Journal of Autonomous Intelligence (2023) Volume 6 Issue 2
doi: 10.32629/jai.v6i2.588

ORIGINAL RESEARCH ARTICLE

Heterogeneity issues in IoT-driven devices and services

Shashi Kant Gupta[1,*], Radha Raman Chandan[2], Rupesh Shukla[3], Prabhdeep Singh[4], Ashish Kumar Pandey[5], Amit Kumar Jaiswal[6]

[1] *Computer Science and Engineering, Eudoxia Research University, New Castle, DE 19720, USA*

[2] *Department of Computer Science, School of Management Sciences (SMS), Varanasi 221011, India*

[3] *ILVA Commerce and Science College, Sneh Nagar Behind Lotus Showroom, Indore 452008, India*

[4] *School of Computer Applications, BBD University, Lucknow 226028, India*

[5] *Computer Science and Engineering, Dr. Ram Manohar Lohia Avadh University, Ayodhya 224001, India*

[6] *Computer Science and Engineering, Chandigarh University, Punjab 800001, India*

*** Corresponding author:** Shashi Kant Gupta, raj2008enator@gmail.com

ABSTRACT

Internet of Things (IoT), which connects billions of devices and services to the Internet, is viewed as the future industrial and intellectual revolution in technology. These connected devices are available in a variety of types. Different technologies and standards use various protocols to interact with each other. Due to these difficulties with heterogeneity, the application of IoT on a broad scale is difficult. This inspired us to identify the problems from the literature and offer solutions to solve the IoT scalability problem. This study is based on the systematic literature review (SLR) to identify the diverse problems and their solutions. We chose 81 primary sources in total. We found 14 distinct IoT heterogeneity concerns after extracting and interpreting the data. The following issues have been noted as potential obstacles: heterogeneity in data formats, heterogeneity of devices, heterogeneity in communication, and interoperability difficulty because of heterogeneity. From the perspectives of digital libraries and timeframes, the stated challenges have been addressed. Additionally, we have discovered 81 solutions in total for these problems, with at least 5 different answers for every issue. In the future, we will use a multi-criteria decision-making issue to classify the problems and evaluate the solutions.

Keywords: Internet of Things (IoT); heterogeneity challenges; multi-criteria decision-making; interoperability issue; systematic literature review (SLR)

ARTICLE INFO

Received: 12 April 2023
Accepted: 7 July 2023
Available online: 1 August 2023

1. Introduction

The term "IoT" refers to devices that can communicate with the network but are not often assumed to have an internet connection. Therefore, the IoT is a system of devices that communicate with one another. Smart home automation is a term used to describe a system that keeps tabs on and/or manages aspects of a home's infrastructure, such as its lighting, temperature, entertainment systems, and appliances. The system may be operated via a ceiling terminal, a tablet or desktop computer, a mobile phone app, or a Web interface that may be accessed remotely via the Internet[1]. Smart home gadgets have been available for decades, and they are seen as one of the most promising realizations of the IoT since they allow users to conduct activities involving a wide variety of devices in the house with no effort and no need for complex configuration or bespoke programming[2]. There are many network-enabled devices in today's homes, but there are few applications that can coordinate these devices to accomplish a single task. Furthermore,

the absence of dominant standards for IoT communication, control, and data management has led to the proliferation of highly fragmented smart home systems, with proprietary solutions provided by each device vendor. This means that to get the most out of their smart home gadgets, customers either have to use a variety of different control interfaces (such as smartphone applications) or stick with equipment from a single manufacturer[3]. The IoT can be used in all aspects of human existence, including health, smart homes, smart cities, energy, and logistics. IoT users are in a new era of physical contact in which everything around us may be connected to the internet at any time and from anywhere. Heterogeneity refers to the fact that we communicate with IoT devices through a variety of service providers, but each request demands a different application[4]. To avoid future issues, all devices or defined devices should be incorporated into a single protocol type, allowing them to be controlled by any Android app. The high degree of heterogeneous heterogeneity is one of the primary challenges that IoT faces. Different communication protocols, technology, and hardware are used by different devices. One of the primary problems to be addressed while establishing and integrating new IoT ecosystems is interoperability. Interoperability issues can reduce the IoT's benefits by up to 40%. Interoperability in the IoT refers to the capacity of two components or systems to share and utilize data with one another. Interoperability can be created at multiple levels in the IoT context, such as protocol interoperability and data interoperability. Protocol interoperability refers to the ability to connect multiple network technologies directly[5].

The IoT's heterogeneity in terms of methods, device file formats, device connectivity, capabilities, equipment, etc., is one of its major drawbacks. These kinds of difficulties are why the IoT has only seen limited deployments thus far. These barriers must be eliminated on several fronts for IoT to reach its goal of worldwide adoption. Devices need Internet access to activate and perform the service. The existing methods taken and/or applied by different studies for addressing heterogeneity in IoT systems need to be emphasized, and the identification of heterogeneity-based difficulties that occur at different levels is required.

1.1. The motivation for the study

The term IoT is used to describe the growth of current Internet services toward the eventual goal of providing connection to every physical object on Earth. As a result, IoT has become the most widely used in the world. It is a new technology that is still being developed, and everyone is attempting to interpret it to suit their requirements. Application and understanding of IoT are faced with significant difficulties related to security, virtualization, and heterogeneity. The multidimensional issue of heterogeneity prevents the IoT concept from being implemented on a wide scale. These difficulties are the reason why IoT system deployments have only been partially realized up to this point. To identify these IoT heterogeneity concerns and their solutions, we conducted a thorough literature study. This study also contributes by undertaking a complete assessment of such challenges utilizing the chi-square test depending on online collections and timeframe.

