the IWF model compared to other architectural standards,
- IWF Architecture is the best model for data management. It defines the data accumulation and abstraction capabilities separately for exhaustive data processing.
- Instead of being conceptual, the IWF reference model is a real and approachable system applicable to any IoT application.
- This model ensures modularity and interoperability by enabling the technologies to be compatible with Industry 4.0

After an extensive analysis of the above nine standard IoT architectures, IWF Architecture has better advantages for designing a reference architecture for any IoT application. This motivated us to consider the IWF model the best model for IoT research.

4. IoT Protocols

The IWF reference model categorizes IoT Protocols into three sections based on the roles they play within the network (as shown in Figure 13) [43–46].

1. **Application Protocols:** Application protocols are responsible for reporting, analytics, and controlling the users' interactions with the applications for adding business value to the services.
2. **Service Discovery Protocols:** Service discovery protocols deal with finding the available services for the client's available requests in the network.
3. **Infrastructure Protocols:** Infrastructure protocols include network technologies and Internet protocols. These fundamental protocols enable communication and access technologies.

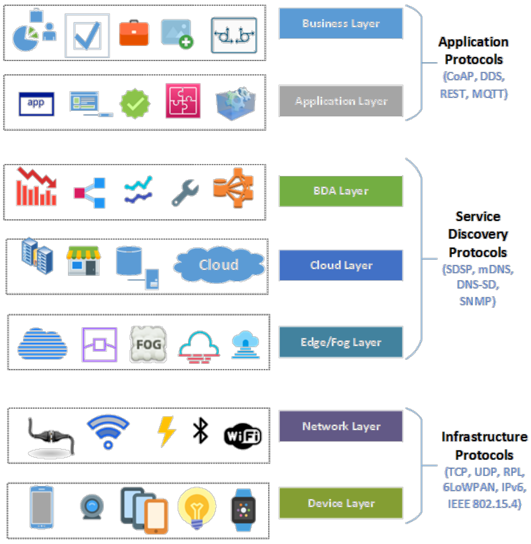


Figure 13. Protocol categorization of IWF layers.

4.1. Application Protocols

- **Message Queue Telemetry Transport (MQTT):** This protocol was invented by IBM in 2000 for telemetry applications using low power data rates [47]. This protocol operates in a publish–subscribe model and is designed exclusively for lightweight applications. It requires a small code footprint and low bandwidth.
- **Extensible Messaging and Presence Protocol (XMPP):** This communication protocol is based on XML to realize the message-oriented middle-ware and applications [48,49]. This protocol is also used in publish–subscribe systems, file transfer services, and some communication applications of embedded IoT.
- **Advance Message Queuing Protocol (AMQP):** This is a standard for asynchronous messaging by wire [50,51]. Encrypted and interoperable messaging between organizations and applications will be done. This protocol is popular for IoT device management that uses client–server messaging.
- **Constrained Application Protocol (CoAP):** A web protocol for constrained devices that exchanges messages in asynchronous mode [52,53]. Uniform resource identifier support is enabled with minimum complexity in this RESTful protocol.
- **Data Distribution Service (DDS):** This is a machine-to-machine communication protocol that enables data exchange through the publish–subscribe method [54,55]. Unlike MQTT and CoAP, DDS uses a broker-less architecture. As this model has a data bus that directly connects producers and subscribers; it employs multi-casting techniques for data transmission and a high-quality service in small memory footprint devices.

4.2. Service Discovery Protocols

- **Multicast DNS (m-DNS):** It resolves host names to IP addresses without using a unicast DNS server [56]. It operates on multicast UDP packets, through which a node acquires terms of all nodes in the local network. This protocol can be implemented irrespective of infrastructure failures.
- **DNS-Service Discovery (DNS-SD):** It uses standard DNS messages to discover services of an IoT network [57]. Host names of the service provider are resolved, and IP addresses are paired with host names using mDNS.
- **Simple Service Discovery Protocol (SSDP):** This protocol is the basis for UPnP used in small-scale networks to advertise and discover network services [58]. It does not use any server-based configuration mechanism such as DHCP or DNS, based on an IP suite.

4.3. Infrastructure Protocols

4.3.1. Network Technologies

The network technology layer consists of the physical/device layer and link layer protocols.

- **Zigbee:** It uses the IEEE 802.15.4 standard and operates in the 2.4 GHz frequency range with 250 kbps [59]. The maximum number of nodes in the network is 1024, and has a capacity of up to 200 m. Zigbee can use 128-bit AES encryption.
- **Bluetooth Low Energy (BLE):** It provides the same range as classic Bluetooth with considerably less energy consumption [60]. This is used in beacons used to send contextual information based on location (Google Beacon Platform, Google Physical Web, Apple ibeacon)
- **Near Field Communication (NFC):** It is a short-range, high frequency (13.56 MHz) wireless technology based on RFID [61]. Two devices have to come closer to initiate the transaction, such as a phone and payment terminal.
- **IEEE 802.15.4:** It is a standard that specifies the physical layer and media access control for low-rate wireless personal area networks [62]. It has the Zigbee, Wireless HART, and MiWi specifications. It is used with 6LoWPAN and standard Internet protocols to build a wireless embedded Internet.

4.3.2. Internet Protocols

Internet protocols consist of a transport layer, routing protocols, and network-layer protocols.

- **Internet Protocol v6 (IPv6):** It is a 128-bit addressable protocol that provides improved remote access and large-scale IoT device management [63]. It ensures the security, scalability, and connectivity of IoT ecosystems. Thus, it is the perfect solution for real-time IoT deployment.
- **IPv6 over Low Power Wireless Personal Area Network (6LoWPAN):** This is an adaptation layer for IPv6 over IEEE 802.15.4 links [64]. It operates only in the 2.4 GHz frequency range with a 250 kbps transfer rate. It is a network encapsulation protocol.
- **Routing Protocol for Low Power and Lossy Networks (RPL):** It was developed by the IETF ROLL working group. It is ideal for N to 1 links (meters reading) [65]. It is a proactive protocol that is susceptible to packet loss. It is implemented in Contiki OS for usage on microcontrollers and sensor nodes.
- **User Datagram Protocol (UDP):** This connection-less and lightweight communication protocol focuses on low latency communication, rather than reliability, which is the desirable characteristic of IoT communication [66].

5. IoT Applications and Challenges

IoT solves many real-life problems and makes our lives simpler and smarter [67]. Many applications are already being deployed extensively, bringing immense value and fruitfulness to our lives [68]. The significant IoT applications are smart health, smart agriculture, smart industry, smart cities, and smart supply chains [69]. This section presents the analysis table about IoT applications' issues and corresponding countermeasures.

Table 2 presents the significant IoT applications and the issues in their real-time implementations along with the possible counter measures. Table 3 Presents various IoT protocols and their IoT applications.

Table 2. Layers and respective responsibilities of the IWF Architecture.

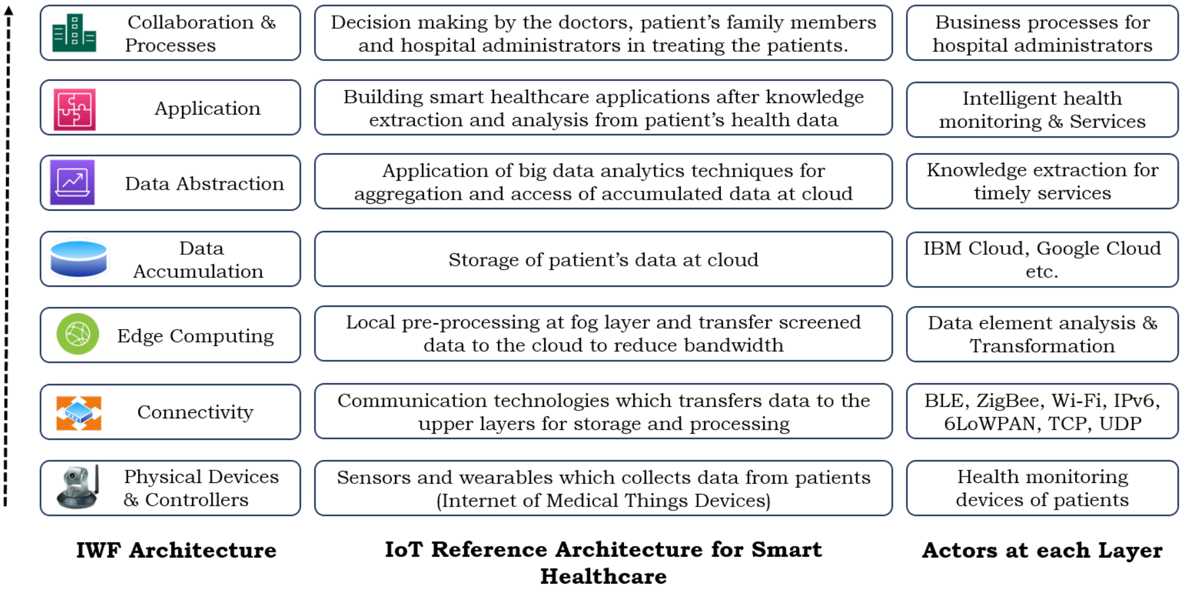
Layer	Responsibility
1—Edge Devices/Controllers	Physical devices like sensors, actuators, RFID tags
2—Connectivity	Sum of all hardware and protocols
3—Edge/Fog Computing	Data handling and network security such as the end to end data encryption, Data filtering, Data scrubbing, Event generation
4—Data Accumulation	Data in motion becomes Data at Rest, creation of database records, allowing data query, accumulation, and filtering strategies for data optimization
5—Data abstraction	Ensures quality and completeness of data, Extract, Transform, Load (ETL) functions, Data Processing, Data Comparison and reconciliation, and many types of data manipulations
6—Applications	Data interpretation, Reporting, Analytics and System Control
7—Users/Collaboration	User interaction is coordinated with all functions of the system.

Table 3. Issues and corresponding solutions of IoT applications/services.

IoT Application	Issues in Implementation	Corresponding Countermeasures
Smart Health	Handling high dimensional and weakly-structured data, Handling physical-digital ecosystems	Knowledge Discovery and Data mining, Human–Computer Interaction
Smart Agriculture	Interoperability of different standards, connectivity in rural areas, Constrained devices	Authentication and Access control, Privacy-preserving, Block-chain based solutions for data integrity, Physical countermeasures
Smart Wearable	Privacy, Security, Battery life, Connectivity, Platform standardization, design, data handling	Data management techniques, lightweight encryption, passive devices, BLE, IPv6 protocols
Smart Industry	Lack of real-time data, disparate data systems	Smart asset monitoring, enterprise IoT platform
Smart Transportation in Smart Cities	Designing Sustainable, effective, and secure transport systems, Autonomous and Connected vehicles	Mobility As A Service, Intelligent Traffic Management Solutions, Micro mobility Management
Smart Supply Chain	Optimize inventory and supply chain demands across multiple channels, Improve quality and speed in supply chain	Predictive and Prescriptive Analytics to Identify and model sales trends, Introducing internal check points in DBMS, Cryptography, and Key management.

