IoT Architectural Concerns: A Systematic Review

Asif Qumer Gill
School of Software
University of Technology Sydney
Ultimo, NSW 2007, Australia
Telephone +61 2 9514 7938
asif.gill@uts.edu.au

Vahid Behbood
School of Software
University of Technology Sydney
Ultimo, NSW 2007, Australia
Telephone +61 2 9514 2263
vahid.behbood@uts.edu.au

Rania Ramadan-Jradi
School of Software
University of Technology Sydney
Ultimo, NSW 2007, Australia
Telephone +61 2 9514 7938
rania.jradi@uts.edu.au

Ghassan Beydoun
School of Systems, Management and Leadership
University of Technology
Ultimo, NSW 2007, Australia
Telephone +61 2 9514 2646
ghassan.beydoun@uts.edu.au

ABSTRACT

There is increasing interest in studying and applying Internet of Things (IoT) within the overall context of digital-physical ecosystems. Most recently, much has been published on the benefits and applications of IoT. The main question is: what are the key IoT architectural concerns, which must be addressed to effectively develop and implement an IoT architecture? There is a need to systematically review and synthesize the literature on IoT architectural challenges or concerns. Using the SLR approach and applying customised search criteria derived from the research question, 22 relevant studies were identified and reviewed in this paper. The data from these papers were extracted to identify the IoT architectural challenges and relevant solutions. These results were organised into to 9 major challenge and 7 solution categories. The results of this research will serve as a resource for practitioners and researchers for the effective adoption, and setting future research priorities and directions in this emerging area of IoT architecture.

CCS Concepts

• Information systems→Information integration • Hardware→Analysis and design of emerging devices and systems.

Keywords

Architecture; digital-physical ecosystem; enterprise architecture; IoT; Internet of Things.

1. INTRODUCTION

IoT involves a number of devices that are connected via a common network that can be connected to humans, vehicles, buildings and electronics [1]. Internet of Things (IoT) is defined as the "the infrastructure of the information society" [2]. It is a network of labels, sensors and actuators that enables remote sensing and exchange of data and connects digital and physical systems [3].

Each thing in the IoT network can be uniquely identified and addressed. There are a number of applications of IoT such as the smart cities, smart homes, smart campus, smart hospitals. IoT is disrupting the academia, industry, government and society [4, 10]. For instance, academia may use IoT for smart campus. Industry may use IoT for operational excellence, product and service innovation, customer excellence and effective decision-making. Government may adopt IoT for offering citizen-centric IoT- enabled digital-physical services. Society may be interested in IoT- enabled smart living, smart health, smart home etc.

Researchers are taking keen interest in IoT and a considerable amount of research is being conducted in IoT-enabled smart digital- physical ecosystems [5]. Most recently, the emergence and convergence of a number of digital technologies such as analytics, big data, blockchain, cloud, mobile, social, machine learning, commodity computing, sensors, and actuators are continuously evolving the vision and scope of IoT [6, 11, 12]. This increasingly complex and evolving vision and scope of IoT provide both opportunities and challenges [7]. Despite the growing interest in IoT, the fundamental question is: what are the key concerns of evolving IoT architecture, which must be addressed to effectively develop and implement the IoT-enabled smart digital-physical ecosystems. There is a need to systematically review and synthesize the literature on IoT architectural challenges and concerns. Hence, this paper focuses on the following main research question:

RQ. What is known about the architecture of the Internet of Things? (Main research question)

RQ1. What are the IoT architectural issues or challenges?

RQ2. What strategies, techniques or practices are being used to deal with these issues or challenges?

This paper adopts a systematic literature review (SLR) approach [8] to answer the above mentioned research questions. The main contribution of the paper is that it provides a granular understanding and yields pragmatic guidance about the key IoT architectural challenges and solutions. This study represents an initiative to provide a knowledge-base to guide organisations to effectively design and implement IoT architecture for digital-physical ecosystems. This paper is organised as a follows. Firstly, it discusses the research method. Secondly, it presents the study results. Thirdly, it discusses the results followed by conclusion and future research directions.

2. RESEARCH METHOD

This study has been conducted using a well-known systematic literature review (SLR) approach [8]. SLR is characterised as a formal, structured and repeatable method. SLR method has been used because it offers a rigorous and systematic evaluation of available research papers relevant to a research topic, area or question(s). This SLR study comprises of following key stages:

- data sources and search strategy
- inclusion and exclusion criteria
- study selection process
- data extraction
- data synthesis

2.1 Data Sources and Search Strategy

Search strategy involved utilizing a number of well-known electronic databases, as well as manual methods of searching. Structured search strings were developed and applied to the following key data sources. The following five well-known electronic databases were used to get the required papers for this SRL.