1.2. The objective of the study

- This research aims to perform a comprehensive literature review to identify these IoT heterogeneity concerns, as well as to discover the methods applied by various studies to address these issues.
- The value of this research is that it will identify and analyze problems created by heterogeneity in IoT systems, as well as present an overview of previous research that has implemented various ways to deal with heterogeneity.
- A further important contribution is that it will point academics in the right direction as they work to improve the standalone design with the end goal of meeting heterogeneity concerns at various tiers of IoT systems.
- As a result of this, IoT solutions are applicable and implementable in a broad variety of industries.

The following outline constitutes the organization of this paper: In Section 2, a literature overview of the history, problems, and heterogeneity issues of the IoT is presented. In Section 3, we will discuss the research approach that was applied to accomplish the aims of this study. In Section 4, the findings and a discussion of the issues presented by heterogeneity in IoT are presented, as are the solutions to those challenges that were identified in this study. This study comes to a close in Section 5, which also makes some recommendations for further research.

2. Literature review

Due to the vastness and complexity of the IoT, there is no one, agreed-upon definition that applies to all users everywhere. A digital innovation specialist was the first to use and define the term "IoT". Since then, several academics, practitioners, academics, developers, and entrepreneurs have characterized the IoT in their own words. Huang et al.[6] present a stochastic optimization problem for the combined admission control and computation resource allocation in the Mobile edge computing (MEC) enabled small cell network (SCN). The objective is to combine throughput and fairness while limiting the queue to optimize system value. They split the original issue into three separate issues that may be resolved on a distributed basis without the need for system statistics. Chen et al.[7] suggest a hybrid energy supply paradigm that involves incorporating energy harvesting technologies into IoT devices. Together, they improve the system's local processing, offloading window, and edge computing decisions to lower the overall system's cost. They use optimization theory to develop a novel online method for offloading dynamic tasks from MEC using a hybrid energy supply, which they call dynamic task offloading for mobile edge computing (DTOME). DTOME may decide which tasks to offload by balancing system cost and queue stability. To find the best task-offloading method, we use dynamic programming theory. The efficacy of DTOME is confirmed by simulation findings, which also demonstrate that DTOME has a lower system cost than two standard task offloading schemes.

A new area of study[8] called heterogeneous IoT (HetIoT) has the potential to significantly alter both how we now comprehend basic computer science concepts and how we live in the future. One of the most crucial challenges for sensor hubs is energy efficiency. This research suggests a work scheduling system for sensor hubs to address this issue and increase their energy efficiency[9]. The design of a multi-queue-based framework is provided, together with its theoretical model and related mathematical studies. A strategy for scheduling tasks in sensor hubs that consume the least amount of energy is suggested by improving the model using Lyapunov optimization techniques. Cloud gaming is suggested as a possible method for enabling users to play any games by streaming video game scenes that have been remotely produced in the cloud. However, it has significant problems with a long latency and a large amount of network capacity. To do this, a novel architecture called EdgeGame is suggested to enhance the cloud gaming experience by utilizing edge resources. In contrast to other cloud gaming platforms, EdgeGame offloads computation-heavy rendering to the network edge, which can significantly reduce network latency and bandwidth use[10].

The researcher presents a method[11], learning-based edge caching method to allow for reciprocal collaboration across several edge servers with constrained cache resources, effectively lowering the latency of information delivery. Particularly, they characterize the NP-hard cooperation information storage optimization model. They develop a brand-new learning-based cooperative caching technique with three essential parts to address this issue. To accurately forecast content popularity, a temporal convolution network-driven prediction model is first created. To optimize the content caching value (CCV) overall, a unique dynamic programming algorithm is created. To better understand the relevant tool, technology, and technique and to support developer needs, this literature reviews[12] IoT-oriented designs. The given designs either directly or indirectly suggest developing and implementing potent IoT concepts to address real-world issues. They offer a SecEdge-Learn Infrastructure that employs supervised learning and applies the theory to generate a safe MEC setting. Finally, we talk about the MEC environment's importance to the industry[13].

The goal of this study[14] conducted is to hasten the uptake of sophisticated digital signatures. They fill the gap between the recently developed, highly theoretical digital signatures used in papers with a cryptographic focus and the actual IoT systems. It helps researchers increase security, privacy, and certain special functional elements. Noting that quality of service (QoS) and security are not matters to be taken lightly, they stress the importance of researching these topics together to cut down on diversity (or vice versa). To do this, they first discuss relevant and plausible use cases to inspire more study into QoS and security as a whole to bring homogeneity to the control plane of Software-defined networks (SDNs) for the Internet of Things. Second, they put forth a paradigm that effectively converts n groups of homogeneous controllers from heterogeneous controllers. The SDN controller's reaction time serves as the primary measurement in our observation and analysis. Following that, a proof of concept (PoC) in a hypothetical SDN ecosystem is provided to verify our technique using the mathematical model. The suggested architecture greatly reduces heterogeneity, which contributes to maintaining QoS and enhancing security, according to performance assessment results[15].

Constrained IoT device demand is predicted to rise, and this issue is projected to increase in the future. As a result, the IoT will need to better integrate a lot of limited devices. In this work, we employed SLR to detect heterogeneity concerns and present an outline of the solutions taken to address those obstacles.

3. Methodology

With the use of a systematic literature review (SLR), we've been able to pinpoint the challenges caused by heterogeneity in IoT systems that are preventing the realization of a world-spanning IoT vision and locating workable solutions.

3.1. Study queries

Creating study questions is the first stage in performing a systematic literature review. The study queries (SQ), are categorized and presented below.

SQ 1: Which difficulties are associated with the heterogeneous IoT in the existing literature?

SQ 2: In the research on heterogeneous IoT, what kinds of solutions have been proposed for the problems that have been identified?