6. Designing a Smart Healthcare Reference Architecture

IWF Architecture is a standard architectural specification from which a reference architecture for smart healthcare can be drawn analogously [70]. Thus, we designed the Smart Healthcare Reference Architecture (SHRA) based on the IWF Architecture (as shown in Figure 14). This section presents the roles and responsibilities of each layer of the designed architecture.



IWF Architecture	IoT Reference Architecture for Smart Healthcare	Actors at each Layer
Collaboration & Processes	Decision making by the doctors, patient's family members and hospital administrators in treating the patients.	Business processes for hospital administrators
Application	Building smart healthcare applications after knowledge extraction and analysis from patient's health data	Intelligent health monitoring & Services
Data Abstraction	Application of big data analytics techniques for aggregation and access of accumulated data at cloud	Knowledge extraction for timely services
Data Accumulation	Storage of patient's data at cloud	IBM Cloud, Google Cloud etc.
Edge Computing	Local pre-processing at fog layer and transfer screened data to the cloud to reduce bandwidth	Data element analysis & Transformation
Connectivity	Communication technologies which transfers data to the upper layers for storage and processing	BLE, ZigBee, Wi-Fi, IPv6, 6LoWPAN, TCP, UDP
Physical Devices & Controllers	Sensors and wearables which collects data from patients (Internet of Medical Things Devices)	Health monitoring devices of patients

Figure 14. Smart Healthcare Reference Architecture (SHRA).

6.1. Layer 1: Sensor Data of Patients

The sensors collect the data from the patients' wearables and other health monitoring IoT devices [71,72]. Here, patients with critical health conditions and elderly persons are the actors in this layer. This layer is analogous to layer 1 of the IWF Architecture with physical devices and controllers.

6.2. Layer 2: Transmission of Patient Data

Various IoT communication technologies, including Zigbee, Bluetooth Low Energy (BLE), NFC, Wi-Fi, IPv6, 6LoWPAN, TCP, and UDP, are used to transmit the collected data from patients to the upper layers for further processing [73]. This layer is analogous to layer 2 of the IWF Architecture, including connectivity technologies and protocols.

6.3. Layer 3: Transformation of Collected Data at Edge/Fog Layer

A tremendous amount of healthcare data is collected by the sensors that need to be processed. Sending this bulk data to the cloud consumes high bandwidth, resulting in ineffective computing. Thus, it is an optimal choice to process the data at the edge/fog layer [74]. Pre-processing, data element analysis, and transformation of sensor data regarding patients' health care are the primary responsibilities of this layer. These are analogous to the IWF Architecture's edge/fog computing layer.

6.4. Layer 4: Accumulation of Transformed Data to the Cloud

The preprocessed sensor data are stored in the cloud. The most popular cloud computing and storage platforms are IBM, Microsoft, Google, and AWS. At this layer, data-in-motion is converted into data-at-rest [75,76]. Filtering and selective storage techniques are applied at the cloud to store patients' data permanently. This layer is analogous to the data accumulation layer of the IWF Architecture.

6.5. Layer 5: Abstraction and Analytics of Accumulated Data

Big data analytics techniques are applied for abstraction and aggregation as a part of data analytics [77]. Knowledge extractions are performed to alert the ambulance services and doctor appointments for the patients who need immediate diagnosis and health checkups [78]. This layer is analogous to the data abstraction layer of the IWF Architecture.

6.6. Layer 6: Building Smart Healthcare Applications

Smart healthcare applications can be developed for intelligent health monitoring, and alert services are based on analytics and extracted knowledge. Some popular e-healthcare applications are glucose monitoring applications, heart rate monitoring applications, depression mood indication applications, and many more. This layer was designed to be analogous to the application layer of the IWF Architecture [79,80].

6.7. Layer 7: Collaboration of Hospital Staff

The patient's family members, doctors, and other hospital staff decide on the treatment of the patient based on application data [81]. Smart healthcare includes business modeling for hospital administrators. This layer is analogous to the collaboration and processes layer of the IWF Architecture.

7. Architectural Challenges in Designing Any Smart Healthcare Application

The IoT in smart healthcare includes emergency services, smart computing, sensors, security, remote monitoring, lab on chip, wearables, big data, and connectivity [82]. The deployment of IoT-based smart healthcare system applications such as remote patient monitoring, glucose monitoring, heart-rate monitoring, hand hygiene monitoring, depression monitoring, Parkinson's disease monitoring, connected inhalers, ingestible sensors, connected contact lenses, and robotic surgeries face many challenges [83] in real-time [84]. In this review, we have considered the top eight IoT challenges that hinder the successful land safe implementation of IoT services [85]. The challenges of IoT architectural standards concerning smart healthcare are:

1. Connectivity.
2. Data Handling.
3. Heterogeneity.
4. Interoperability.
5. Privacy.
6. Scalability.
7. Security.
8. Authentication.

7.1. IoT Connectivity in Smart Healthcare

Smart healthcare needs the connectivity and integration of multiple IoT devices that collect patient's data. A generic architecture of IoT connectivity in smart health care is presented in Figure 15. The manufacturers of the sensors and wearables uses different communication protocols and standards in the healthcare sector. Thus, the connectivity hinders the flow of transmitting the medical data for effective and timely diagnoses [86]. Wireless connectivity technologies must support the massive connectivity of IoT devices, as there are billions of connected smart devices [87]. In this paper, we have reviewed the communication protocols, and the technologies were analyzed, along with technical challenges and possible solutions based on coverage range. Short-range wireless communication technologies such as Zigbee, Bluetooth, NFC, and Wi-Fi are used in many short coverage areas. Sigfox, LoRa, LTE-M, and NB-IoT are long-range wireless network technologies with low power consumption and low data rates, which are the desirable qualities of IoT device deployment. The existing wireless IoT connectivity technologies such as short-range, LTE, 5G, Unlicensed LPWAN technologies (LoRa and Sigfox), and Licensed LPWAN technologies (LTE-M, NB-IoT) are facing many challenges in supporting the massive connectivity of IoT devices. Some of these issues are high signaling overhead, wireless resource scarcity, and inefficient wireless resource usage. Random access protocols of these existing technologies are based on ALOHA and CSMA/CA. However, these schemes do not apply to IoT devices due to their high latency, signaling overhead, and access collisions.

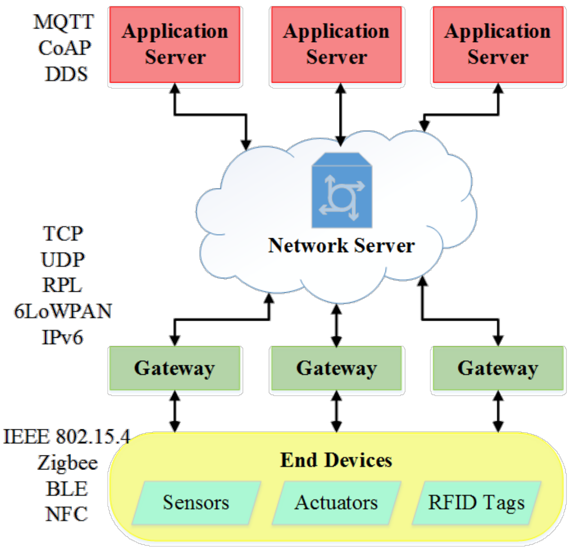


Figure 15. IoT connectivity architecture.

End IoT devices such as sensors, gateways, and RFID tags connect to gateways through protocols such as NFC, BLE, Zigbee, etc. LoRaWAN connects these gateways to the cloud network server, and this will be connected to application servers IPv6 and UDP. Application layer protocols such as MQTT and CoAP are responsible for IoT applications to get user interaction.

Four emerging technologies have been reviewed in [3], apart from the existing connectivity technologies. They are Compressive Sensing Random Access (CSRA) [88], Non-Orthogonal Multiple Access (NOMA), massive Multiple Input Multiple Output (mMIMO), machine-learning-based technologies (MLRA). These are promising technologies that can solve the shortcomings of existing technologies and enhance the efficiency of IoT devices' spectrum usage.

7.1.1. CSRA

Instead of the request–grant procedure, the grant-free RA is proposed to reduce signaling overhead. Compressive grant-free RA (cGFRA) schemes have been submitted by utilizing the sporadic traffic of MTC (machine type communication) [89]. Here, sparse sequences are used instead of binary lines to increase the amount of IoT device communication. Multiple grant-free RA (mGFRA) is another variant that uses multiple resource blocks to reduce preamble collisions. However, these GFRA schemes are highly complex algorithms, even though they are well suited for IoT devices and have lesser signaling overheads. To avoid this complexity, the following schemes are proposed.

7.1.2. NOMA

It is proven to be a promising technology by achieving wireless resource utilization [90]. The advantage of NOMA is that it allows the overlapping of signals from various devices using Power Domain Multiplexing (PDM) and Code Domain Multiplexing (CDM). Each device will undergo separate decoding using its Base Station using successive interference cancellation. It is proved that NOMA-based RA with multi-channel ALOHA is suitable for IoT device communication by allowing grant-free massive access. However, this scheme suffers from a few challenges in its implementation. Detection algorithms, decoding strategies, overloading factors, and receiver capacity are some challenges of NOMA.

7.1.3. mMIMO

To handle the heavy data traffic of 5G networks and mitigate the resource scarcity of wireless networks, many antennas are placed at the base station to realize the mMIMO system. This mMIMO based grant-free RA (mGFRA) is a promising technology for future

IoT with massive connectivity support. However, hardware costs increasing as a centralized way of gathering antennas is wrong. An alternate approach is keeping antennas around the devices distributed over a geographical area instead of base station (BS) surrounded by devices. This distributed mMIMO scheme is helpful for future IoT, but very little research has been carried out.

7.1.4. MLRA

Machine-learning-based IoT connectivity techniques have gained attention due to their capabilities of solving many IoT communication issues, including resource allocation, traffic control, and link adaption. Four machine learning algorithms are applicable for wireless connectivity, including supervised, semi-supervised, unsupervised, and reinforcement learning. IoT's dynamic wireless environments cannot be handled using optimization techniques to decide the resource allocation. Thus, ML algorithms are powerful tools for managing this. However, achieving accuracy in models is the biggest challenge in this scheme.