- IEEE Xplore (www.ieeexplore.ieee.org/Xplore)
- ACM Digital Library (www.portal.acm.org/dl.cfm)
- Elsevier ScienceDirect (www.sciencedirect.com)
- EBSCO Host (www.ebscohost.com)
- ProQuest (www.proquest.com)

These databases were selected for their relevance to the field of study, their renowned and respected status, and capabilities to provide sufficient literature search and coverage for this study. In addition to these databases, manual searching was conducted on a number of seminal works, such as the Internet of Things – Architecture (IoT-A) consortium’s studies, the IoT Architecture Reference Model (ARM) [9], and conference proceedings from the Internet of Things and Cloud Computing Conference (ICC). Based on the focus of our research, a search string was constructed as recommended by Kitchenham [8]. Table 1 presents the search terms and keywords, which are organised into (1) Internet of things, (2) technology and architecture, and (3) challenges. Using these search terms, a search string was created to find relevant literature to answer the research questions in hand. This was done by combining the terms *within* each category via the Boolean “OR” operator, then combining the three search categories *together* via the Boolean “AND” operator, to result in the following string:

((Internet of things OR IoT OR internet-of-things OR EIoT OR future internet OR emerging internet OR internet of everything OR enterprise internet of things); AND
(architecture OR cloud OR reference architecture OR application OR IoT facility; AND
(problems OR challenges OR concerns OR issues)).

Table 1. Search terms

Search Category	Search Terms
Internet of Things	Internet of things, IoT, internet-of-things, EIoT, future internet, emerging internet, internet of everything, enterprise internet of things
Technology and Architecture	Architecture, cloud, reference architecture, application, IoT facility
Challenges	Problems, challenges, concerns, issues

2.2 Inclusion and Exclusion Criteria

The following inclusion and exclusion criteria was used to select the relevant papers for this SLR.

- Relevant to the three defined search categories: Internet of Things, technology and architecture, and challenges;
- Academic, experimental or commercial projects;
- Case study, conference paper, journal, workshop, empirical study, experimental study, comparative study, meta-analysis, survey, action research or literature review;
- Published from Jan 2014 onwards;
- Full text available and written in English.

Since the research questions are focused on IoT architecture challenges and solutions (not limited to a specific technology), therefore, studies that focused on a specific technology or model were still included if they satisfied the rest of the inclusion criteria. Papers published from Jan 2014 onwards were selected to include the most recent studies. Furthermore, studies that do not answer the research question and meet the following exclusion criteria were excluded from this study:

- Magazines, blogs, podcasts, websites, newspapers, and wire feeds;
- Duplicate studies (when the same study existed in multiple sources, the most complete and/or recent version of the study was included).

2.3 Study Selection Process

An initial search resulted in a total of 3,216 “hits” across all data sources. 2,420 of these were unique. Figure 1 presents the three stage selection process involving identification, screening and selection of a paper. This multi stage selection process was adopted to ensure that only relevant studies are selected. Further, Table 3 presents a number of studies sourced from each database across each study selection stage. In the Identification and Screening stages of the study selection process, database results and citations were exported into RefWorks [13] - a bibliography and database manager. Throughout the selection process, a new sub-folder was created for each review stage alongside a new Excel sheet for effective tracking and management. This ensured full traceability and transparency of the work.

A standard method of assessment and publication acceptance criteria was applied to each stage of the review, which is summarized in Table 2. The method involved increasingly granular reviews on the selected studies. For example, in the first review stage, relevant studies were identified based on our search strategy (total 2,420 without duplicates). Next, in the second stage, the title and keywords of studies were reviewed. At this stage, the majority of papers were excluded due to their irrelevance. This left us with 156 studies. Where it was not possible to make a decision on inclusion based on the title and keywords alone, then the paper was included for further review. Further, based on the review of abstract, we got 65 possibly relevant studies. Finally, the further review of the 65 studies resulted in the final selection of 22 papers. These final 22 studies are listed in Appendix A.