3.2. Query properties

Searching for applicable studies is the second step in a systematic literature review. It was determined which online libraries were used for the initial work. "IEEE Xplore, Google Scholar, ScienceDirect, SpringerLink, and ACM". Finally, search strings were created and employed to assemble recent literature for the study. **Table 1** is provided possible query properties.

Table 1. Query properties.

Context	Sources	Query properties
IoT heterogeneity	Google Scholar	("Heterogeneous IoT") and ("issues or challenges")
	SpringerLink	("IoT") and ("heterogeneity") and ("challenges")
	IEEE Explore	"Heterogeneous" and ("IoT" or "Internet of Things") and "challenges"
	ACM	("IoT") and ("heterogenous") and ("challenges")
	ScienceDirect	("IoT" or "Internet of Things") and ("heterogenous") and ("challenges")

3.3. Study selection

The method of choosing a study topic involves searching digital libraries using a tollgate approach while considering the search strings into consideration. A collection of articles employing the tollgate techniques are shown in **Figure 1**.

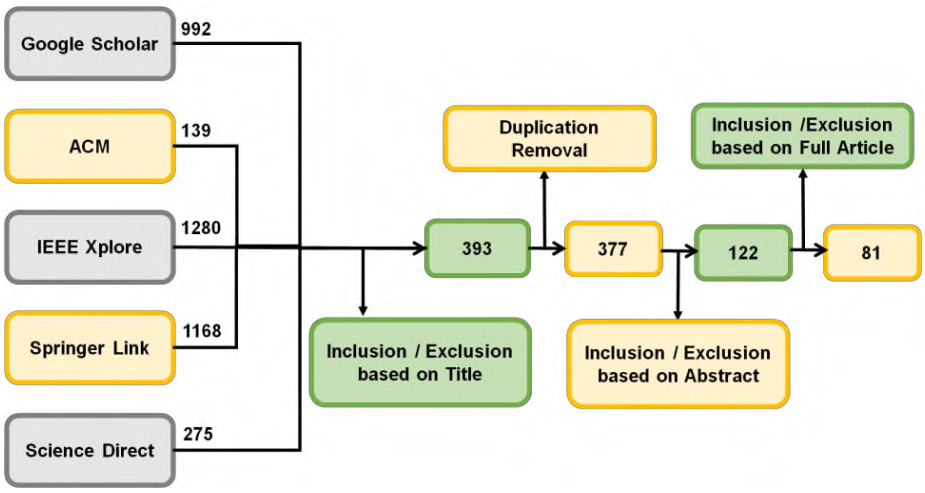

Figure 1. Articles selected using the tollgate system.

As part of the snowball effect, we evaluated and examined the content of nine articles published in journals and presented at conferences. In the beginning, 3854 papers were identified by using a search methodology on the chosen digital libraries. Keywords, titles, duplication elimination, abstracts, and full texts of chosen publications were used in a selection procedure. We didn't include these types of papers in the assessment:

- Research that has appeared in settings apart from traditional academic publications, patents, and technical reports.
- Studies that haven't been published in English.
- Research done before 2010.
- Research that does not fit the predetermined criteria.

We used the following criteria to determine the overall quality of the articles we included in our study. **Figures 2** and **3** provide a synopsis of both digital library selection and yearly paper selection.

- Any difficulty resulting from the diverse nature of the IoT is addressed in this report.
- The research provides an unmistakable answer to the problem of heterogeneity.
- The article comes from a reputable and respected journal.

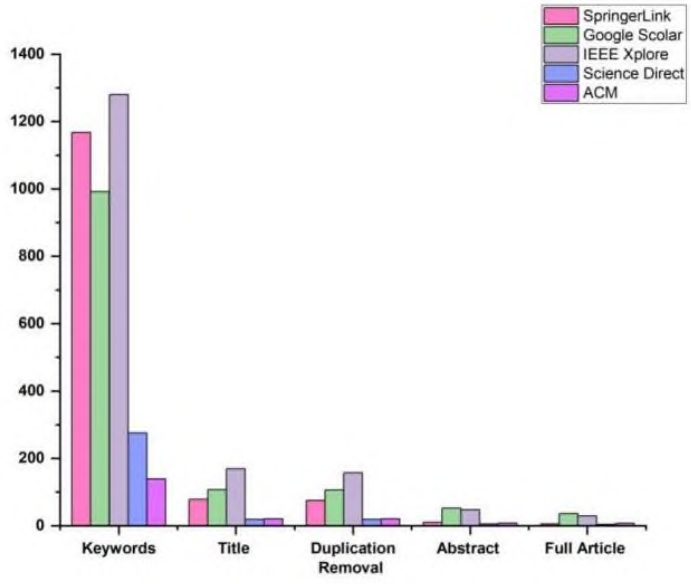

Figure 2. Article selection based on digital libraries.

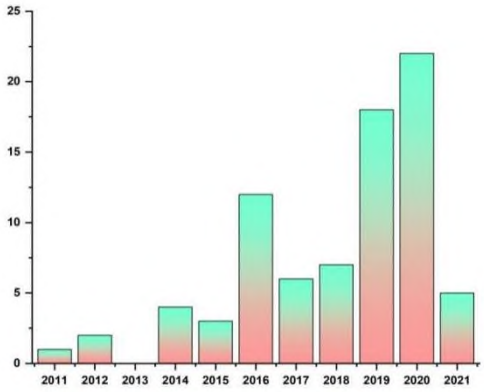

Figure 3. Article selection based on every year.

3.4. Statistical analysis

The linear chi-square test was utilized for correlation in this investigation.

3.4.1. Chi-square test

A statistical test known as the chi-squared test can be used to determine whether detectable variance in the collection of category data is unpredictable. It looks at whether the frequency analysis of particular events collected matches a statistical model. All options must be unique and also have an aggregate value. Because all of the occurrences get a category collected data, it is a regular occurrence.