The advantages and disadvantages of the emerging IoT connectivity technologies can be summarized as CSRA enabling massive access but requiring high bandwidth. NOMA uses less bandwidth but suffers from a high error rate. mMIMO handles resource scarcity but reports high hardware costs. MLRA can explore dynamic patters, but it is very time consuming. This implies there is still a large research gap in IoT Connectivity technologies.

7.2. IoT Data Handling in Smart Healthcare

Smart healthcare uses different communication technologies and standards, which results in difficulties in data aggregation [91]. A tremendous amount of medical data is generated by sensors. It is extremely difficult for doctors to manage, which ultimately affects the quality of decision-making. This will eventually lead to patient safety issues [86]. A generic architecture for IoT data handling is presented in Figure 16. Physical devices, such as sensors and RFID tags, generate vast amounts of data that should be stored and processed efficiently and effectively. Many big data and analytic data techniques are employed to handle this data, but there are still some challenges in managing and utilizing massive volumes of data [92]. Traditional database management systems cannot take IoT data, as unstructured and heterogeneous massive data are produced. IoT IWF Reference Architecture layers, including the edge computing layer, data accumulation layer, and data abstraction layer, are responsible for handling IoT systems' data. Service discovery protocols such as m-DNS and DNS-SD operate at the fog level and send the patterns to the cloud. The frontend is a communication-centric and online-based platform that collects, filters, aggregates, and delivers the patterns to the back end, which is offline based. This storage-centric backend is responsible for preprocessing, storing, and analyzing the familiar patterns of the applications/service layer that result from historical and global queries. The edge computing layer is responsible for producing, processing, storing, updating, and delivering the processed patterns to the application/service layer. This application layer supports query retrieval, which can again be given to the edge computing framework for reporting the data to the interested parties. This reporting can produce real-time and localized queries [5]. Traditional database management techniques cannot be applied for IoT data management. Table 4 provides the fundamental differences between both [5].

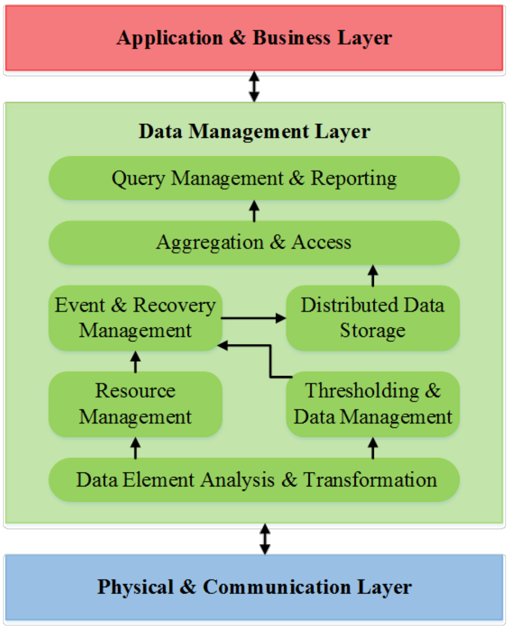

Application & Business Layer
Data Management Layer
Query Management & Reporting
Aggregation & Access
Event & Recovery Management
Distributed Data Storage
Resource Management
Thresholding & Data Management
Data Element Analysis & Transformation
Physical & Communication Layer

Figure 16. IoT data handling architecture.

Table 4. IoT protocols and respective applications.

IoT Protocols	Respective IoT Application
NFC	Payments and loyalty points, Identity Validation, Access Control, Attendance tracking, and record-keeping
BLE	Fitness trackers, Smart watches, Beacons, Medical devices, Home automation devices
Zigbee	Security systems, Light control systems, Gaming consoles, Wireless control, Industrial automation, Health care, Fire extinguishers
Wi-Fi	Mobile applications, Business applications, Smart home, Computerized applications, Automotive segment
6LoWPAN	Automation, Industrial monitoring, Smart grid, Smart home
IPV6	Net utilities (ping, ipconfig), FTP, TELNET, SMTP
LoRa WAN	Smart city, Industrial applications, Smart home applications, Smart health, Smart applications
LTE-M	Smart city services, Asset tracking, Wearable, E-Health solutions
NB-IoT	Smart metering, Facility management services, Intruder and fire alarms, Appliances measuring health parameters, Object tracking, Smart city infrastructure, Connected Industrial appliances
MQTT	Gathering sensor data, Synchronization of sensors, Monitoring health parameters via sensors, Alert messages, Facebook Messenger
CoAP	Smart energy, Building automation

The data management layer in the above architecture includes the middle three layers of IoT IWF Architecture, and Table 5 presents the responsibilities of these layers.

Table 5. Advantages and disadvantages of emerging IoT connectivity technologies.

Parameter	**Traditional Data Management**	**IoT Data Management**
Data collection	From finite sources	From a growing number of sources
Form of storage	Scalar form with strict normalized rules	Unstructured storages
Frequency of updating	Occasional updating	Continuous streaming
Maintenance of ACID properties	It can be realized easily	It's challenging to realize while executing transactions.
Data accumulation	No issues in storing static data	Problems in storing generating mobile data

Scalability and security are the significant challenges of IoT data handling. Processing and extracting the patterns based on client requirements will simplify data handling. The secured protocols must be implemented for data integrity and access control.

7.3. IoT Heterogeneity in Smart Healthcare

Smart healthcare systems comprise heterogeneous medical sensors and protocols for transmitting patient's data for decision making by doctors. These healthcare-based IoT sensors generate tremendous amounts of heterogeneous data which are difficult to be handled by the organizations [83]. IoT architectures are highly heterogeneous, as they have devices from various vendors and use various communication technologies [93]. Thus, there are many challenges in implementing IoT applications in each layer of the IWF Architecture. Some solutions for these challenges are presented below in detail [6]

7.3.1. Self-Organizing Network Topologies (Architectures and Routing Protocols)

Self-organizing network design has gained attention from researchers with its advantages of robustness and durability. MeshUp, an integrated architecture based on two mesh topologies (GPeterNet, FraNtic), is presented in [94] to interconnect heterogeneous network elements. The implementation of Safari Architecture is presented in [95], which can integrate large ad hoc networks. Safari supports the collaboration of heterogeneous networks with high data transfer and low packet overheads. Self-organizing protocols are supported by frameworks, including the distributed hash table (DHT), which can construct topology in wireless sensor networks.

7.3.2. Technology Advancements in Data Processing and Transmission

Channel allocation, energy consumption, transmission speed, and network throughput are the primary goals in designing data transmission strategies. WMN is a multi-hop network of less capacity that uses an efficient channel assignment scheme in distributed channel assignment protocols such as AODV [96]. Cooperative channel assignment protocols such as COCA solve channel optimization strategies for data transmission with less propagation delay. For IoT data transfer, TDOCP [97] is the most used protocol for applications that require high throughput.

7.3.3. Approaches to Efficient Power Supply and Energy Consumption

DADNES is a framework for reducing power consumption in the backbone network [98]. Energy-aware and QoS-aware renewable policies have been implemented in recent days.

7.3.4. Advanced Mechanisms for Ensuring Privacy and Security

The intrusion detection system mainly uses security mechanisms for heterogeneous IoT environments. MANETS provides flexible and inexpensive communication but is vulnerable to many attacks, including sleep deprivation and black hole attacks. An IDS [99] is proposed for MANETS to withstand the above attacks.

7.3.5. Modern Techniques for Decision Making and Sensing

Heterogeneous IoT solutions can be applied for each layer of the IWF model, including sensing, collecting, storing, and analyzing IoT data. A cluster-based distributed algorithm is presented in [100], a robust decision support system. Smart decision-making and sensing techniques are being invented to support heterogeneous IoT for topology construction and routing protocol designs.

7.3.6. Heterogeneous Network Elements (HNEs)

HNEs form heterogeneous IoT systems, which should solve the problems of big data integration, data transfer, self-organizing sensor network, trustworthiness, hardware design, and big data processing [100].

7.4. IoT Interoperability in Smart Healthcare

For delivering the effective services of smart healthcare, the technologies used must be interoperable with one another. The context-aware services, drug administration, semantic processing, community health monitoring, and child healthcare services need interoperability for timely diagnosis. However, achieving the interoperability is difficult to achieve [82]. There are many definitions for IoT interoperability. IEEE has defined it as, "The ability of two or more systems to exchange the information and to use this exchanged information". Achieving interoperability of IoT is a challenging issue due to multiple vendors and legacy systems [7,101]. IoT interoperability can be presented in various layered models, as shown in Table 6.

Table 6. Responsibilities of IoT data handling layers.

Fog Computing	Data Accumulation	Data Abstraction
Data filtering, clean up, aggregation, Packet content inspection, Network and data level analytics, Thresholding, Event generation	Event filtering and sampling, and comparison, Rule evaluation and aggregation, North bound/south bound altering, Event persistence in storage	Integration of multiple data formats, Maintaining consistent semantics of data, Placing data in the appropriate database, Altering high-level applications, Data virtualization, Data protection, Normalization, De-normalization, and Indexing for fast application access

Some standard approaches are proposed to handle interoperability. Adapters/gateways improve IoT devices' interoperability with different specifications and data, but the standards need a bridge to be operated collectively. IoT devices use other communication technologies and dissimilar application protocols. Gateways are dedicated hardware or embedded firmware or software with programmable logic control. A one-to-one protocol gateway has restricted complexity for "n" connected IoT devices, as given in Equation (4), and one-to-any protocol gateways are used for achieving open interoperability. Table 7 presents the interoperability layers and respective features.

$$EventualComplexity = n(n-1)/2 \tag{1}$$

Table 7. Interoperability layers and features.

Layers of IoT Interoperability Model in [102]	Layers of IoT Interoperability Model in [103]	Feature of Layer
Connection	No connection	No interoperability between systems
Communication	Technical	Basic Network connectivity
Semantic	Syntactical	Data exchanging
Dynamic	Semantic	Understanding the meaning of the data
Behavioral	Programmatic/Dynamic	Application of information
Conceptual	Conceptual	Shared view of the world

Virtual networks/overlay-based solutions are presented in [102], integrating sensors and other IP smart devices with the Internet. The Internet of Things Virtual Network (IoT-VN) [104] is the implementation of "Managed Ecosystems of Networked Objects (MENO)" for end-to-end communication using different protocols. Networking technologies, including IP-based approaches, software defined networking (SDN), network function virtualization (NFV), and fog computing technologies, each provide a high level of interoperability. Open APIs provide cross-platform and cross-domain interoperability—for example, Google Maps, YouTube, Facebook, and Amazon. To overcome API heterogeneity, the widgets written in Java Script, HTML, and CSS can be distributed on platforms that make the application of the system independent of hardware.