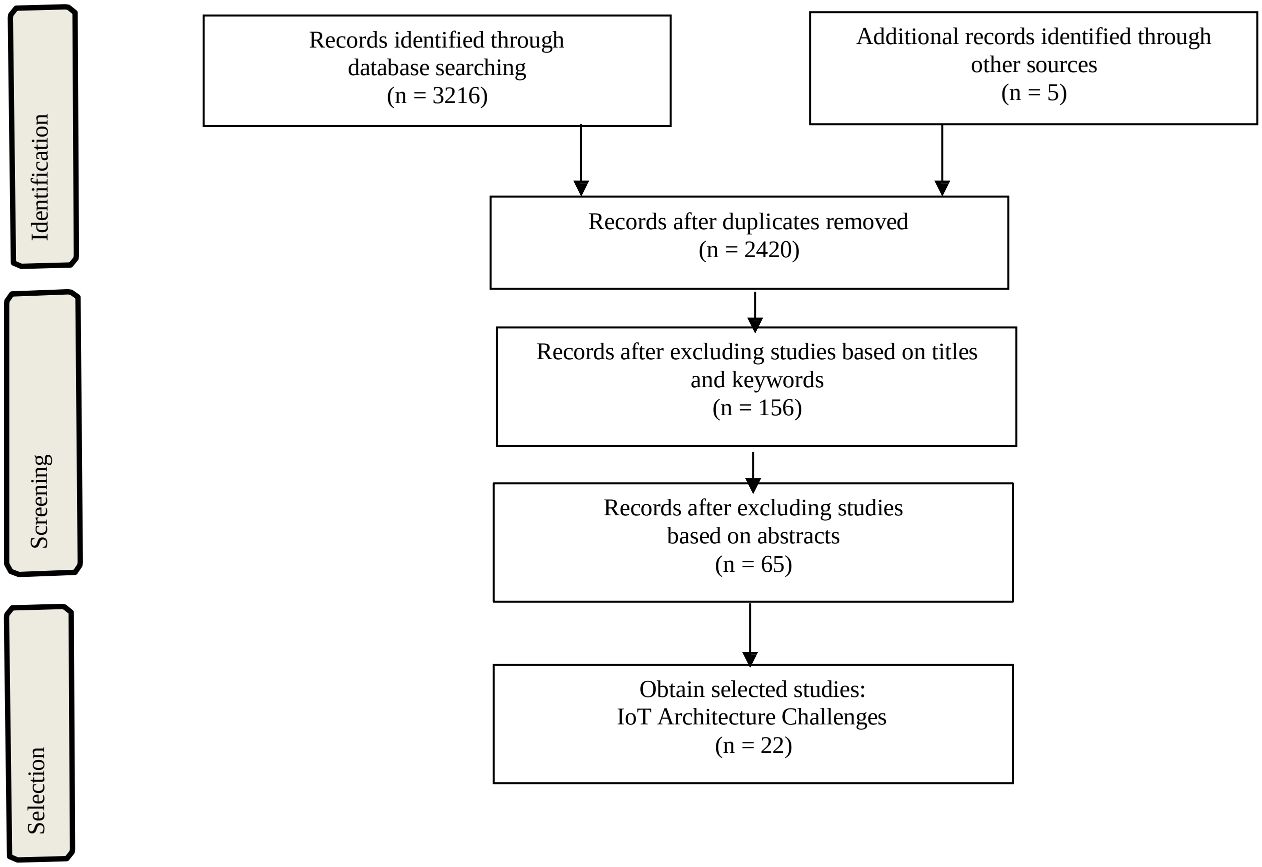
Identification
Screening
Selection
Records identified through database searching (n = 3216)
Additional records identified through other sources (n = 5)
Records after duplicates removed (n = 2420)
Records after excluding studies based on titles and keywords (n = 156)
Records after excluding studies based on abstracts (n = 65)
Obtain selected studies: IoT Architecture Challenges (n = 22)

Figure 1. Study selection process

Table 2. Search results

Database	1st stage	2nd stage	3rd stage	Studies selected	Percent selected (%)
IEEE Xplore	621	118	49	20	91
ACM Digital Library	161	13	6	0	0
ScienceDirect	855	6	2	1	4.5
EBSCO	241	17	7	1	4.5
ProQuest	542	2	1	0	0
Total	*2420*	*156*	*65*	*22*	*100*

Table 3. Assessment method at each review stage

Review stage	**Method**	**Acceptance criteria**
1st stage	Identify relevant studies from data sources	Keywords
2nd stage	Exclude studies based on titles and keywords	Title = search term.
3rd stage	Exclude studies based on abstracts	Abstract = IoT AND architecture
Final selection	Select final studies based on full-text review	Must address at least one IoT architecture challenge OR at least one IoT architecture solution / proposal OR both of the above.

2.4 Data Extraction

We analysed the final set of 22 papers and extracted IoT challenges and solutions (data). To accurately collect data from each of the selected paper, a data extraction form was developed. The form captured the following items:

- Study metadata: Including title, authors, full source, and direct hyperlink;
- Publication channel (journal, conference, book);
- Summary of IoT architectural challenges;
- Examples of IoT architectural challenges;
- Summary of IoT architectural strategies;
- Examples of IoT architectural strategies;

Not all fields were able to be populated for each study. For example, some studies reported on IoT architectural challenges *only* and did not discuss strategies to overcome these. Other studies only proposed strategies, solutions or prototypes without discussing the challenges.

2.5 Data Synthesis

All the data extracted from the selected studies was synthesized in a tabular form against each of the three research questions. This method facilitated the identification of basic concepts and categories of IoT architecture challenges or concerns, as well as strategies or best-practices to overcome those challenges. An extensive analysis of the data led to the codification of broad "categories" related to a challenge or solution concept. These categories are presented in **Table 5** and **Table 6** of the results section. Furthermore, a frequency analysis of each category was conducted to identify the strength and trend of research interest in that area. For example, the most important challenge of security and privacy was discussed by 68% of the total number of studies reviewed in this paper.

