Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Position Paper:

Privacy and security federated reference architecture for Internet of Things[#]

Musab KAMAL[1], Imran RASHID[1], Waseem IQBAL[†‡1], Muhammad Haroon SIDDIQUI[1],
Sohaib KHAN[1], Ijaz AHMAD[2]

[1]*Department of Information Security, National University of Sciences and Technology, Islamabad 44000, Pakistan*

[2]*Faculty of Information Technology, Majan University College, Muscat 112, Oman*

[†]E-mail: waseem.iqbal@mcs.edu.pk

Received Aug. 31, 2022; Revision accepted Dec. 13, 2022; Crosschecked Mar. 27, 2023

Abstract: Physical objects are getting connected to the Internet at an exceptional rate, making the idea of the Internet of Things (IoT) a reality. The IoT ecosystem is evident everywhere in the form of smart homes, health care systems, wearables, connected vehicles, and industries. This has given rise to risks associated with the privacy and security of systems. Security issues and cyber attacks on IoT devices may potentially hinder the growth of IoT products due to deficiencies in the architecture. To counter these issues, we need to implement privacy and security right from the building blocks of IoT. The IoT architecture has evolved over the years, improving the stack of architecture with new solutions such as scalability, management, interoperability, and extensibility. This emphasizes the need to standardize and organize the IoT reference architecture in federation with privacy and security concerns. In this study, we examine and analyze 12 existing IoT reference architectures to identify their shortcomings on the basis of the requirements addressed in the standards. We propose an architecture, the privacy-federated IoT security reference architecture (PF-IoT-SRA), which interprets all the involved privacy metrics and counters major threats and attacks in the IoT communication environment. It is a step toward the standardization of the domain architecture. We effectively validate our proposed reference architecture using the architecture trade-off analysis method (ATAM), an industry-recognized scenario-based approach.

Key words: Architecturally significant requirement (ASR); Architecture trade-off analysis method (ATAM); Internet architecture board; Internet of Things (IoT); Privacy enhancing technologies; Privacy validation chain

https://doi.org/10.1631/FITEE.2200368 **CLC number:** TP393

1 Introduction

In this technology-driven era in which everything is interconnected with each other, we can communicate despite being separated by thousands of miles. This usually refers to the Internet of Things (IoT) where everything is connected. IoT is a system of smart lightweight devices that consist of embedded processors, sensors, actuators, and communication hardware that intelligently acquire, collect, and send data from their respective environments. These IoT devices share the collected data through the gateway or other edge devices that analyze data on the cloud or locally. These are called smart and intelligent devices because they do all the work without human intervention. IoT has evolved greatly over the years; if we observe the statistics, the number of IoT devices is projected to increase to 75.44 billion in 2025 (Zhou et al., 2019). It was expected

[‡] Corresponding author

[#] Electronic supplementary materials: The online version of this article (https://doi.org/10.1631/FITEE.2200368) contains supplementary materials, which are available to authorized users

ORCID: Waseem IQBAL, https://orcid.org/0000-0002-3616-2621 that by 2022, the machine-to-machine (M2M) traffic flows would constitute up to 45% of the entire Internet traffic. The market share and economic impact of IoT was expected to be between 2.7 trillion to 6.2 trillion dollars by 2025 (Al-Fuqaha et al., 2015). IoT has been the center of attention for quite a while in research and development. It constitutes the platforms that use radio frequency identification (RFID) for the traceability of goods and algorithms for new solutions. It promises to evolve further in the context of cloud computing (CC), big data, networking, and social networks.