7.5. IoT Privacy in Smart Healthcare

Versatile privacy challenges arise in the real-time deployment of any smart healthcare applications or services. The significant privacy issues include location privacy, data privacy, resiliency, and identity threats [82]. Ensuring individual privacy is the essential requirement of IoT applications and services, as users' smart devices are connected to the Internet. There is an increased chance of stolen personal raw data with this connectivity. Widespread user adaption depends on the IoT ecosystem's privacy policies [105]. IoT device limitations and the complex heterogeneity of IoT technologies are the two primary bottlenecks hindering users' privacy. IoT devices are resource-constrained, unreliable, and operate at low data rates [106]. Many researchers have found that IoT devices as weak access points which can leak sensitive data. Thus, network-based privacy approaches are better than host-based approaches, and traditional defense systems for IoT privacy cannot serve the purpose [107]. Communication of heterogeneous technologies and devices poses challenges in designing and deploying IoT privacy policies [11]. Significant privacy challenges of IoT ecosystems are presented as:

- User identification.
- User tracking.
- Profiling.
- Utility monitoring and controlling.

Privacy preservation in the IoT environment is challenging, as there are no well-defined ecosystem boundaries. Users' data are stored only when they are highly needed. The solutions of IoT privacy preservation for these challenges are:

- Lightweight authentication.
- Device fingerprinting techniques.
- Context-aware access control.
- Edge computing software modules.
- Privacy-aware systems of user data.

- Decentralized clouds.
- Data brokers and separation algorithms.
- Denaturing frameworks.
- Data mining.
- Data summarization.

Some privacy-enhancing technologies are virtual private networks, transport layer security, DNS security extensions, onion routing, and private information retrieval. The Privacy by Design (PbD) scheme can mitigate issues arising from device limitations. Secure data communications, anonymous transmission, and data hiding are some of the practices of PbD. Privacy-enhancing techniques and Privacy by Design techniques achieve confidentiality and anonymity [10]. There are some challenges in privacy regulations of IoT, namely, privacy infringement determination, data and context quality, data transparency and minimization requirement identification, interoperability, and connectivity acknowledgments.

7.6. IoT Scalability in Smart Healthcare

Development of scalable smart healthcare applications is very challenging issue. The data collected by the medical sensors need to be stored, processed, analyzed, and further used by the hospital management system. Thus, achieving both horizontal and vertical scalability is a challenging issue in IoT-enabled smart healthcare applications [108]. IoT Scalability is the ability of the IoT devices and other technologies to adopt the changes in the IoT ecosystem and to stand the future needs. Thus, IoT technologies should handle the growth of devices, future network traffic, emerging data storage, and aggregation techniques [109–112]. There are mainly two types of scalability in IoT, namely, vertical scalability and horizontal scalability. In the first category, the system's ability is increased by adding more devices and technologies to the existing system. It consumes less power, costs less, and is easy to implement. In the second category, multiple software and hardware entities are connected to work together. Research challenges and issues of IoT scalability include protocol and network security, identity management, privacy issues, trust and governance, fault tolerance, access control, creating knowledge, and big data. Major techniques to improve IoT Scalability are given as:

- The scalability of IoT platforms can be increased by maximizing the use of edge or fog computing techniques [113].
- Usage of a software define virtual private network (SD-VPN) can improve the security and scalability of IoT networks [114].
- Scalable application design using a multi-stage approach [115]. There are emerging techniques to achieve scalability using automated bootstrapping, controlling the IoT data pipeline, a three-axis approach for scaling, a microservice architecture, multiple data storage systems, and easily expanded systems.

7.7. IoT Security in Smart Healthcare

One of the most significant challenges in smart healthcare that IoT poses is data security. IoT devices collect health-related data from patients. These devices are not fully facilitated with security credentials and protocols. Thus, the cyber criminals can hack the healthcare system and compromise personal health information (PHI) of patients. Using the retrieved information, the hackers can create fake IDs for buying drugs or medical equipment and for selling them later [116]. In addition to this, a fraudulent insurance claim can be filed [86]. Traditional security is different from IoT security in many aspects. IoT, as far as built-in security, only has lightweight algorithms for resource-constrained devices, leaving privacy issues open. IoT is a heterogeneous environment with a large attack surface, few security measures, and IoT devices located in open environments. These IoT features make the ecosystem vulnerable to attacks [117]. Data confidentiality, data integrity, and data availability are the three primary security goals of any IoT implementation. Standard IoT security mechanisms are data encryption and access control for ensuring confidentiality and data integrity algorithms for ensuring integrity, firewalls, ids, and redundancy methods for ensuring availability (CIA triad).

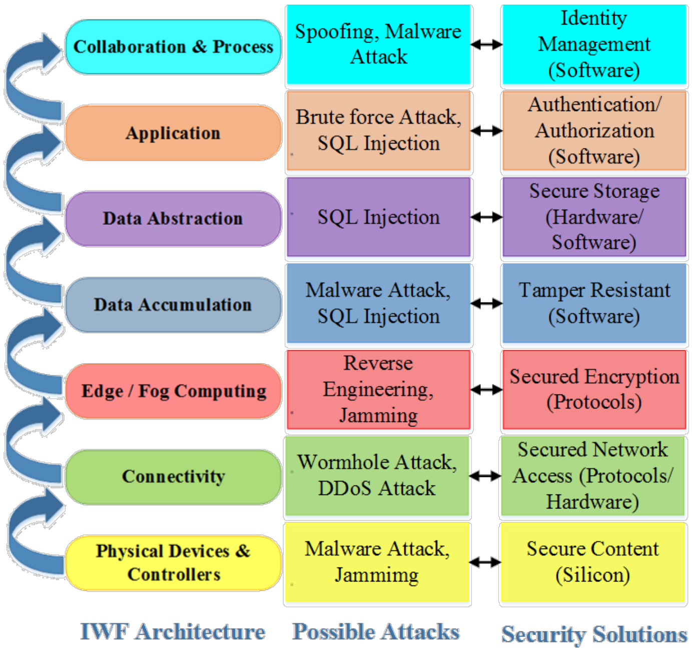

Collaboration & Process
Spoofing, Malware Attack
Identity Management (Software)
Application
Brute force Attack, SQL Injection
Authentication/ Authorization (Software)
Data Abstraction
SQL Injection
Secure Storage (Hardware/ Software)
Data Accumulation
Malware Attack, SQL Injection
Tamper Resistant (Software)
Edge / Fog Computing
Reverse Engineering, Jamming
Secured Encryption (Protocols)
Connectivity
Wormhole Attack, DDoS Attack
Secured Network Access (Protocols/ Hardware)
Physical Devices & Controllers
Malware Attack, Jammimg
Secure Content (Silicon)
IWF Architecture
Possible Attacks
Security Solutions

Figure 17. Possible attacks and respective security solutions of IWF layers.

IoT security is the major challenge due to its heterogeneity features, massive communication volume, and simple authentication or access control of physical devices [118,119]. Figure 17 depicts the possible attacks and respective security solutions of IWF layers. The Mirai botnet attack happened in 2016, a self-propagating worm targeting IoT devices that ran Linux. There are many variants of Mirai botnets that lead to distributed denial of service attacks by turning all devices into bots that are part of the network. IZIH9, Ex0, Ares, LZRD, and Miori are the major variants of Mirai that target Ethereum mining clients and Linux servers running vulnerable versions of Hadoop YARN. Much research is carried out in IoT security countermeasures for various attacks that are possible in each layer of the IWF Architecture [120]. The possible attacks and respective solutions are provided in [117] for three-layered architectures of IoT, including the perception layer, network layer, and application layer. Figure 13. presents the possible attacks and possible security solutions at each layer of the IWF Architecture. The IoT protocols are mainly classified in these layers only. IEEE 802.15.4, BLE, Wi-Fi, and LTE are perception layer protocols that use the AES-CCM algorithm; black network solutions; WEP, WPA, and WPA2 protocols; EEA; and EIA security solutions. IPv4 or IPv6, 6LoWPAN, and RPL are network layers and transport protocols that use IPSec protocols, SEND protocols of IPv6, the Compressed IPSec protocol, Compressed DTLS, 802.15.4 security features, the SVELTE IDS solution, and AES-CCM algorithms as their security solutions. MQTT and CoAP are the most used application layer protocols and use the DTLS protocol (PSK, RPK, certificates) and Lithe solution as the countermeasures of attacks [117]. IoT security through an emerging paradigm called software-defined networking (SDN) is presented in [121]. A central program called the "SDN controller" takes overall network control. This promising technology improves network performance by providing security solutions for existing challenges, including DoS attack, RFID spoofing, and sinkhole attacks. IoT Authentication is the major part of IoT security described in the subsection below.

IoT Authentication in Smart Healthcare

Smart healthcare systems require robust authentication for the patient's health information. A three-factor authentication scheme is mostly used for authenticating the users of healthcare applications. The users can be both patients and doctors [119]. IoT authentication enables secure communication between user and IoT devices, and secures data retrieval and access control. The essential requirements while designing IoT authentication schemes are lightweight security, key agreement, and mutual and multifactor authentication [14]. A user's credentials must be validated through an authenticator that uses X.509 certificates, secure session establishment, key management, monitoring, and auditing. Further communication from the user's smart device to the IoT device will be carried out using secured transmission algorithms to achieve better IoT security. Figure 18 presents the generic IoT authentication mechanisms.

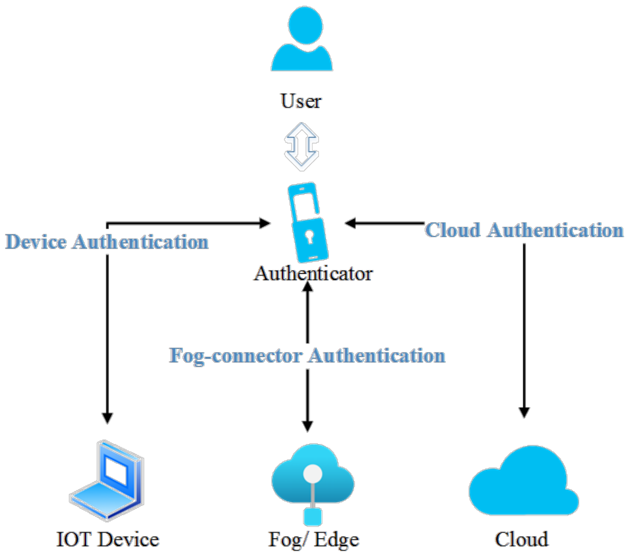


Figure 18. A generic IoT authentication mechanism.

Many authentication schemes/techniques can be applied to IoT-based architectures [14,15].