3. Results

Final 22 papers were reviewed (S1 – S22) based on inclusion and exclusion criteria as discussed in the research method section. Papers S1 – S22 are presented in Appendix A. The majority of studies covered all aspects of the research questions (challenges AND solutions) with regards to IoT architecture. The selected studies were sourced from a wide variety of publication channels (conferences and journals) as shown in Table 4. Seven studies were published in a variety of journals, such as Mobile Computing, Communications Surveys, and the Industrial Informatics journal. Fifteen studies were published at conferences, such as the WF-IoT and WCNCW conferences.

Table 4. Publication channels

Publication Channel	**Type**	**Study**	**Number**
Communications Surveys & Tutorials	Journal	S1	1
Pervasive and Mobile Computing	Journal	S6	1
Mobile Computing	Journal	S9	1
Industrial Informatics	Journal	S13	1
Access	Journal	S15	1
Communications Magazine	Journal	S20	1
Distributed Sensor Networks	Journal	S21	1
EuCNC	Conference	S2	1
WoWMoM	Conference	S3	1
ICIN	Conference	S4	1
Mobile Services	Conference	S5	1
Local Computer Networks	Conference	S7	1
IMIS	Conference	S8	1
ICEBE	Conference	S10	1
WF-IoT	Conference	S11, S16, S18	3
FiCloud	Conference	S12	1
WCNCW	Conference	S14	1
ISSC	Conference	S17	1
SEAA	Conference	S19	1
NOMS	Conference	S22	1

These 22 selected papers were reviewed to identify the challenges and solutions relevant to IoT architecture (RQ1 and RQ2). By investigating and analyzing these research questions, we aim to provide a synthesis of the body of knowledge available regarding IoT architectural challenges and solutions. In analyzing the selected studies, a number of common themes or categories emerged with regards to architectural challenges and solutions. Table 5 (A1-A9) presents nine major categories of IoT architectural challenges and Table 6 (B1-B7) presents seven categories of solutions to overcome the challenges.

Table 5. IoT Architectural challenges and categories

Ref.	**Category**	**IoT Architectural Challenges**
A1	Security & Privacy	Authentication, data integrity, non-repudiation, authorisation
A2	Lack of standardisation	Standardisation, interoperability, varying protocols and interpretations of standards, abstractions.
A3	Performance	Processing speed, communication speed, overhead, computational and memory limitations.
A4	Device Management	Faults, Configuration, Accounting and Security of multiple devices, plus device updates.

A5	Evolvability	Changing requirements, new functions, continuous improvements.
A6	Complexity	Data analysis, big data, distributed systems.
A7	Cost Limitations	Financial concerns.
A8	People	Lack of development toolkits.
A9	Quality of Service	Reliability, maintainability, mobility, scalability, availability.

Table 6. IoT Architectural proposed solutions and categories

Ref.	Category	IoT Proposed Solutions
B1	Standardisation	Improving interoperability. Building multi-use standards and protocols.
B2	Networking	Software-defined networking (SDN).
B3	Architecture	Generic IoT reference architecture. Service-oriented architecture (SOA). Identity Management Architecture.
B4	Cloud	Open-source APIs and interoperability using cloud computing. Fog computing.
B5	Gateways	Intelligent and semantic IoT gateways.
B6	Security	Public-Key Infrastructure (PKI) certificates, encryption, cryptographic protocols.
B7	Best practices	Redundancy, caching, tunnelling, pub/sub messaging.

Table 7. Frequency analysis in selected studies for IoT Architectural Challenges

Ref.	Category	Frequency	%	Studies
A1	Security & Privacy	15	68	S1, S3, S5, S10-S21
A2	Lack of Standardisation	14	64	S1 – S8, S11, S13, S15, S16, S20, S22
A3	Performance	9	41	S1, S9, S12, S13, S15, S17, S18, S19, S20
A4	Device Management	7	32	S1, S3, S7, S13, S18, S19, S21
A5	Evolvability	1	5	S9
A6	Complexity	1	5	S12
A7	Cost Limitations	1	5	S13
A8	People	4	18	S4, S8, S15, S19
A9	Quality of Service	9	41	S1, S2, S9, S12, S13, S14, S15, S16, S21

3.1 RQ1 - Challenges

The identified nine challenge categories represent a combination of technical, human, financial and ethical aspects. For example, security and privacy – one of the most commonly cited concern or challenge reported by 68% of the selected studies as shown in Table 7 (A1:A9). It is both a technical and ethical challenge. Moreover, some challenges are purely technical such as device management and performance. Others, such as computational limitations and costs, are financially in nature. Table 7 presents a frequency analysis of the most commonly discussed and cited challenges in the selected studies. These challenges are discussed below.