It is a generalization to believe that a regular 6 die is "just". Pearson's chi-squared evaluation examines the efficiency, uniformity, and then dependability of 3 pairs of associations.

A simple test that determines if an observed frequency analysis varies from the analytical probability. A regularity test analyses the range of data across various factions using the same category variable.

Independent assessment helps determine whether two components' measured values, as shown in a categorical variable, have been self-sufficient of each other.

$$Pearson'schi - squaredtest = \sum_{i=1}^{q} \frac{(D_i - M_i)^2}{i}$$

where,

D_i = measurements of type i,

D = sum of measurements,

M = predicted count of type i,

q = amount of cells.

Without addressing them, the situation would be dire. Predicted chi-square numbers are discovered using the following formula:

$$H = \frac{n_h \times m_v}{m}$$

where,

H = following its productivity,

n_h = connotes the lateral border of a row of nuclei in a cell,

m_v = represents the population as a whole represented by the sample,

m = cell's row boundary.

For every unit, the overall response rate is divided by a combination of the row's margin as well as the margin of the column.

$$x = \frac{(B-K)^2}{K}$$

Quantitative assessments of the strength of a link may be found in statistical analyses of correlations. Cramer's *H* is the most used measure of Chi-squared significance. Applying the following equation, the process is straightforward:

$$\sqrt{\frac{x^2/B}{(l-1)}} = \sqrt{\frac{x^2}{B(l-1)}}$$

The chi-square is a method of evaluating data and understanding the structure of data.

4. Analysis and discussion

In this section, we have analyzed the results that are most relevant to our SQs. We used a linear chi-square test of association to analyze the data. When both the predictor and result variables contain categorical values, the chi-square test is preferred over alternative statistical tests. In response to SQ1, problems and key concerns that were discovered during the SLR are shown in **Table 2**. We have discovered that heterogeneity problems showed significant differences.

Table 2. Issues discovered by SLR.

#	Issues	%	*f*	Articles ID
1	Management and configuration of devices	18	13	AiD11, AiD14, AiD16, AiD30, AiD33, AiD34, AiD35, AiD36, AiD37, AiD54, AiD61, AiD62
2	Interoperability issue	22	16	AiD5, AiD9, AiD23, AiD27, AiD30, AiD37, AiD51, AiD59, AiD65, AiD66, AiD67, AiD68, AiD69, AiD70, AiD71, AiD72
3	Communication between heterogeneous devices	21	15	AiD3, AiD7, AiD10, AiD18, AiD28, AiD29, AiD30, AiD31, AiD32, AiD33, AiD47, AiD50, AiD53, AiD69, AiD71
4	Heterogeneity in standards, platform	14	10	AiD1, AiD34, AiD36, AiD56, AiD57, AiD58, AiD59, AiD60, AiD66, AiD72
5	Heterogeneity of devices issues	49	35	AiD21, AiD22, AiD23, AiD24, AiD25, AiD26, AiD27, AiD28, AiD45, AiD46, AiD47, AiD50, AiD51, AiD56, AiD57, AiD58, AiD62, AiD63, AiD65, AiD68, AiD70, AiD71, AiD72, AiD77
6	Communication security	22	16	AiD19, AiD23, AiD31, AiD32, AiD35, AiD43, AiD44, AiD47, AiD48, AiD49, AiD50, AiD51, AiD52, AiD53, AiD54, AiD55
7	Heterogeneous communication issues	36	26	AiD28, AiD29, AiD49, AiD57, AiD58, AiD61, AiD62, AiD64, AiD65, AiD68, AiD70, AiD72, AiD73, AiD75, AiD80, AiD81
8	Fragmentation in connectivity, protocols	10	14	AiD4, AiD2, AiD4, AiD5, AiD36, AiD54, AiD60, AiD66, AiD74, AiD78
9	Management of networks	8	6	AiD8, AiD11, AiD13, AiD14, AiD15, AiD16
10	Heterogeneous data/data formats	36	26	AiD36, AiD38, AiD39, AiD40, AiD41, AiD42, AiD57, AiD58, AiD62, AiD64, AiD65, AiD68, AiD69, AiD70, AiD72, AiD79
11	Diversity in network technologies	13	9	AiD3, AiD6, AiD7, AiD8, AiD9, AiD10, AiD46, AiD54, AiD63
12	Data security	12	17	AiD23, AiD31, AiD43, AiD44, AiD45, AiD46, AiD49, AiD52, AiD53, AiD76, AiD77
13	Integration of devices and data	14	20	AiD12, AiD18, AiD21, AiD23, AiD38, AiD41, AiD53, AiD56, AiD60, AiD61, AiD62, AiD63, AiD64, AiD65
14	Device security	20	14	AiD8, AiD19, AiD23, AiD24, AiD31, AiD43, AiD48, AiD49, AiD52, AiD53, AiD54, AiD55, AiD67

4.1. Challenges are compared based on the timeframe

The analysis of the highlighted difficulties according to the timeline is shown in **Table 3**. Two timeframes, Timeframe I from 2010 to 2015 and Timeframe II from 2016 to 2021—have been created to separate the length.

We found the following as a result of the analysis: as demonstrated in **Table 3**, heterogeneity in communication is crucial in Timeframe I, which runs from 2010 to 2015.

- Device heterogeneity is essential in Timeframes I and II.
- Data formats must be heterogeneous in Timeframe I and Timeframe II.

Table 3. Time-based summary of the issues.