- Cloud-based IoT authentication.
- Lightweight authentication.
- Decentralized blockchain-based authentication. Blockchain technology is beneficial for storing, distributing, and verifying the authentication of any user. Access control policies are stated in the resource–requester pair as a transaction. Token-based propagation to the blockchain is done via an auditing tool.
- Bio-metrics-based Remote User Authentication: Elliptic curve pairing-based one time password (OTP) authentication schemes of IoT are presented in [122]. The public key generator (PKG) generates OTP and validation at the IoT platform, and it occurs in four phases.

  Phase 1: PKG produces 2 prime numbers, p, and q.

$$p = (2)^2 \pm c, c \leq log2n \tag{2}$$

$$q = 3(mod4) \tag{3}$$

$$p|q+1 \tag{4}$$

Equation (3) defines a super singular elliptic curve. These parameters are used to realize a lightweight algorithm.

Phase 2: IoT devices and applications obtain public and private keys (torsion points on the elliptic curve) by registering with PKG.
Phase 3: PKG at the IoT cloud generates the key of the requesting device, which acts as a torsion point.
Phase 4: Applications and devices exchange data through OTP. Later, the verification of

OTP at the device level is carried out. This method is based on the Lamport algorithm to generate OTP to achieve secure authentication.

A detailed survey on authentication techniques of the IoT ecosystem is presented in [16]. A detailed taxonomy of authentication schemes is presented in [17] based on authentication factors, use of tokens, authentication procedures, authentication architectures, IoT layers, and hardware. Analysis of IoT authentications schemes is provided for IoT applications such as smart grids, RFID and NFC-based applications, vehicular networks, smart homes, wireless sensor networks, mobile IoT networks, and some generic IoT applications. GLARM, a group-based lightweight authentication scheme, is presented in [123]. It is a simple authentication mechanism based on two stages, namely, identification and a group authentication key agreement. A novel protocol for user-server-based authentication is presented in [124]. It is a simple two-step verification scheme for IoT devices with two authentication factors called password and PUF. Speaker-to-Microphone (S2M) is a lightweight authentication protocol which can achieve distance authentication among IoT devices is presented in [125]. The implementation of a PUF-based elliptic curve algorithm for IoT devices for enrollment, authentication, and decryption is presented in [126]. The machine learning attacks are handled using the combination of physically unclonable functions (PUF) and elliptic curve cryptography (ECC). A two-way authentication protocol is presented in [127] using Datagram Transport Layer Security (DTLS) with RSA based exchange certificates.

8. Approaches of SHRA to Avoiding Each Architectural Challenge

IWF Architecture enables the easy and quick deployment of IoT applications and services. This model changes the view of IoT from conceptual to real and practical, so the realization of the IoT ecosystem will be approachable. This reference model enables the researchers to practice the countermeasures for IoT easily. The role of the IWF Architecture in facing each of the IoT challenges is presented in detail in this section.

8.1. IWF Architecture for Solving Connectivity Challenges

As mentioned for the IWF IoT Reference Architecture in Section 2, Layer 2 (connectivity layer) of the IWF model clearly defines the interconnection of IoT things through routers, switches, gateways, etc. This layer is responsible for transferring gathered data from the sensor to the upper layers for further processing. The white paper on the IWF Architecture by Cisco [128] has given a detailed view of the capabilities of the IWF Architecture in solving IoT connectivity issues by clearly defining the responsibilities and approaches. Reliable communication across different networks, efficient implementation of appropriate protocols, effective routing, protocol translation, and analyzing the network traffic are the essential responsibilities of Layer 2 of the IWF Architecture, which will help mitigate the issues of IoT connectivity.

8.2. IWF Architecture in Solving Data Handling Challenges

As mentioned in the IWF IoT Reference Architecture in Section 2, three layers of the IWF Architecture are collectively responsible for handling IoT device-generated data, namely, Layer 3 (edge computing layer), Layer 4 (data accumulation layer), and Layer 5 (data abstraction layer). The white paper on building the Internet of Things by Cisco [129] has elevated the issue that the data generated by the device are created faster than the data are accepted by the IoT applications. Another issue is the storage and processing of vast and heterogeneous data. The IWF Architecture provides data reduction in Layer 3, data accumulation in Layer 4, and data aggregation in Layer 5. These three layers solve IoT data handling issues. Layer 3 performs data filtering and cleanup, Layer 4 performs selective storing, and Layer 5 performs data reformatting to serve the client's applications.

8.3. IWF Architecture in Solving Heterogeneity Challenges

IoT heterogeneity arises from different IoT device vendors, different communication technologies, different data processing techniques, and different application areas. Some layers of the IWF Architecture can overcome the issues of heterogeneity. Layer 1 (physical layer) deals with hardware platforms and their communication technologies. This layer solves heterogeneity issues by employing interoperable technologies among these platforms. Layer 2 specifications define the self-organizing network architectures and protocols that will enable the smooth communication of heterogeneous networks. Hany F. Atlam et al. [130] reviewed the responsibilities of the IWF Architecture. Layer 5 plays the role of combining data from various heterogeneous sources. Thus, data heterogeneity can be handled by this layer of the IWF model.

8.4. IWF Architecture in Solving Interoperability Challenges

IoT system productivity increases if IoT devices and communication technologies are interoperable. However, realizing this interoperability is a major issue of IoT ecosystems. The IWF Architecture makes it easy for researchers to develop techniques to achieve IoT interoperability. The white paper on building the Internet of Things by cisco [129] has ensured application interoperability via the IWF Architecture. This model can also provide legacy compatibility by interoperating with existing legacy IoT applications and services.

8.5. IWF Architecture in Solving Privacy Challenges

Each layer of the IWF model outputs the privacy solutions for IoT applications and services. Layer 1 defines Privacy by Design schemes and some authentication and access control policies. Layer 2 defines encryption and an IP Sec secured channel to ensure privacy in connectivity. Layer 3 defines secured communication through some protocols and encryption techniques. Layer 4 uses tamper-resistant software while accumulating data. Layer 5 provides secure abstraction techniques by either software or hardware platforms. Layer 6 includes privacy through authentication and authorization techniques. Layer 7 provides identity management software techniques for privacy preservation of business processes. Hany F. Atlama et al. [86] presented the privacy-preserving mechanisms of Layer 6 and Layer 7 of the IWF Architecture. Privacy protection is employed for securing users' application and analytic information.

8.6. IWF Architecture in Solving Scalability Challenges

IoT ecosystems' scalability-enhancing techniques can be implemented through different layers of the IWF model. Scalable IoT systems are designed by developing standard APIs for web and mobile applications that will be dealt with in Layer 6. Designing dynamic data storage and analytics systems in Layers 4 and 5 will result in scalable IoT platforms. IoT infrastructure becomes more scalable if the communication stack from the end devices to the cloud is made asynchronous. Maximizing the usage of edge or fog computing will result in scalable IoT applications with a minimal computational overhead at Layer 3. Distributed systems offer great scalability and high availability by adding more servers at Layers 2, 3, and 4. Concurrency and parallelism increase the horizontal scalability of the IoT ecosystem that can be employed in all layers of the IWF model. The white paper on building the Internet of Things by Cisco [129] presented a complete IoT system in the IWF Architecture. All layers provide scalability and agility by decoupling capability.

8.7. IWF Architecture in Solving Security Challenges

Security mitigation in IoT systems is encompassed in all layers of the IWF model. IoT security mechanisms such as authentication, encryption, trust management, and secure routing are implemented in various layers [131]. Authentication techniques are applied in Layers 1, 2, 6, and 7. Encryption techniques are used to achieve end-to-end security at Layers 1 and 2 of the IWF model, in the form of lightweight cryptography. User revocation support is provided by encryption at Layer 7. Trust management focuses on eliminating malicious nodes in the network, which is implemented in Layer 2 of the IWF model. Secure routing aims to withstand security breaches of transmission of IoT device-generated data. Route optimization protocols, secure trust-aware routing protocols, and efficient protocols to mitigate the attacks on IoT systems will be designed for Layers 1, 2, and 3 of the IWF Architecture. Hany F. Atlama et al. [86] have presented the security capabilities of all layers of the IWF Architecture. Layer 1 enables lightweight encryption for providing sensor data. Layer 2 allows identity authentication for secure routing. Layers 3, 4, and 5 provide secure edge and cloud computing, along with secure storage mechanisms. Layers 6 and 7 ensure authentication and key agreement.

IoT Authentication and the Role of the IWF Model in Solving These Issues

IoT authentication mechanisms are generally employed in Layer 6 and Layer 7 of the IWF model. Identity authentication is used in Layer 2. Infrastructure protocols such as Zigbee and Zwave; and application protocols such as MQTT and DDS, support authentication by default, which will be employed in Layers 1 and 2, and Layers 6 and 7 of the IWF model, respectively. IoT's lightweight authentication schemes will provide sensor authentication at Layer 1, key establishment-based authentication at Layer 2, and secure and effective user authentication at Layer 7. Hany F. Atlama et al. [86] have presented the role of the IWF Architecture in providing the authentication capability of the IoT ecosystem. The lower layers ensure identity authentication, and the uppermost layers provide authentication with the key agreement. These authentication mechanisms must be employed to deliver a safe IoT system.

9. Significance of Smart Healthcare during COVID-19 Pandemic

Coronavirus disease (COVID-19) is an infectious disease caused by SARS-CoV-2. The statistics have shown that approximately 300 million cases and 5.5 million deaths have been registered to date. To control the spread of SARS-CoV-2 and reduce COVID-19, the strategies such as contract tracing, telemedicine, and the Internet clinic are expedited. Smart healthcare facilitated more significant support in monitoring the remote patients during COVID-19 quarantine. With the deployment of smart health applications, efficient and effective health monitoring can be enabled through remote communication of COVID-19 symptoms for doctors' assistance and diagnosis. The primary symptoms of COVID-19 are cough, fever, headache, myalgia, sore throat, breathing difficulty, diarrhea, etc. Prescriptions can be drawn by remotely interpreting the severity of a patient's symptoms. Thus, smart healthcare services are beneficial during the pandemic to improve the standard of living for COVID-19 patients. Physical devices such as sensors (pulse sensor), Arduino boards (Arduino Uno), and gateways (Bluetooth module) collect the data from COVID-19 patients. In addition, the wearables such as COVID-19 smart bracelets can detect some of the symptoms and collect the data. Communication technologies such as Wi-Fi and Bluetooth can transmit collected data for diagnosis. Mobile applications or web applications are used for data visualizations by doctors and alert generation for patients. The results can be seen in the respective health management applications. The usage of smart healthcare applications and their services has seen a drastic increment during the COVID-19 pandemic. The adaption of digital health technologies increased from 19% in 2018 to 57% in 2021 after the pandemic. Medical 4.0 is the fourth medical revolution representing the extensive utilization of intelligent healthcare applications through the Internet of Medical Things. COVID-19 pandemic needs the comprehensive utilization of IoT and AI-enabled smart devices. Medical 4.0 will adequately handle the ongoing and upcoming situation of the COVID-19 pandemic [132].