Security & Privacy: The challenge of security and privacy appears to be well-connected and overlapping, thus being combined into the same category. This challenge is prominent in the selected studies, with 68% of the studies highlighting this issue. The security and privacy concern is related to the data being transmitted by IoT devices and networks. More specifically, selected studies [e.g. S1] report that securing data exchanges will be critical to avoid losing or compromising privacy due to the proliferation of smart "things" with sensitive data. This is currently a challenge, and perhaps due to the IoT's explosive and haphazard growth. There is a concern regarding the lack of basic privacy and security principles in IoT, including authentication, data integrity, non-repudiation and authorization [e.g. S3, S5]. However, some studies call for the need to facilitate more open access between devices to allow vendors to work with various permissions on different data and levels [e.g. S13, S14].

Lack of Standardization: The lack of a common standardization is reported as a second major challenge after security and privacy-reported by the 64% of the selected studies. This is due to the need to handle a large number of heterogeneous things that belong to different platforms [S1]. The current IoT landscape encompasses different protocols, different interpretations of the same standard, different priorities between application developers and device manufacturers, different levels of abstraction and generalization, and a lack of consensus regarding IP-based open standards to enable communication compatibility between entities in different domains [e.g. S3, S5]. This leads to the challenge and need of standardization in IoT.

Performance: 41% of the total selected studies highlighted the concerns or challenges around performance of the resources or components of the IoT architecture. It has been identified that IoT relies on a multitude of components and underlying technology, which have different levels of performance concerns [S1]. Processing speed, communication speed, overheads, computational limitations, memory limitations and battery / energy limitations were all commonly cited challenges at different levels [e.g. S9, S12, S13]. Further, lack of thorough performance evaluations or testing of IoT applications was underlined as an important issue.

Device Management: The premise of IoT relies on the management of a plethora of devices. 32% of the total selected studies reported this challenge [e.g. S1, S3, S7]. IoT devices need to be remotely managed, whether in terms of faults, configurations, accounting, performance, security, or device updates. There are also challenges around device naming and discovery. The identification of each IoT device with a canonical, scalable and expandable unified device or resource identifier is essential for accurate device management. Further, there are concerns regarding the process of discovering new devices or services in the cloud-enabled IoT, which is another emerging area of interest.

Evolvability: Surprisingly, only 5% of the selected studies highlighted this concern about the evolvability of IoT architecture [S9]. The need for adaptability and flexibility in architecture is essential to deal with the always changing requirements of customers. This may include incorporating new functions, data formats, devices and accommodate continuous improvements.

Complexity: The complexity of distributed systems underpinning IoT architecture is raised as a concern (only 5% of the selected studies). For example, the use of Microservices for IoT is another layer of complexity, which needs to be addressed in the IoT architecture [S12]. Additionally, it has been identified that complexity has impacts on the field of data management and analytics as well. Data analytics may not appropriately be performed without the effective ways to source, ingest, clean, mine, understand and analyse the massive amount of complex data generated from both IoT applications and existing IT systems. In short, data management and its quality could be a challenge due to the complex nature of large number of interconnected devices and applications.

Cost Limitations: It has been identified that all service-based "things" suffer from cost limitations, particularly in IoT architecture [S13]. Although, only 5% of the selected studies reported this, however, financial concerns may have significant impacts on IoT services and applications and thus warrant further investigation.

People: The difficulty in the development of IoT architecture, applications and services has been cited by a small number of studies (18% of the selected studies) [e.g. S4, S8, S15]. It has been found that there is a more need of development toolkits and trainings to enable developers to create and evaluate IoT prototypes in simple and flexible ways [e.g. S4]. Developers currently need expertise in disparate fields (e.g. sensor components, network protocols, data formats, data management etc.) to be able to develop and implement IoT architecture. This may require merging different heterogeneous IoT tools and programming platforms to save time, effort and overall development costs.

Quality of Service: A number of general quality of service concerns and challenges were reported by 41% of the selected studies. These concerns are related to availability, scalability, mobility and service assurance [e.g. S1, S2, S9]. Availability is about the ability for IoT applications to meet software and hardware service levels. Scalability is the ability to add new devices, services and functions without negatively affecting the quality of existing services. This seems to be a difficult task in the presence of diverse IoT hardware platforms, communication protocols and multiple different service providers. Mobility is another issues, which is about the difficulty in delivering IoT services to mobile users who are continuously on the move in different geo restrictions and locations. Service interruptions may occur when devices transfer the gateways or move into another geo restriction. Assurance highlights the concerns of reliability and maintainability for IoT-enabled environments. In summary, these challenges can be used as a guiding lens and be addressed when developing the IoT architecture for a particular situation.

3.2 RQ2 – Solutions

In order to address RQ2, a number of solutions strategies were identified to overcome the IoT architectural challenges. These solutions were extracted from the selected studies and organised into seven major categories as shown in Table 8 (B1:B7): standardisation, networking, adaptive architecture, cloud, gateways, security and generic best practices.