This evolution of things (devices, sensors, and actuators) connected with the Internet has brought up heterogeneity in the ecosystem of IoT, giving rise to security and privacy concerns for the users. IoT devices have become significantly prone to cyber attacks. The Mirai malware affected several vulnerable IoT devices such as printers, Internet protocol (IP) cameras, residential gateway, and baby monitors. The load of this attack was 1.2 terabits per second (Tb/s); experts labeled it to be the largest distributed denial of service (DDoS) attack on record (Frustaci et al., 2018). Not much work has been done on the privacy of users in the IoT ecosystem. Very limited work has been done on the privacy and data security of sensitive sensors and actuators. The sensors store sensitive information about the habits and patterns of the end users, including details such as when they are present at home, when they leave, and when guests arrive. This could also be perceived as a violation of privacy (Psychoula et al., 2019). There remain big questions regarding whether the data of users are being profiled based on identities, where the data are being stored on the cloud, and for what purpose. Psychoula et al. (2018a) described the data-retention-time concerns and privacy concerns for people, especially the younger group. This study highlighted that women care more about privacy than men. Psychoula et al. (2020) introduced a privacy-risk awareness framework to enable privacy-preserving data management and suggested integrating privacy into wearable IoT devices.

IoT devices are gaining ground in smart homes and health care systems. They have been used to address sleep disorders. Fallmann and Chen (2019) highlighted the importance of wearables for sleep monitoring and assessment. Sensors were used in Doppler radar devices and smartwatches to collect data. Dhelim et al. (2021) highlighted the new research area of artificial social intelligence in mental and behavioral disorders. Such applications predict the mental health condition of patients. Chen LM et al. (2012) analyzed smart homes and activities of daily living. Okeyo et al. (2011) presented a novel approach in learning and behavior models. Smart health care and smart homes are the applications of IoT in digital health and assisted living. Vehicular ad hoc networks (VANETs), mission-critical applications, and control systems are also the applications of IoT (Javed et al., 2017). Without the incorporation of privacy, security, and standardization in the IoT architecture, there is a huge risk in the functionality and reliability of such applications.

To deliver quality products to the consumers in the market, IoT needs a standard architecture. To meet the challenges of IoT, its architecture should be revised. This can be achieved only through a refined reference architecture. Many organizations are working on the building blocks of IoT, following different standard bodies such as the International Organization for Standards (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), World Standards Cooperation (WSC), Electronic Product Code Global (EPCglobal), China Electronics Standardization Institute (CESI), and National Institute of Standards and Technology (NIST) (Solapure and Kenchannavar, 2016). There is a need to make the standard bodies converge to address the IoT ecosystem as a whole. Standardization leads to interoperability, which enhances the integration and exchange of information between distributed systems (Al-Qaseemi et al., 2016).

Pan et al. (2022) adopted a federated-learning mechanism, incorporating energy security and information privacy to mitigate the concerns in energy harvesting technology. Energy harvesting has a propitious future in IoT as it helps overcome the vulnerabilities and energy limitations in the context of the limited battery capacity of IoT. They proposed a joint protection framework for both energy security and privacy leakage but limited its application to energy harvesting technology rather than the complete IoT architecture.

The Internet Architecture Board (IAB) has defined communication models as device to device (D2D), device to cloud, device to gateway, and back-end sharing models. Each model has its way of communication. IoT devices are usually resource-constrained entities, containing limited processing, power, and storage capabilities. The combination of multi-functional devices and sensors is extremely effective for communication with each other and the Internet. This physical world, using these smart devices, is connected to cyberspace and IoT. These physical objects are equipped with RFID tags, near-field communication (NFC) tags, and electronic bar codes, which can be scanned by smartphones, tablets, and other smart devices integrated with RFID/NFC readers (Kraijak and Tuwanut, 2015). The structure of the paper is shown in Fig. 1. There is a need for a modular and interoperable architecture that leads us toward a standard architecture for IoT, just like the Open Systems Interconnection (OSI) layered model for network communications. Systemic privacy flaws are found in popular IoT devices from manufacturers such as iHome, Merkury, Momentum, Oco, Practecol, TP-Link, Wyze, and Zmodo. These devices can be purchased from popular retailers such as Walmart, Best Buy, and Amazon (O'Donnell, 2019). There is a need to fully develop a privacy-federated IoT security reference architecture (PF-IoT-SRA) that could help develop a standard and facilitate implementation of privacy and security metrics from the root in the architecture of IoT.