During the post-pandemic period, the patients need not to physically attend the clinical trial sites, and the diagnosis can be carried out remotely to prevent any further spread of COVID-19. In future, we will develop a clear protocol and flow using SHRA framework for designing any smart healthcare application that is useful for post-pandemic situations.

10. Discussions

The discussions on the open research issues of this review are presented in this section. IoT devices are lightweight devices, and powerful techniques and algorithms that are applicable for overcoming the IoT challenges, were discussed by Petar Radanliev et al. [133]. Research gaps in authentication schemes are reviewed in [16], such as poor transport encryption, password limitations, faulty or complex IoT systems, financial implications, insecure interfaces, faulty authorization schemes, and flaws in firmware and software. Emerging connectivity technologies such as CS, NOMA, mMIMO, and ML-based random access also face challenges and possible research directions [3]. The IoT data handling techniques, including optimal data collection algorithms, data storage, and data processing, are requirements for managing massive data [5]. For handling heterogeneity, distributed nodes, data transfer interfaces, secure algorithms, DRM, and big data processing techniques are the solutions for the large-scale processing of IoT data [6]. Popular IoT interoperability approaches, including adapters, virtual gateways, and semantic web technologies, are discussed in the paper [8]. Privacy-preserving techniques of each layer of the IWF model, including data encryption and network virtualization, have some future challenges that need to be solved [10]. Some future challenges need to be considered using automated bootstrapping, controlling IoT data pipelining, and developing microservices architecture to handle IoT scalability [12]. Significant challenges arise in designing IoT security solutions, including hash-based encryption, lightweight cryptography, and some risk assessment techniques [13]. In the future, these algorithms as countermeasures must be designed and developed with less complexity to be suitable for IoT ecosystems. For attaining robust IoT security, building trust, reputation, and autonomy are the major challenges. Giancarlo Fortino et al. [134] have presented state-of-art approaches for achieving trust and reputation in IoT environments. The authors have presented several techniques for building trust in IoT using the social networking context, fuzzy techniques, cooperative approaches, and identity-based approaches. The emerging research challenges in achieving trust in IoT were also summarized by the authors. The authors have also presented a comparative study of the emerging IoT architectures and their applicability in modeling trust in IoT environments. Enrico Corradini et al. [135] have proposed a two-tier blockchain framework for ensuring autonomy and protection in IoT networks. Trust, reliability, and reputation are guaranteed with trust computation using smart contracts. The cyber risks on IoT networks were quantified and discussed by Petar Radanliev et al. [136].

We have designed an SHRA and discussed the responsibilities of each layer. The essence of smart healthcare in the COVID-19 pandemic was discussed, as the pandemic has dramatically increased the use of telemedicine, which involves the use of digital channels to provide care. The presented SHRA architecture could be used as a reference in the future for designing any smart healthcare application. The intelligent medical care can adopt SHRA for realizing the automation of smart hospitals in future during post-pandemic circumstances.

11. Conclusions

This review presents the standard IoT architectures, along with their advantages and disadvantages. After the analysis, it was concluded that IWF Architecture is the best for designing a reference architecture for any IoT-based application. We have discussed the IoT protocol stack of the IWF Architecture and their roles and responsibilities. We have presented the importance of smart healthcare and designed the Smart Healthcare Reference Architecture (SHRA) based on the IWF Architecture. The IoT challenges in the real-time deployment of SHRA are addressed and elaborated. The role of the IWF Architecture in solving the mentioned challenges of SHRA is discussed. Finally, a brief introduction on the significance of smart healthcare during the COVID-19 pandemic is presented in this review. This systematic investigation provides the optimal details and discussions for the formulated research questions.

Author Contributions: Conceptualization, A.D.A. and E.S.B.; methodology, A.D.A. and E.S.B.; formal analysis, A.D.A. and E.S.B.; data curation, A.D.A. and E.S.B.; writing—original draft preparation, A.D.A. and E.S.B.; writing—review and editing, S.R.N., A.S. and A.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research has received no external funding.

Informed Consent Statement: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shancang, L.; Li, X.D.; Shanshan, Z. The Internet of Things: A survey. *Inf. Syst. Front.* **2015**, *17*, 243–259.
2. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of things(iot): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
3. Ding, J.; Nemati, M.; Ranaweera, C.; Choi, J. IoT Connectivity Technologies and Applications: A Survey. *arXiv* **2020**, arXiv:2002.12646v1.
4. IoT-A. *Converged Architectural Reference Model for the IoT v2.0*; SAP: Zurich, Switzerland, 2012.
5. Abu-Elkheir, M.; Hayajneh, M.; Ali, N.A. Data Management for the Internet of Things: Design Primitives and Solution. *Sensors* **2013**, *13*, 15582–15612. [CrossRef]
6. Qiu, T.; Chen, N.; Li, K.; Atiquzzaman, M.; Zhao, W. How Can Heterogeneous Internet of Things Build Our Future: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2011–2027. [CrossRef]
7. Haseeb, S.; Hashim, A.H.A.; Khalifa, O.O.; Ismail, A.F. Connectivity, Interoperability and Manageability Challenges in Internet of Things. *AIP Conf. Proc.* **2017**, *1883*, 020004. [CrossRef]
8. Ait Abdelouahid, R.; Chhiba, L.; Marzak, A.; Mamouni, A.; Sael, N. IoT Interoperability Architectures: Comparative Study. In Proceedings of the First International Conference on Real Time Intelligent Systems, Casablanca, Morocco, 18–20 October 2017; Springer: Cham, Switzerland, 2017; pp. 209–215. [CrossRef]
9. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mob. Netw. Appl.* **2019**, *24*, 796–809. [CrossRef]
10. Weber, R.H. Internet of Things: Privacy Issues Revisited. *Comput. Law Secur. Rev.* **2015**, *31*, 618–627. [CrossRef]
11. Seliem, M.; Elgazzar, K.; Khalil, K. Towards Privacy Preserving IoT Environments: A Survey. *Hindawi Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1032761. [CrossRef]
12. Gupta, A.; Christie, R.; Manjula, R. Scalability in Internet of Things: Features, Techniques and Research Challenges. *Int. J. Comput. Intell. Res.* **2017**, *13*, 1617–1627.
13. Sadique, K.M.; Rahmani, R.; Johannesson, P. Towards Security on Internet of Things: Applications and Challenges in Technology. *Procedia Comput. Sci.* **2018**, *141*, 199–206. [CrossRef]
14. Kavianpour, S.; Shanmugam, B.; Azam, S.; Zamani, M.; Narayana Samy, G.; De Boer, F. A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices. *J. Comput. Netw. Commun.* **2019**, *2019*, 5747136.
15. Trnka, M.; Cerny, T.; Stickney, N. Survey of Authentication and Authorization for the Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*, 4351603. [CrossRef]
16. Atwady, Y.; Hammoudeh, M. A Survey on Authentication Techniques for the Internet of Things. In Proceedings of the International Conference on Future Networks and Distributed Systems ICFNDS'17, Cambridge, UK, 19–20 July 2017. [CrossRef]
17. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
18. Capra, M.; Bussolino, B.; Marchisio, A.; Shafique, M.; Masera, G.; Martina, M. An Updated Survey of Efficient Hardware Architectures for Accelerating Deep Convolutional Neural Networks. *Future Internet* **2020**, *12*, 113. [CrossRef]
19. Alabdan, R. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet* **2020**, *12*, 168. [CrossRef]
20. Ghazal, T.M.; Hasan, M.K.; Alshurideh, M.T.; Alzoubi, H.M.; Ahmad, M.; Akbar, S.S.; Al Kurdi, B.; Akour, I.A. IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review. *Future Internet* **2021**, *13*, 218. [CrossRef]
21. Available online: https://libguides.umn.edu/systematicreviews (accessed on 26 July 2022).
22. Gill, A.Q.; Behbood, V.; Ramadan-Jradi, R.; Beydoun, G. IoT architectural concerns: A systematic review. In Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing (ICC'17), Cambridge, UK, 22–23 March 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1–9. [CrossRef]
23. Adrianto, D.; Lin, F.J. Analysis of security protocols and cor-responding cipher suites in ETSI M2M standards. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 777–782. [CrossRef]
24. Chen, H.C.; You, I.; Weng, C.E.; Cheng, C.H.; Huang, Y.F. A security gateway application for End-to-End M2M communications. *Comput. Stand. Interfaces* **2016**, *44*, 85–93. [CrossRef]
25. Joachim, W.W. Internet-of-Things Architecture IoTA Project Deliverable D1.2-Initial Architectural Reference Model for IoT. Available online: https://cocoa.ethz.ch/downloads/2014/01/1360_D1%202_Initial_architectural_reference_model_for_IoT.pdf (accessed on 26 July 2022).