Standardisation: The majority of the selected studies (60%) suggest standardization as a solution to current IoT architectural challenges [e.g. S1-S3, S5, S8]. The studies propose the creation and acceptance of a number of standards to be used in IoT, including security standards, communication standards, and identification standards, as well as standards for various protocols and layers such as CoAP, XMPP and MQTT. Standards could be the key enablers for the effective IoT architecture. For example, [S3] proposes the use of MQTT protocol for smart phone notification for push services due to its simplicity, efficiency, small cost footprint, low power consumption on embedded devices, and flexibility in message distribution.

Networking: Connectivity or network is core to the IoT architecture. 23% of the selected studies highlight the need for networking solutions to address the concerns that involve network services [e.g. S6, S7, S9]. For example, the use of Software-Defined Networking (SDN) has been highlighted as a successful method to abstract and decouple lower level functionalities by splitting control and data flows. SDN would move the former control to a high logically centralized layer. This will enable the implementation of separation of concerns architecture design principle.

Adaptive Architecture: A large number of studies (55%) proposed varying or flexible or agile or adaptable architecture as a solution for IoT challenges [S1, S2, S4, S5, S6]. For example, a flexible IoT architecture model has been suggested by [S1], [S11], [S12] and [S20] as a means of providing scalability and a reference architecture to tailor and develop customer-centric IoT architecture. Further, some studies suggest a flexible and agile Service-Oriented Architecture (SOA) to simplify the development of IoT architecture and applications [S4, S13]. Similarly, a semantic-based IoT architecture is proposed by [S5] and [S8], which can be adapted to cloud, devices, gateways, and has the added benefit of being compatible with existing standardizations initiatives such as ETSI M2M and oneM2M. Various other proposals are presented by [S13], including the use of Microservices architectures, where services are small, highly decoupled, and focus on a very small task. A top-down Sensing and Actuation as a Service (SAaaS) architecture has been proposed for IoT devices. Further, [S16] proposes a Distributed Internet-like Architecture of Things (DIAT). This is a layered and distributed architecture that provides decoupling of orthogonal features, binds similar functionalities together, and provides a hierarchical structure to functionalities. DIAT addresses a number of challenges, including heterogeneity, scalability, interoperability, and configuration issues.

Cloud: A small number of selected studies (18%) present cloud-based solution strategies for supporting the IoT architecture [e.g. S1, S14, S18]. Cloud computing is presented as a solution strategy where open-source APIs provide immense interoperability with well-known protocols via JSON, XML and CSV. Additionally, fog computing (aka cloudlets or edge computing) is suggested by [S1] and [S19] as a viable solution which would act as a bridge between smart devices and large-scale cloud computing and storage devices. Thus, fog computing has the potential to increase overall performance concerns of IoT and address service and cost limitation concerns.

Gateways: Gateways are also critical for enabling connectivity in the IoT architecture. The creation of new intelligent IoT gateways that enable better horizontal integration and interoperability are suggested by [S1], [S5] and [S8] (e.g. 14% of the selected studies). For example, [S5] specifies a semantic gateway as a service, whereby the gateway provides translation between various protocols and thus makes their semantic integration possible and seamless for supporting the complex IoT architecture.

Security: With regards to security, Public Key Infrastructure (PKI) certificates are proposed as solutions by [S17], [S19] and [S20]. The analysis of the studies (18%) state that certificates and cryptographic protocols are essential, however they still pose their own challenges in regards to their large size, complex structures, and requirement for complex parsers. This warrants further investigation in this important area of IoT security.

Generic best practices: Finally, 23% of the selected studies propose extending and implementing IT service management best-practices into the IoT architectural landscape with a view to address multiple challenges. For example, [S1] highlights the benefits of building in redundancy (resilience) in the IoT architecture for critical devices and services to address availability concerns. Similarly, the use of caching and tunneling would support service mobility. Similar to other industries, [S4] proposes the creation of development toolkits to support inexperienced developers in rapidly building IoT prototypes using a model-driven development approach to test the ideas and concerns.

Table 8. Frequency analysis in selected studies for IoT Architectural Solutions

Ref.	Category	Frequency	%	Studies
B1	Standardisation	13	60	S1, S2, S3, S5, S8, S10, S11, S12, S13, S15, S18, S20, S22
B2	Networking	5	23	S6, S7, S9, S21, S22
B3	Adaptive Architecture	12	55	S1, S2, S4, S5, S6, S8, S10, S11, S12, S13, S14, S16
B4	Cloud	4	18	S1, S14, S18, S19
B5	Gateways	3	14	S1, S5, S8
B6	Security	4	18	S13, S17, S19, S20
B7	Generic best practices	5	23	S1, S3, S4, S17, S18

4. DISCUSSION

IoT seems to offer lucrative benefits and application to academia, industry, government and society. It is still challenging whether IoT can be effectively adopted at an optimal scale due to inherent complex nature of its architecture. Thus, despite its acknowledged importance, we found a number of IoT architectural challenges and solutions using the SRL approach, which were presented in this paper.