Issues	**Timeframe I**		**Timeframe II**		**Chi-square test, $\alpha = 0.05$**	
	%	***f***	**%**	***f***	***p***	x^2
Management and configuration of devices	13	3	17	10	0.5769	0.3112
Interoperability issue	22	5	19	11	0.9257	0.0086
Communication between heterogeneous devices	17	4	19	11	0.7669	0.0878
Heterogeneity in standards, platform	13	3	12	7	0.9901	0.0001
Heterogeneity of devices	57	13	38	22	0.8052	0.3695
Communication security	13	3	22	13	0.3192	0.9920
Heterogeneous communication issues	35	8	31	18	0.9478	0.0042
Fragmentation in connectivity, protocols	9	2	14	8	0.4831	0.4918
Management of networks	13	3	5	3	0.2902	1.1185
Heterogeneous data/data formats	35	8	31	18	0.9478	0.0042
Diversity in network technologies	22	5	7	4	0.0972	2.7502
Data security	9	2	17	10	0.3078	1.0399
Integration of devices and data	26	6	14	8	0.3015	1.0677
Device security	9	2	20	12	0.1951	1.6784

4.2. Comparison of issues with digital libraries

The study of the issues based on digital libraries is depicted in **Table 4**. As digital libraries, we have Google Scholar, IEEE Xplore, SpringerLink, ScienceDirect, and ACM. We found the following as a result of the analysis:

(1) Communication heterogeneity is crucial in Google Scholar and SpringerLink.
(2) Device heterogeneity in Google Scholar, IEEE Xplore, and SpringerLink is crucial.
(3) Data formats in ScienceDirect, SpringerLink, and IEEE Xplore must be heterogeneous.
(4) ACM and SpringerLink must address the key interoperability issue.

Table 4. A collection of issues associated with digital libraries.

Heterogeneity in standards, platform	19	7	1	14	2	1	14	1	0	0	3.4381	0.0640
Heterogeneity of devices issues	44	16	100	5	34	10	29	2	100	5	1.6342	0.2011
Communication security	22	8	0	0	17	5	14	1	-	-	-	-
Heterogeneous communication issues	33	12	40	2	24	7	14	1	40	2	0.3876	0.5336
Fragmentation in connectivity, protocols	14	5	1	14	21	6	29	2	0	0	4.1393	0.0419
Management of networks	8	3	0	0	10	3	0	0	0	0	1.6683	0.1965
Heterogeneous data/data formats	25	9	40	2	34	10	29	2	-	-	-	-
Diversity in network technologies	11	4	1	0	17	4	0	0	20	1	1.6701	0.1962
Data security	11	4	0	0	10	3	0	0	0	0	1.9809	0.1593
Integration of devices and data	17	6	20	1	14	5	14	1	0	0	1.0421	0.3073
Device security	14	5	0	0	21	6	14	1	0	0	1.3884	0.2387

4.3. Proposed solutions

Table 5 offers solutions to the issues described to respond to SQ2. We have discovered 81 solutions in all, with three different answers for each of the issues.

Table 5. Proposed solutions.

Issue	Ref	Year of publishing	Approach	Proposed solutions
Management and configuration of devices	[16]	2019	Platform	Using an intuitive interface, M4DN.IoT is a platform for managing IoT networks.
	[17]	2016	Framework	Utilizing an open standard for IoT communication protocol, EC-IoT (COAP).
	[18]	2020	Framework	A framework for IoT device decentralized identification and access management is called DIAM-IoT.
Interoperability issue	[19]	2018	Framework	SHIOT is an ontology-based SDN architecture that uses SDN controllers.
	[20]	2019	Platform	Decentralized IoT platform with a new edge, fog, and cloud computing capabilities.
	[21]	2014	Framework	An easy-to-use, middleware-free framework for interoperability monitoring.
Communication between heterogeneous devices	[22]	2018	Architecture	Utilizing a multimodal approach and a range of heterogeneous wireless networks.
	[23]	2020	Protocol	To provide secure inter-device communication, a lightweight security protocol based on symmetric keys should be developed.
	[24]	2018	Architecture	An IoT access control system that is entirely decentralized and built on the blockchain technology architecture.
Heterogeneity in standards, platform	[25]	2018	Method	Intelligent governance strategy for managing heterogeneous IoT systems.
	[26]	2021	Platform	For addressing interoperability barriers across diverse IoT systems, there is a federated platform called Data Spine.
	[27]	2017	Model	Generic driver injection is a strategy for creating mobile apps that may be used in many contexts and middleware.
Heterogeneity of devices	[28]	2014	Architecture	Cognitive skills paired with architecture that promotes informed decision-making and automates service development.
	[29]	2020	Middleware	Cuttlefish is a lightweight, flexible middleware that provides standardized APIs for creating applications that may run on a wide variety of devices.
	[30]	2020	Mechanism	Mechanism using SPARQL queries for transparent IoT device discovery and access.
Communication security	[31]	2019	Protocol	Using a multigroup important management protocol is the best way to guarantee network security, data privacy both upstream and downstream, and resilience against collision threats.
	[32]	2020	Protocol	Using proxy re-signature, a heterogeneous system authentication approach that protects the privacy.
	[33]	2015	Algorithms	Algorithms for elliptic curve cryptography (ECC) that are optimized for NXP/Jennic JN5148-based devices.
Heterogeneous communication issues	[34]	2016	Proposed system	A dependable and adaptable IoT access control solution is TACIoT.
	[35]	2020	Framework	Computing as part of an expertise architecture for supporting diverse IoT network topologies.
	[36]	2021	Algorithm	Based on both optimization and game theory, a distributed online optimization technique. The system makes decisions on how to distribute processing resources, manage battery power, and offload a variety of activities online.
Fragmentation in connectivity, protocols	[37]	2016	Platform	SPOT, a platform for smartphones that uses XML-based open device driver models.
	[38]	2019	Protocol	Concurrent routing technique based on physical layer technology.
	[39]	2020	Mechanism	Based on a dependable 5G network, a new roaming mechanism for the LoRaWAN protocol.
Management of networks	[40]	2016	Architecture	Combining methods to present management that are direct and indirect.
	[41]	2020	Model	A dictionary of services is used in the message-based communication architecture to facilitate communication between servers and devices.
	[42]	2014	Architecture	Adding SDN multilayer IoT controller to the multi-network information architecture (MINA) middleware.