26. Saad, M.; Soomro, T.R. Cyber Security Andinternet of Things. *Pak. J. Eng. Technol. Sci.* **2017**, *7*. [CrossRef]
27. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [CrossRef]
28. Romdhani, I.; Abdmeziem, R. Architecting the Internet of Things: State of the Art. *Robot. Sens. Clouds* **2015**, *36*, 55–75.
29. Amaral, L.A. Middleware Technology for IoT Systems:Challenges and Perspectives Toward 5G. *Internet Things (IoT) 5G Mob. Technol.* **2016**, *8*, 333–367. [CrossRef]
30. Ungurean, I. A middleware based architecture for the industrialinternet of things. *KSII Trans. Internet Inf. Syst. (TIIS)* **2016**, *10*, 2874–2891. [CrossRef]
31. Xiao, L.; Xiao, N.; Li, M.; Xie, S.; Hou, K.; Li, Y. Architecture and Implementation of IoT Middlewarefor Ground Support Systems in Launch Site. In Proceedings of the 2020 International Conference on Sensing, Measurement & Data Analytics in the Era of Artificial Intelligence (ICSMD), Xi'an, China, 15–17 October 2020. [CrossRef]
32. Mesmoudi, Y.; Lamnaour, M.; El Khamlichi, Y.; Tahiri, A.; Touhafi, A.; Braeken, A. A Middleware based on Service Oriented Architec-ture for Heterogeneity Issues within the Internet of Things (MSOAH-IoT). *J. King Saud Univ.-Comput. Inf. Sci.* **2020**, *32*, 1108–1116. [CrossRef]
33. Mishra, S.K.; Sarkar, A. Service-oriented architecture for internet of things: A semantic approach. *J. King Saud Univ.-Comput. Inf. Sci.* 2021, *in press*. [CrossRef]
34. Lan, L.; Li, F.; Wang, B.; Zhang, L.; Shi, R. An Event-Driven Service-Oriented Architecture for the Internet of Things. In Proceedings of the 2014 Asia-Pacific Services Computing Conference, Fuzhou, China, 4–6 December 2014. [CrossRef]
35. Abd Rahim, M.R.; Rashid, R.A.; Rateb, A.M.; Sarijari, M.A.; Abdullah, A.S.; Hamid, A.H.F.A.; Sayuti, H.; Fisal, N. Service-Oriented Architecturefor IoT Home Area Networking in 5G. *Fundam. Requir. Enabling Technol. Oper. Manag.* **2018**, 577–602. [CrossRef]
36. Antao, L.; Pinto, R.; Reis, J.; Gonçalves, G. Requirements for Testing and Validating the IndustrialInternet of Things. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Västerås, Sweden, 9–13 April 2018. [CrossRef]
37. Liu, X.; Lam, K.H.; Zhu, K.; Zheng, C.; Li, X.; Du, Y.; Liu, C.; Pong, P.W.T. Overview of Spintronic Sensors, Internet of Things, and Smart Living (2016). *IEEE Trans. Magn.* **2019**, *55*, 1–22.
38. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)–When social networks meet the Internet of Things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
39. Cauteruccio, F.; Cinelli, L.; Fortino, G.; Savaglio, C.; Terracina, G.; Ursino, D.; Virgili, L. An approach to compute the scope of a social object in a Multi-IoT scenario. *Pervasive Mob. Comput.* **2020**, *67*, 101223. [CrossRef]
40. Ursino, D.; Virgili, L. Humanizing IoT: Defining the Profile and the Reliability of a Thing in a Multi-IoT Scenario. In *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*; Springer: Cham, Switzerland, 2020. [CrossRef]
41. Cauteruccio, F.; Cinelli, L.; Corradini, E.; Terracina, G.; Ursino, D.; Virgili, L.; Savaglio, C.; Liotta, A.; Fortino, G. A framework for anomaly detection and classification in Multiple IoT scenarios. *Future Gener. Comput. Syst.* **2021**, *114*, 322–335. [CrossRef]
42. Hakim, A.E. Internet of Things (IoT) System Architecture and Technologies. *White Pap.* **2018**, *10*, 2. [CrossRef]
43. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017. [CrossRef]
44. Heđi, I.; Špeh, I.; Šarabok, A. IoT network protocols com-parison for the purpose of IoT constrained networks. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017. [CrossRef]
45. Sharma, S.; Kumar, S. A Review on IoT:Protocols, Architecture, Technologies, Application and Research Chal-lenges. In Proceedings of the 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 29–31 January 2020. [CrossRef]
46. Geng, H. Networking protocols and standardsfor internet of things. In *Internet of Things and Data Analytics Handbook*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2016. [CrossRef]
47. Mishra, B. The Use of MQTT in M2M and IoT Systems: A Survey. *IEEE Access* **2020**, *8*, 201071–201086. [CrossRef]
48. Wang, H. A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices. *IEEE Access* **2017**, *5*, 16393–16405. [CrossRef]
49. Nikolov, N. Research of MQTT, CoAP, HTTP and XMPP IoT communication protocols for embedded system. In Proceedings of the 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020. [CrossRef]
50. Uy, N.Q.; Nam, V.H. A comparison of AMQP and MQTT protocols forInternet of Things. In Proceedings of the 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 12–13 December 2019. [CrossRef]
51. Naik, N. Choice of effective messaging protocols for IoT systems:MQTT, CoAP, AMQP and HTTP. In Proceedings of the 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria, 11–13 October 2017. [CrossRef]
52. Coetzee, L.; Oosthuizen, D.; Mkhize, B. An Analysis ofCoAP as Transport in an Internet of Things Environment. In Proceedings of the 2018 IST-Africa Week Conference (IST-Africa), Gaborone, Botswana, 9–11 May 2018.
53. Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016. [CrossRef]

54. Alaerjan, A.; Kim, D.K.; Al Kafaf, D. Modeling functionalbehaviors of DDS. In Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA, USA, 4–8 August 2017. [CrossRef]
55. Ho, M.H.; Yen, H.C.; Lai, M.Y.; Liu, Y.T. Imple-mentation of DDS Cloud Platform for Real-time Data Acquisition of Sensors. In Proceedings of the 2021 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Hualien City, Taiwan, 16–19 November 2021. [CrossRef]
56. Jara, A.J.; Martinez-Julia, P.; Skarmeta, A. Light-Weight Multicast DNS and DNS-SD (lmDNS-SD): IPv6-Based Resource and Service Discovery for the Web of Things. In Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Palermo, Italy, 4–6 July 2012. [CrossRef]
57. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
58. Achir, M.; Abdelli, A.; Mokdad, L. A taxonomy of service discovery approaches in IoT. In Proceedings of the 2020 8th International Conference on Wireless Networks and Mobile Communications (WINCOM), Reims, France, 27–29 October 2020. [CrossRef]
59. Purnama, B.; Budiarto, R.; Stiawan, D.; Hanapi, D. Monitoring Connectivity of In-ternet of Things Device on Zigbee Protocol. In Proceedings of the 2018 International Conference on Electrical Engineering and Computer Science (ICECOS), Pangkal, Indonesia, 2–4 October 2018. [CrossRef]
60. Chandan, A.R.; Khairnar, V.D. Bluetooth Low Energy(BLE) Crackdown Using IoT. In Proceedings of the 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 11–12 July 2018. [CrossRef]
61. Vagdevi, P.; Nagaraj, D.; Prasad, G.V. Home: IOT based homeautomation using NFC. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017. [CrossRef]
62. *802.15.4-2015*; IEEE Standard for Low-Rate Wireless Networks. IEEE: Piscataway Township, NJ, USA, 22 April 2016. 978-1-5044-0845-5. [CrossRef]
63. Geng, H. IPv6 for IoT and gatewa. In *Internet of Things and Data Analytics Handbook*; Wiley: New York, NY, USA, 2016. ISBN 978-1-119-17364-9. [CrossRef]
64. McGee, K.; Collier, M. 6LoWPAN Forwarding Techniques for IoT. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019. [CrossRef]
65. Mahmud, M.A.; Abdelgawad, A.; Yelamarthi, K. Improved RPL for IoT Applications. In Proceedings of the 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), Windsor, ON, Canada, 5–8 August 2018. [CrossRef]
66. Masirap, M.; Amaran, M.H.; Yussoff, Y.M.; Ab Rahman, R.; Hashim, H. Evaluation of reliable UDP-based transport protocols for Internet of Things (IoT). In Proceedings of the 2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Penang, Malaysia, 30–31 May 2016. [CrossRef]
67. Porkodi, R.; Bhuvaneswari, V. The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. In Proceedings of the 2014 International Conference on Intelligent Computing Applications, Coimbatore, India, 6–7 March 2014. [CrossRef]
68. Giri, A.; Dutta, S.; Neogy, S.; Dahal, K.; Pervez, Z. Internet of things (IoT): A survey on architecture, enabling technologies, applications and challenges. In Proceedings of the 1st International Conference on Internet of Things and Machine Learning (IML '17), Liverpool, UK, 17–18 October 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1–12. [CrossRef]
69. Khanna, A.; Kaur, S. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wirel. Pers. Commun.* **2020**, *114*, 1687–1762. [CrossRef]
70. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
71. Choi, J.; Choi, C.; Kim, S.; Ko, H. Medical Information Protection Frameworks for Smart Healthcare based on IoT. In Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics, Seoul, Korea, 26–28 June 2019. [CrossRef]
72. Ahmed, S.; Ilyas, M.; Raja, M.Y.A. Internet of Things: Applications in Smart Healthcare. In Proceedings of the 9th International Conference on Society and Information Technology (IICSIT 2018), Orlando, FL, USA, 13–16 March 2018; pp. 19–24.
73. Ahad, A.; Tahir, M.; Yau, K.L.A. 5G-Based Smart Healthcare Network: Architecture, Tax-onomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]
74. Khaloufi, H.; Abouelmehdi, K.; Beni-Hssane, A. Fog Computing for Smart Healthcare data Analytics: An Urgent Necessity. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 31 March–2 April 2020. [CrossRef]
75. Ma, X.; Wang, Z.; Zhou, S.; Wen, H.; Zhang, Y. Intelligent Healthcare Systems Assisted by Data Analyticsand Mobile Computing. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018. [CrossRef]
76. Ullah, A.; Azeem, M.; Ashraf, H.; Alaboudi, A.A.; Humayun, M.; Jhanjhi, N.Z. Secure Healthcare Data Aggregation and Transmission inIoT—A Survey. *IEEE Access* **2021**, *9*, 16849–16865. [CrossRef]
77. Lytras, M.D.; Chui, K.T.; Visvizi, A. Data Analytics in Smart Healthcare: The RecentDevelopments and Beyond. *Appl. Sci.* **2019**, *9*, 2812. [CrossRef]