Our findings reveal nine major categories of IoT architectural challenges (Tables 7): security and privacy, lack of standardisation, performance, device management, evolvability, complexity, cost limitations, people and quality of service. Security and privacy (68%) and lack of standardisation (64%) were the most reported challenges for IoT architecture. This highlight the current focus and urgent needs of stakeholders to address these pressing concerns. This warrants the need for more research and development in IoT standards, security and privacy reference models, patterns, principles and solutions. Surprisingly, evolvability, complexity and cost were the least mentioned (only 5%) concerns in the selected studies. IoT is a complex architecture of heterogeneous connected things, and should have the ability to evolve. Although, these concerns were least mentioned, however, it does not indicate that these are not important. This may be due to the under developed or overlooked areas of IoT architecture, which may require further attention and development.

In addition to these identified challenges, this study also reported seven major categories of solutions to the challenges (Table 8): standardisation, networking, adaptive architecture, cloud, gateways, security and other generic best practices. Standardisation (60%) and adaptive architecture (55%) were the most reported solutions for the IoT challenges. This compliments and links to the identified challenge of lack of standardisation and evolvability (as discussed earlier). This highlights that the current focus is on developing standards to enable the effective adoption of IoT. Adaptive or flexible architecture approach suggests (as discussed earlier) the need for using a combination of SOA, sematic architecture and Microservices to build in adaptability in the IoT architecture to address the various dynamic needs of stakeholders and relevant standards. Surprisingly, security was the least mentioned (only 18%) solution, however, it was the most mentioned concern (68%). Perhaps, this is due to the fact the IoT security area is still in its early stages and requires more research and development. In summary, these numerical figures provide us useful insights and highlight the areas, which may require further work.

Like any other studies, this study has also some limitations. Given the project scope and time constraints, this SLR study is limited to the number of selected databases, search strings and coverage of years (2014 onwards). However, these provided sufficient recent literature for identifying the challenges and relevant solutions for IoT architecture. It is important to mention that there was no relationship bias between the researchers and the authors of the selected studies used in this review. We followed a systematic staged approach (Figure 1) to help ensure that the selection process was unbiased. Like any other SLR study, this study does not claim that the keywords and search strings used have not caused the omission of other relevant studies. To further ensure the unbiased selection and quality of the papers, we applied inclusion/exclusion criteria at every stage. The analysis and categorization of the identified concepts (e.g. challenges and solutions) are subject to human error and mistakes, which may lead to inconsistencies. The concepts and categories and their interconnections were continuously checked to minimize any possible omissions, errors or coding bias. The extracted data were then reviewed, and disagreements were resolved by consensus during research project review meetings. This review lays a foundation for further work in IoT architecture.

5. CONCLUSION

IoT has sparked a significant interest among practitioners and researchers. It is a complex digital-physical ecosystems of heterogeneous devices, data, software, physical build environment and humans. The effective design and implementation of IoT architecture is not a straight forward task. We need to effectively identify, understand and address the underlying challenges before jumping on the bandwagon of IoT. This paper is a small attempt to address this important need and research gap, and presented a set of IoT architectural challenges and relevant solutions using the well-known SLR approach. This study highlighted the least and most pressing areas of focus both in the problem (e.g. security and privacy, lack of standardisation) and solution (e.g. standardisation, varying architecture options) space. Surprisingly, the most commonly mentioned challenge of security and privacy has less mentioned solutions in the selected studies. This indicates more work in this important area of IoT security architecture. The findings of this SLR study provide a knowledge base that can be helpful to practitioners and researchers who intend to use or work in this emerging area.

6. SECTIONS APPENDIX A – SELECTED STUDIES FOR REVIEW

[S1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. Communications Surveys & Tutorials, IEEE, 17(4), 2347-2376.

[S2] Amadeo, M., Campolo, C., Iera, A., & Molinaro, A. (2014). Named data networking for IoT: An architectural perspective. Networks and Communications (EuCNC), 2014 European Conference on, pp. 1-5.

[S3] Chen Zhou, & Xiaoping Zhang. (2014). Toward the internet of things application and management: A practical approach. World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a, pp. 1-6.

[S4] Conzon, D., Brizzi, P., Kasinathan, P., Pastrone, C., Pramudianto, F., & Cultrona, P. (2015). Industrial application development exploiting IoT vision and model driven programming. Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, pp. 168-175.

[S5] Desai, P., Sheth, A., & Anantharam, P. (2015). Semantic gateway as a service architecture for IoT interoperability. Proceedings of the 2015 IEEE International Conference on Mobile Services, pp. 313-319.

[S6] Distefano, S., Merlino, G., & Puliafito, A. (2015). A utility paradigm for IoT: The sensing cloud. Pervasive and Mobile Computing, 20, 127-144.

[S7] El-Mougy, A., Ibnkahla, M., & Hegazy, L. (2015). Software-defined wireless network architectures for the internet-of-things. Local Computer Networks Conference Workshops (LCN Workshops), 2015 IEEE 40th, pp. 804-811.