Table 5. (*Continued*)

Issue	Ref	Year of publishing	Approach	Proposed solutions
Heterogeneous data/data formats	[43]	2016	Framework	Using the ideas of the semantic web and linked data, SIGHTED is a framework.
	[44]	2011	Framework	An innovative system for managing heterogeneous sea-cloud-based data called SeaCloudDM.
	[45]	2020	Architecture	The software infrastructure of the IoT is designed to process and evaluate data from a wide variety of sources with a wide variety of topologies.
Diversity in network technologies	[46]	2011	Framework	To directly link the devices that are associated with one another, use the IDRA reconfigurable network architecture.
	[47]	2017	Middleware	Mobile gateway powered by smartphones that offer a flexible and open interface for connecting devices to the Internet.
	[48]	2020	Proposed system	Using IoT devices, a decentralized cloud platform built on the blockchain may be used to create complicated network edge services.
Data security	[49]	2021	Framework	Architecture for Trusted Multiparty Computation in Device Data Verification.
	[50]	2020	Proposed system	Users have the option to subscribe to and unsubscribe from data.
	[51]	2016	Model	Safe data storage methods to protect the privacy and reliability of Internet of Things information.
Integration of devices and data	[52]	2019	Proposed system	A cutting-edge plug-and-play system called SensPnP integrates hardware and firmware.
	[53]	2015	Proposed system	A method based on managing device dispersion across gateways and utilizing web service delegation.
	[54]	2016	Architecture	Integration of data from many, potentially unreliable, sources, such as government databases, is enabled by the architecture we've developed.
Device security	[55]	2019	Proposed system	An original, lightweight identification and based consensus mechanism for the IoT heterogeneous components.
	[56]	2018	Algorithm	Algorithm for authenticating and authorizing network nodes based on ECC.
	[57]	2021	Framework	The MECshield framework uses mobile edge computing (MEC) to block distributed denial of service attacks.

5. Conclusion and future scope

This evaluation was conducted with a methodical approach that systematically selected studies that dealt with the challenges brought on by heterogeneous IoT. There was a total of 81 research publications from various online archives published between 2010 and 2021 that were selected for this study. This period was split into two periods for examination. Both span the years 2010 through 2010 and 2017 through 2021, respectively. For the sake of implementing IoT on a broad scale, we have highlighted 14 main heterogeneity problems in this SLR. The most serious challenges are those that occur more frequently than 30% of the time. In this work, we examine the timing and incidence of such issues using digital libraries. In our investigation, we discovered that several problems were more pressing in the older than in the more recent timeframe.

Additionally, we learned that certain difficulties exist at both times. We found at least five solutions for each of those problems once we had identified the problems. **Table 5** is a summary of those responses. In a further study, we want to apply a multi-criteria decision-making problem to better categorize the concerns and assess the efficacy of the proposed remedies.

Author contributions

Conceptualization, SKG and RRC; methodology, SKG; software, RRC; validation, RS, PS and AKP; formal analysis, AKJ; investigation, AKP; resources, AKJ; data curation, PS; writing—original draft preparation, SKG; writing—review and editing, SKG; visualization, RRC; supervision, RRC; project administration, SKG.

Conflict of interest

The authors declare no conflict of interest.