78. Tian, S.; Yang, W.; Le Grange, J.M.; Wang, P.; Huang, W.; Ye, Z. Smart healthcare: Making medical care more intelligent. *Glob. Health J.* **2019**, *3*, 62–65. [CrossRef]
79. Thakare, V.; Khire, G. Role of Emerging Technology for Building Smart Hospital Information System. *Procedia Econ. Financ.* **2014**, *11*, 583–588. [CrossRef]
80. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
81. Udo, I.J.; Ekpenyong, M.E. Improving Emergency Healthcare Response using Real-Time Collaborative Technology. In Proceedings of the 2020 4th International Conference on Medical and Health Informatics, Kamakura City, Japan, 14–16 August 2020. [CrossRef]
82. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health. *IEEE Consum. Electron. Mag.* **2017**, *7*, 18–28. [CrossRef]
83. Khodkari, H.; Maghrebi, S.G.; Asosheh, A.; Hosseinzadeh, M. Smart Healthcare and Quality of Service Challenges. In Proceedings of the 2018 9th Inter-national Symposium on Telecommunications (IST), Tehran, Iran, 17–19 December 2018; pp. 253–257. [CrossRef]
84. Abdullah, H.; Jalil, S.Z.A.; Sarip, S.; Izhar, M.A.M.; Bani, N.A. Internet of things devices and issues in iot system development for healthcare. *Turk. J. Physiother. Rehabil.* **2021**, *32*, 2.
85. Saleem, J.; Hammoudeh, M.; Raza, U.; Adebisi, B.; Ande, R. IoT standardisation: challenges, perspectivesand solution. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18), Amman, Jordan, 26–27 June 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–9. [CrossRef]
86. Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In *Digital Twin Technologies and Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 123–149. [CrossRef]
87. Ahad, A.; Tahir, M.; Aman Sheikh, M.; Ahmed, K.I.; Mughees, A.; Numani, A. Technologies Trend towards 5G Network for SmartHealth-Care Using IoT: A Review. *Sensors* **2020**, *20*, 4047. [CrossRef] [PubMed]
88. Schlegel, C.; Kempter, R.; Kota, P. A novel random wireless packet multiple access method using cdma. *IEEE Trans. Wirel. Commun.* **2006**, *5*, 1362–1370. [CrossRef]
89. Choi, J.; Yu, N.Y. Compressive channel division multiple access for mtc under frequency-selective fading. *IEEE Trans. Commun.* **2017**, *65*, 2715–2725. [CrossRef]
90. Lv, T.; Ma, Y.; Zeng, J.; Mathiopoulos, P.T. Millimeter-wave noma transmission in cellular m2m communications for internet of things. *IEEE Internet Things J.* **2018**, *5*, 1989–2000. [CrossRef]
91. Osorio, C.A.C.; Echeverry, G.A.I.; Ossa, L.F.C.; Bedoya, O.H.F. Computational architecture of IoT data analytics for connected homebased on deep learning. In Proceedings of the 10th Euro-American Conference on Telematics and Information Systems (EATIS '20), Aveiro, Portugal, 25–27 November 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–8. [CrossRef]
92. Dorj, U.O.; Lee, M.; Choi, J.Y.; Lee, Y.K.; Jeong, G. The Intelligent Healthcare Data ManagementSystem Using Nanosensors. *J. Sens.* **2017**, *2017*, 7483075. [CrossRef]
93. Kazmi, A.; Jan, Z.; Zappa, A.; Serrano, M. Overcoming the Heterogeneity in the Internet ofThings for Smart Cities. In Proceedings of the International Workshop on Interoperability and Open-Source Solutions, Stuttgart, Germany, 7 November 2016; Springer: Cham, Switzerland, 2016. [CrossRef]
94. Ghosh, S.; Basu, K.; Das, S.K. 'MeshUp': Self-organizing meshbased topologies for next generation radio access networks. *Ad Hoc Netw.* **2007**, *5*, 652–679. [CrossRef]
95. Du, S.; Khan, A.; PalChaudhuri, S.; Post, A.; Saha, A.K.; Druschel, P.; Johnson, D.B.; Riedi, R. Safari: A self-organizing, hierarchical architecture for scalable ad hoc networking. *Ad Hoc Netw.* **2008**, *6*, 485–507. [CrossRef]
96. Gong, M.X.; Midkiff, S.F.; Mao, S. On-demand routing and channel assignment in multi-channel mobile ad hoc networks. *Ad Hoc Netw.* **2009**, *7*, 63–78. [CrossRef]
97. Jiang, H.; Zhou, C.; Wu, L.; Wang, H.; Lu, Z.; Ma, L.; Li, Y. TDOCP: A two-dimensional optimization integrating channel assignment and power control for large-scale WLANs with dense users. *Ad Hoc Netw.* **2015**, *26*, 114–127. [CrossRef]
98. Patota, F.; Chiaraviglio, L.; Bella, F.; Deriu, V.; Fortunato, S.; Cuomo, F. DAFNES: A distributed algorithm for network energy saving based on stress-centrality. *Comput. Netw.* **2016**, *94*, 263–284. [CrossRef]
99. Raza, S.; Wallgren, L.; Voigt, T. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2661–2674. [CrossRef]
100. Li, S.; Oikonomou, G.; Tryfonas, T.; Chen, T.M.; Xu, L.D. A distributed consensus algorithm for decision making in serviceoriented Internet of Things. *IEEE Trans. Ind. Informat.* **2014**, *10*, 1461–1468.
101. Khan, W.A.; Hussain, M.; Latif, K.; Afzal, M.; Ahmad, F.; Lee, S. Process Interoperability in Healthcare Systemswith Dynamic Semantic Web Services. *Computing* **2013**, *95*, 837–862. [CrossRef]
102. Hoebeke, J.; De Poorter, E.; Bouckaert, S.; Moerman, I.; Demeester, P. Managed ecosystems of networked objects. *Wirel. Pers.Commun.* **2011**, *58*, 125–143. [CrossRef]
103. Tolk, A. Composable mission spaces and M&S repositories–applicability of open standards. In *Spring Simulation Interoperability Workshop*; Springer: Arlington, VA, USA, 2004.

104. Ishaq, I.; Hoebeke, J.; Moerman, I.; Demeester, P. Internet of things virtual networks: bringing network virtualization to constrained devices. In Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Besancon, France, 20–23 November 2012.
105. Ahmed, S.M.; Rajput, A. Threats to patients' privacy in smart healthcareenvironment. In *Innovation in Health Informatics*; Academic Press: Cambridge, MA, USA, 2020. [CrossRef]
106. Ranjith, J.; Mahantesh, K. Privacy and Security issues in Smart HealthCare. In Proceedings of the 2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, 13–14 December 2019. [CrossRef]
107. Masood, I.; Wang, Y.; Daud, A.; Aljohani, N.R.; Dawood, H. Towards Smart Healthcare: Patient Data Pri-vacy and Security in Sensor-Cloud Infrastructure Survey. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 2143897. [CrossRef]
108. Sharma, C.; Sunanda, D. Survey on Smart Healthcare: An Application of IoT. *Int. J. Emerg. Technol.* **2017**, *8*, 330–333.
109. Gia, T.N.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fault Tolerant and Scalable IoT-based Architecturefor Health Monitoring. In Proceedings of the 2015 IEEE Sensors Applications Symposium (SAS), Zadar, Croatia, 13–15 April 2015. [CrossRef]
110. Kalid, N.; Zaidan, A.A.; Zaidan, B.B.; Salman, O.H.; Hashim, M.; Muzammil, H.J.J.O.M.S. Based Real Time Remote Health Monitoring Systems: A Review on Patients Prioritization and Related "Big Data" UsingBody Sensors information and Communication Technology. *J. Med. Syst.* **2018**, *42*, 1–30. [CrossRef]
111. Borujeni, A.M.; Fathy, M.; Mozayani, N. A hierarchical, scalable architecture for areal-time monitoring system for an electrocardiography, using context-aware computing. *J. Biomed. Inform.* **2019**, *96*, 103251. [CrossRef] [PubMed]
112. Alabdulatif, A.; Khalil, I.; Yi, X.; Guizani, M. Secure Edge of Things for Smart Healthcare Surveillance Framework. *IEEE Access* **2019**, *7*, 31010–31021. [CrossRef]
113. Tseng, C.-L.; Lin, F.J. Extending scalability of IoT/M2M platforms with Fog computing. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018. [CrossRef]
114. Shif, L.; Wang, F. Improvement of security and scalability for IoT network using SD-VPN. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018. [CrossRef]
115. Venkatesh, J.; Aksanli, B. Scalable-Application Design for the IoT. *IEEE Softw.* **2017**, *34*, 62–70. [CrossRef]
116. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats?: A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
117. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating Critical Security Issues of the IoTWorld: Present and Future Challenges. *IEEE Internet Things J.* **2018**, *5*, 2483–2495. [CrossRef]
118. Lu, Y.; Sinnott, R.O. Security and privacy solutions forsmart healthcare systems. In *Innovation in Health Informatics*; Academic Press: Cambridge, MA, USA, 2020. [CrossRef]
119. Karunarathne, S.M.; Saxena, N.; Khan, M.K. Security and Privacy in IoT SmartHealthcare. *IEEE Internet Comput.* **2021**, *25*, 37–48. [CrossRef]
120. Wheelus, C.; Zhu, X. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. *IoT* **2020**, *1*, 259–285. [CrossRef]
121. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Abbas, Y. An In-Depth Analysis of IoT Security Requirements, Challenges and their Countermeasures via Software Defined Security. *IEEE Internet Things J.* **2020**, *7*, 10250–10276. [CrossRef]
122. Shivraj, V.L.; Rajan, M.A.; Singh, M.; Balamuralidhar, P. One timepassword authentication scheme based on elliptic curves for internet of things (iot). In Proceedings of the 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 17–19 February 2015; pp. 1–6.
123. Lai, C.; Lu, R.; Zheng, D.; Li, H.; Shen, X.S. GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Comput. Netw.* **2016**, *99*, 66–81. [CrossRef]
124. Aman, M.N.; Chua, K.C.; Sikdar, B. Mutual Authentication in IoT Systems Using Physical Unclonable Functions. *IEEE Internet Things J.* **2017**, *4*, 1327–1340. [CrossRef]
125. Chen, D.; Zhang, N.; Qin, Z.; Mao, X.; Qin, Z.; Shen, X.; Li, X. S2M: A Lightweight Acoustic Fingerprintsbased Wireless Device Authentication Protocol. *IEEE Internet Things J.* **2016**, *4*, 88–100. [CrossRef]
126. Wallrabenstein, J.R. Practical and Secure IoT Device Authentication Using Physical Unclonable Functions. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016.
127. Kothmayr, T.; Schmitt, C.; Hu,W.; Brünig, M.; Carle, G. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2710–2723. [CrossRef]
128. DRAFT–Controlled Distribution, White Paper, The Internet of Things Reference Model, © 2014 Cisco and/or its affiliates. All Rights Reserved. Available online: https://dl.icdst.org/pdfs/files4/0f1d1327c5195d1922175dd77878b9fb.pdf (accessed on 26 July 2022).
129. Building the Internet of Things, White Paper, © 2013 Cisco and/or Its Affiliates. All Rights Reserved. Available online: https://www.cisco.com (accessed on 26 July 2022).
130. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. *Adv. Comput.* **2019**, *115*, 1–39. [CrossRef]
131. Noor, M.b.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]

132. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access* **2020**, *8*, 118433–118471. [CrossRef]
133. Radanliev, P.; De Roure, D. Review of Algorithms for Artificial Intelligence on Low Memory Devices. *IEEE Access* **2021**, *9*, 109986–109993. [CrossRef]
134. Fortino, G.; Fotia, L.; Messina, F.; Rosaci, D.; Sarné, G.M. Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges. *IEEE Access* **2020**, *8*, 60117–60125. [CrossRef]
135. Corradini, E.; Nicolazzo, S.; Nocera, A.; Ursino, D.; Virgili, L. Increasing protection and autonomy in the IoT through a two-tier blockchain framework. In *CEUR Workshop Proceedings*; Sun SITE Central Europe: Aachen, Germany, 2021.
136. Radanliev, P.; De Roure, D.; Burnap, P.; Santos, O. Epistemological Equation for Analysing Uncontrollable States in Complex Systems: Quantifying Cyber Risks from the Internet of Things. *Rev. Socionetwork Strateg.* **2021**, *15*, 381–411. [CrossRef]