[S8] Gyrard, A., Datta, S. K., Bonnet, C., & Boudaoud, K. (2015). A semantic engine for internet of things: Cloud, mobile devices and gateways. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference on, pp. 336-341.

[S9] Hao Yin, Yong Jiang, Chuang Lin, Yan Luo, & Yunjie Liu. (2014). Big data: Transforming the design philosophy of future internet. Network, IEEE, 28(4), 14-19.

[S10] Ju Chen, Yi Liu, & Yueting Chai. (2015). An identity management framework for internet of things. E-Business Engineering (ICEBE), 2015 IEEE 12th International Conference on, pp. 360-364.

[S11] Krco, S., Pokric, B., & Carrez, F. (2014). Designing IoT architecture(s): A european perspective. Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 79-84.

[S12] Krylovskiy, A., Jahn, M., & Patti, E. (2015). Designing a smart city internet of things platform with microservice architecture. Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, pp. 25-30.

[S13] Li Da Xu, Wu He, & Shancang Li. (2014). Internet of things in industries: A survey. Industrial Informatics, IEEE Transactions on, 10(4), 2233-2243.

[S14] Pohls, H. C., Angelakis, V., Suppan, S., Fischer, K., Oikonomou, G., Tragos, E. Z., et al. (2014). RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects. Wireless Communications and Networking Conference Workshops (WCNCW), 2014 IEEE, pp. 122-127.

[S15] Riazul Islam, S. M., Daehan Kwak, Humaun Kabir, M., Hossain, M., & Kyung-Sup Kwak. (2015). The internet of things for health care: A comprehensive survey. Access, IEEE, 3, 678-708.

[S16] Sarkar, C., Nambi, S. N. A. U., Prasad, R. V., & Rahim, A. (2014). A scalable distributed architecture towards unifying IoT applications. Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 508-513.

[S17] Schukat, M., & Cortijo, P. (2015). Public key infrastructures and digital certificates for the internet of things. Signals and Systems Conference (ISSC), 2015 26th Irish, pp. 1-5.

[S18] Sharma, A., Goyal, T., Pilli, E. S., Mazumdar, A. P., Govil, M. C., & Joshi, R. C. (2015). A secure hybrid cloud enabled architecture for internet of things. Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, pp. 274-279.

[S19] Taivalsaari, A., & Mikkonen, T. (2015). Cloud technologies for the internet of things: Defining a research agenda beyond the expected topics. Software Engineering and Advanced Applications (SEAA), 2015 41st Euromicro Conference on, pp. 484-488.

[S20] Tiburski, R. T., Albernaz Amaral, L., De Matos, E., & Hessel, F. (2015). The importance of a standard securit y archit ecture for SOA-based iot middleware. Communications Magazine, IEEE, 53(12), 20-26.

[S21] Valdivieso Caraguay, Á. L., Peral, A. B., Barona López, L. I., & García Villalba, L. J. (2014). SDN: Evolution and opportunities in the development IoT applications. International Journal of Distributed Sensor Networks, , 1-10.

[S22] Zhijing Qin, Denker, G., Giannelli, C., Bellavista, P., & Venkatasubramanian, N. (2014). A software defined networking architecture for the internet-of-things. Network Operations and Management Symposium (NOMS), 2014 IEEE, pp. 1-9.

7. REFERENCES (ADDITIONAL)

[1] Cisco, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," ed, 2011.

[2] "Internet of Things Global Standards Initiative". ITU.

[3] Ericsson, "More than 50 Billion Connected Devices," ed, 2011.

[4] M. Dohler, “Machine-to-Machine Technologies, Applications & Markets”, 27th IEEE International Conference on Advanced Information Networking and Applications (AINA) (2013).

[5] L. Atzori, A. Iera, and G. Morabito.: The internet of things: A survey. Computer Networks, vol. 54, no. 15, pp. 2787 – 2805 (2010).

[6] A. Q. Gill, Phennel, N., Lane, D., & Phung, V. L. (2016). IoT-enabled emergency information supply chain architecture for elderly people: The Australian context. Information Systems, 58, 75-86.

[7] D. Zeng, S. Guo, and Z. Cheng, "The Web of Things: A Survey," Journal of Communications, vol. 6, pp. 424-38, 2011

[8] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Ver. 2.3 EBSE Technical Report, EBSE,2007.

[9] Internet of Things – Architecture (IoT-A). http://www.iot-a.eu/public.

[10] J. L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," Journal of Computer and System Sciences, vol. 81, pp. 1452-1463, 12// 2015.

[11] N. Marz, Warren, J.: A new paradigm for Big Data. In Big Data – Principles and best practices of scalable real-time data systems, to appear, Chapter 1, Manning Publications Co. Available at http://www.manning.com/marz/, ISBN 9781617290343.

[12] M. Batty, “Smart Cities and Big Data”, http://www.spatialcomplexity.info/.

[13] RefWorks. https://www.lib.uts.edu.au/help/referencing/refworks