Reference

1. Nord JH, Koohang A, Paliszkiewicz J. The Internet of Things: Review and theoretical framework. *Expert Systems with Applications* 2019; 133: 97–108. doi: 10.1016/j.eswa.2019.05.014
2. Jasim NA, AlRikabi HTS, Farhan MS. Internet of things (IoT) application in the assessment of learning process. *IOP Conference Series: Materials Science and Engineering* 2021; 1184(1): 012002. doi: 10.1088/1757-899X/1184/1/012002
3. Stoyanova M, Nikoloudakis Y, Panagiotakis S, et al. A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials* 2020; 22(2): 1191–1221. doi: 10.1109/COMST.2019.2962586
4. Pang J, Huang Y, Xie Z, et al. Realizing the heterogeneity: A self-organized federated learning framework for IoT. *IEEE Internet of Things Journal* 2020; 8(5): 3088–3098. doi: 10.1109/JIOT.2020.3007662
5. Pandey A, Vamsi R, Kumar S. Handling device heterogeneity and orientation using multistage regression for GMM based localization in IoT networks. *IEEE Access* 2019; 7: 144354–144365. doi: 10.1109/ACCESS.2019.2945539
6. Huang J, Lv B, Wu Y, et al. Dynamic admission control and resource allocation for mobile edge computing enabled small cell network. *IEEE Transactions on Vehicular Technology* 2022; 71(2): 1964–1973. doi: 10.1109/TVT.2021.3133696
7. Chen Y, Zhao F, Lu Y, Chen X. Dynamic task offloading for mobile edge computing with hybrid energy supply. *Tsinghua Science and Technology* 2023; 28(3): 421–432. doi: 10.26599/TST.2021.9010050
8. Qiu T, Chen N, Li K, et al. How can heterogeneous Internet of Things build our future: A survey. *IEEE Communications Surveys & Tutorials* 2018; 20(3): 2011–2027. doi: 10.1109/COMST.2018.2803740
9. Huang J, Zhang C, Zhang J. A multi-queue approach of energy efficient task scheduling for sensor hubs. *Chinese Journal of Electronics* 2020; 29(2): 242–247. doi: 10.1049/cje.2020.02.001
10. Zhang X, Chen H, Zhao Y, et al. Improving cloud gaming experience through mobile edge computing. *IEEE Wireless Communications* 2019; 26(4): 178–183. doi: 10.1109/MWC.2019.1800440
11. Zhang X, Qi Z, Min G, et al. Cooperative edge caching based on temporal convolutional networks. *IEEE Transactions on Parallel and Distributed Systems* 2022; 33(9): 2093–2105. doi: 10.1109/TPDS.2021.3135257
12. Ray PP. A survey on Internet of Things architectures. *Journal of King Saud University—Computer and Information Sciences* 2018; 30(3): 291–319. doi: 10.1016/j.jksuci.2016.10.003
13. Garg S, Kaur K, Kaddoum G, et al. Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities. *IEEE Network* 2021; 35(5): 298–305. doi: 10.1109/MNET.211.2000526
14. Alagheband MR, Mashatan A. Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives. *Internet of Things* 2022; 18: 100492. doi: 10.1016/j.iot.2021.100492
15. Sood K, Karmakar KK, Yu S, et al. Alleviating heterogeneity in SDN-IoT networks to maintain QoS and enhance security. *IEEE Internet of Things Journal* 2020; 7(7): 5964–5975. doi: 10.1109/JIOT.2019.2959025
16. Silva JDC, Rodrigues JJPC, Saleem K, et al. M4DN. IoT-A networks and devices management platform for Internet of Things. *IEEE Access* 2019; 7: 53305–53313. doi: 10.1109/ACCESS.2019.2909436
17. Dalipi E, Van den Abeele F, Ishaq I, et al. EC-IoT: An easy configuration framework for constrained IoT devices. In: Proceedings of 2016 IEEE 3rd World Forum on IoT (WF-IoT); 12–14 December 2016; Reston, USA. pp. 159–164.
18. Fan X, Chai Q, Xu L, Guo D. Diam-IoT: A decentralized identity and access management framework for Internet of Things. In: Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure; 6 October 2020; Taipei, Taiwan. pp. 186–191.
19. Tran HA, Tran D, Nguyen LG, et al. SHIOT: A novel SDN-based framework for the heterogeneous Internet of Things. *Informatica* 2018; 42(3): 313–323. doi: 10.31449/inf.v42i3.2245
20. Sodhro AH, Obaidat MS, Abbasi QH, et al. Quality of service optimization in an IoT-driven intelligent transportation system. *IEEE Wireless Communications* 2019; 26(6): 10–17. doi: 10.1109/MWC.001.1900085
21. Grace P, Barbosa J, Pickering B, Surridge M. Taming the interoperability challenges of complex IoT systems. In: Proceedings of the 1st ACM Workshop on Middleware for Context-Aware Applications in the IoT; 9 December 2014; Bordeaux, France. pp. 1–6.
22. Famaey J, Berkvens R, Ergeerts G, et al. Flexible multimodal sub-gigahertz communication for heterogeneous Internet of Things applications. *IEEE Communications Magazine* 2018; 56(7): 146–153. doi: 10.1109/MCOM.2018.1700655
23. Luo X, Yin L, Li C, et al. A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access* 2020; 8: 67192–67204. doi: 10.1109/ACCESS.2020.2978525

24. Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal* 2018; 5(2): 1184–1195. doi: 10.1109/JIOT.2018.2812239
25. Kazmi A, Serrano M, Lenis A. Smart governance of heterogeneous Internet of Things for smart cities. In: Proceedings of 2018 12th International Conference on Sensing Technology (ICST); 4–6 December 2018; Limerick, Ireland. pp. 58–64.
26. Deshmukh RA, Jayakody D, Schneider A, Damjanovic-Behrendt V. Data spine: A federated interoperability enabler for heterogeneous IoT platform ecosystems. *Sensors* 2021; 21(12): 4010. doi: 10.3390/s21124010
27. Saatkamp K, Breitenbücher U, Leymann F, Wurster M. Generic driver injection for automated IoT application deployments. In: Proceedings of the 19th International Conference on Information Integration and Web-based Applications & Services; 4–6 December 2017; Salzburg, Austria. pp. 320–329.
28. Sarkar C, Nambi SNAU, Prasad RV. iLTC: Achieving individual comfort in shared spaces. In: Proceedings of International Conference on Embedded Wireless Systems and Networks (EWSN); 15–17 February 2016; Graz, Austria. pp. 65–76.
29. Pamboris A, Kozis C, Herodotou H. Cuttlefish: A flexible and lightweight middleware for combining heterogeneous IoT devices. In: Proceedings of 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC); 10–13 January 2020; Vegas, NV, USA. pp. 1–6.
30. Cimmino A, Poveda-Villalón M, García-Castro R. eWoT: A semantic interoperability approach for heterogeneous IoT ecosystems based on the Web of Things. *Sensors* 2020; 20(3): 822. doi: 10.3390/s20030822
31. Kandi MA, Lakhlef H, Bouabdallah A, Challal Y. An efficient multi-group key management protocol for heterogeneous IoT devices. In: Proceedings of 2019 IEEE Wireless Communications and Networking Conference (WCNC); 15–18 April 2019; Marrakesh, Morocco. pp. 1–6.
32. Xiong H, Wu Y, Jin C, Kumari S. Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT. *IEEE Internet of Things Journal* 2020; 7(12): 11713–11724. doi: 10.1109/JIOT.2020.2999510
33. Marin L, Piotr Pawlowski M, Jara A. Optimized ECC implementation for secure communication between heterogeneous IoT devices. *Sensors* 2015; 15(9): 21478–21499. doi: 10.3390/s150921478
34. Bernal Bernabe J, Hernandez Ramos JL, Skarmeta Gomez AF. TACIoT: Multidimensional trust-aware access control system for the Internet of Things. *Soft Computing* 2016; 20: 1763–1779. doi: 10.1007/s00500-015-1705-6
35. Xu R, Jin W, Kim DH. Knowledge-based edge computing framework based on CoAP and HTTP for enabling heterogeneous connectivity. *Personal and Ubiquitous Computing* 2022; 26: 329–344. doi: 10.1007/s00779-020-01466-4
36. Xia S, Yao Z, Li Y, Mao S. Online distributed offloading and computing resource management with energy harvesting for heterogeneous MEC-enabled IoT. *IEEE Transactions on Wireless Communications* 2021; 20(10): 6743–6757. doi: 10.1109/TWC.2021.3076201
37. Moazzami MM, Xing G, Mashima D, Chen WP, Herberg U. SPOT: A smartphone-based platform to tackle heterogeneity in smart-home IoT systems. In: Proceedings of 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT); 12–14 December 2016; Reston, VA, USA. pp. 514–519.
38. Wang W, Liu X, Yao Y, et al. Crf: Coexistent routing and flooding using WiFi packets in heterogeneous IoT networks. In: Proceedings of IEEE INFOCOM 2019-IEEE Conference on Computer Communications; 29 April–2 May 2019; Paris, France. pp. 19–27.
39. Torroglosa-Garcia EM, Calero JMA, Bernabe JB, Skarmeta A. Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN MEETS 5G. *IEEE Access* 2020; 8: 103164–103180. doi: 10.1109/ACCESS.2020.2998416
40. Pham C, Lim Y, Tan Y. Management architecture for heterogeneous IoT devices in home network. In: Proceedings of 2016 IEEE 5th Global Conference on Consumer Electronics; 11–14 October 2016; Kyoto, Japan. pp. 1–5.
41. Oniga B, Denis L, Dadarlat V, Munteanu A. Message-based communication for heterogeneous Internet of Things systems. *Sensors* 2020; 20(3): 861. doi: 10.3390/s20030861
42. Qin Z, Denker G, Giannelli C, et al. A software defined networking architecture for the internet-of-things. In: Proceedings of 2014 IEEE Network Operations and Management Symposium (NOMS); 5–9 May 2014; Krakow, Poland. pp. 1–9.
43. Nagib AM, Hamza HS. SIGHTED: A framework for semantic integration of heterogeneous sensor data on the Internet of Things. *Procedia Computer Science* 2016; 83: 529–536. doi: 10.1016/j.procs.2016.04.251
44. Noaman M, Khan MS, Abrar MF, et al. Challenges in integration of heterogeneous Internet of Things. *Scientific Programming* 2022; 2022: 8626882. doi: 10.1155/2022/8626882
45. Corral-Plaza D, Medina-Bulo I, Ortiz G, Boubeta-Puig J. A stream processing architecture for heterogeneous data sources in the Internet of Things. *Computer Standards & Interfaces* 2020; 70: 103426. doi: 10.1016/j.csi.2020.103426
46. De Poorter E, Moerman I, Demeester P. Support for heterogeneous dynamic network environments through a reconfigurable network service platform. In: Proceedings of 2011 1st International Symposium on Access Spaces (ISAS); 17–19 June 2011; Yokohama, Japan. pp. 174–179.
47. Aloi G, Caliciuri G, Fortino G, et al. Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications* 2017; 81: 74–84. doi: 10.1016/j.jnca.2016.10.013

48. Al Ridhawi I, Aloqaily M, Boukerche A, Jaraweh Y. A blockchain-based decentralized composition solution for IoT services. In: Proceedings of ICC 2020—2020 IEEE International Conference on Communications (ICC); 7–11 June 2020; Dublin, Ireland. pp. 1–6.
49. Al-Otaibi YD. Distributed multi-party security computation framework for heterogeneous Internet of Things (IoT) devices. *Soft Computing* 2021; 25(18): 12131–12144. doi: 10.1007/s00500-021-05864-5
50. Ghayyur S, Pappachan P, Wang G, et al. Designing privacy preserving data sharing middleware for Internet of Things. In: Proceedings of the Third Workshop on Data: Acquisition to Analysis; 16–19 November 2020; Virtual Event, Japan. pp. 1–6.
51. Islam MS, Verma H, Khan L, Kantarcioglu M. Secure real-time heterogeneous IoT data management system. In: Proceedings of 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA); 12–14 December 2019; Los Angeles, CA, USA. pp. 228–235.
52. Roy SK, Misra S, Raghuwanshi NS. SensPnP: Seamless integration of heterogeneous sensors with IoT devices. *IEEE Transactions on Consumer Electronics* 2019; 65(2): 205–214. doi: 10.1109/TCE.2019.2903351
53. Olivieri AC, Rizzo G. Scalable approaches to integration in heterogeneous IoT and M2M scenarios. In: Proceedings of 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing; 8–10 July 2015; Santa Catarina, Brazil. pp. 358–363.
54. Montori F, Bedogni L, Bononi L. On the integration of heterogeneous data sources for the collaborative Internet of Things. In: Proceedings of 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI); 7–9 September 2016; Bologna, Italy. pp. 1–6.
55. Liu J, Ren A, Zhang L, et al. A novel secure authentication scheme for heterogeneous Internet of Things. In: Proceedings of ICC 2019—2019 IEEE International Conference on Communications (ICC); 20–24 May 2019; Shanghai, China. pp. 1–6.
56. Sasirekha S, Swamynathan S, Suganya S. An ECC-based algorithm to handle secure communication between heterogeneous IoT devices. In: Kalam A, Das S, Sharma K (editors). *Advances in Electronics, Communication and Computing.* Springer; 2016. pp. 351–362.
57. Dao NN, Phan TV, Sa'ad U, et al. Securing heterogeneous IoT with intelligent DDoS attack behavior learning. *IEEE Systems Journal* 2022; 16(2): 1974–1983. doi: 10.1109/JSYST.2021.3084199