The diverse ways of data generation and utilization of the applications performing data collection, analysis, and prediction, have increased the rate of privacy issues. There must be privacy by design, a framework embedded within the IoT architecture to address all the concerns relevant to it. One of the major building blocks for IoT devices is the wireless sensor network (WSN). It is an ad hoc network that gathers data from the surroundings to deliver to the users. It consists of nodes that can detect, compute, and communicate with the devices. Low-power and lossy networks (LLNs) are used in the IoT network. These are specialized for IoT; however, IoT possesses the constraints of memory, energy, and processing power. Lightweight, encrypted algorithms are used to secure IoT ecosystems. These aspects are not used in conventional wireless networks (Alaba et al., 2017).

IoT has the potential to transform connectivity at any time to anyone from anywhere. These can connect to real-time environments, process smart and intelligent communication, and make autonomous decisions. IoT has the potential to assist our economies, transportation, environment, and health in a way that we never expected before (Kraijak and Tuwanut, 2015).

This paper focuses on federating detailed privacy and security metrics to the reference architecture of IoT. The following salient points are presented in the paper:

1. identifying the core requirements for IoT,
2. breaking down the identified core requirements into quantifiable metrics,
3. identifying the privacy and security requirements through the standards,
4. analyzing the existing IoT reference architectures based on the identified metrics,
5. identifying the shortcomings of the existing IoT reference architectures,
6. proposing a PF-IoT-SRA,
7. identifying PF-IoT-SRA's countermeasures against major IoT threats and attacks, and
8. validating the proposed PF-IoT-SRA.

The contribution of this work is the critical analysis of recent IoT architectures on the detailed requirements of IoT and the metrics of privacy and security. The analysis is comprehensive and includes the privacy metrics which none of the previous studies have incorporated. We propose a novel IoT reference architecture that covers all the security and privacy concerns of the stakeholders. This paper identifies the countermeasures against major threats and attacks in the IoT ecosystem. It is a step toward standardization as we validate our proposed architecture through the architecture trade-off analysis method (ATAM).

2 Gaps and related works

A systematic literature review conducted in 2019 highlighted the existing IoT architectures, their evolution from the initial phases of 2008 through 2018, and concerns regarding security and privacy (Alshohoumi et al., 2019). The study compared the evolution of architectures and defined the architectural stack, challenges, the techniques used, and critical issues of security and privacy. The initial architectures conveyed a basic meaning of IoT, which lacked a sound description of its nature. Advanced architectures provide a comprehensive meaning of

IoT, explaining the data transmission, collection, processing, and dissemination processes. Therefore, the architecture stack has been improved in addressing challenges such as scalability, interoperability, extensibility, and management. However, none of the evolving IoT architectures addresses the concerns of privacy, which is considered to be a critical factor in IoT sustainability and success.

Hu et al. (2019) proposed an open IoT architecture with a newly defined concept of software-defined device. The concept has been adopted from software-defined networking. They designed a centralized logical controller to manage physical devices and incorporated a software-defined device layer between the network and application layers. Software-based control management has been done with the virtualization of device resources. However, this architecture does not incorporate privacy and security metrics.

There must be a comprehensive architecture model that homogenizes heterogeneity in IoT. Division of the functionality to the elements and data flow is known as a reference model. These requirements are controlled by the reference architecture to form the supersets of functionalities, structures, mechanisms, and protocols. The requirements on which the analysis is done are defined by different consortia and manufacturers. The International Telecommunications Union Telecommunication Standardization Sector (ITU-T) reference model and some areas have been highlighted which need to be addressed in upcoming work (Torkaman and Seyyedi, 2016).

Little work has been done to secure the sensor data after transmission. Hence, there is a need for a privacy-preserving mechanism to protect the data against malicious attacks and unauthorized access. Privacy-aware IoT frameworks will ensure

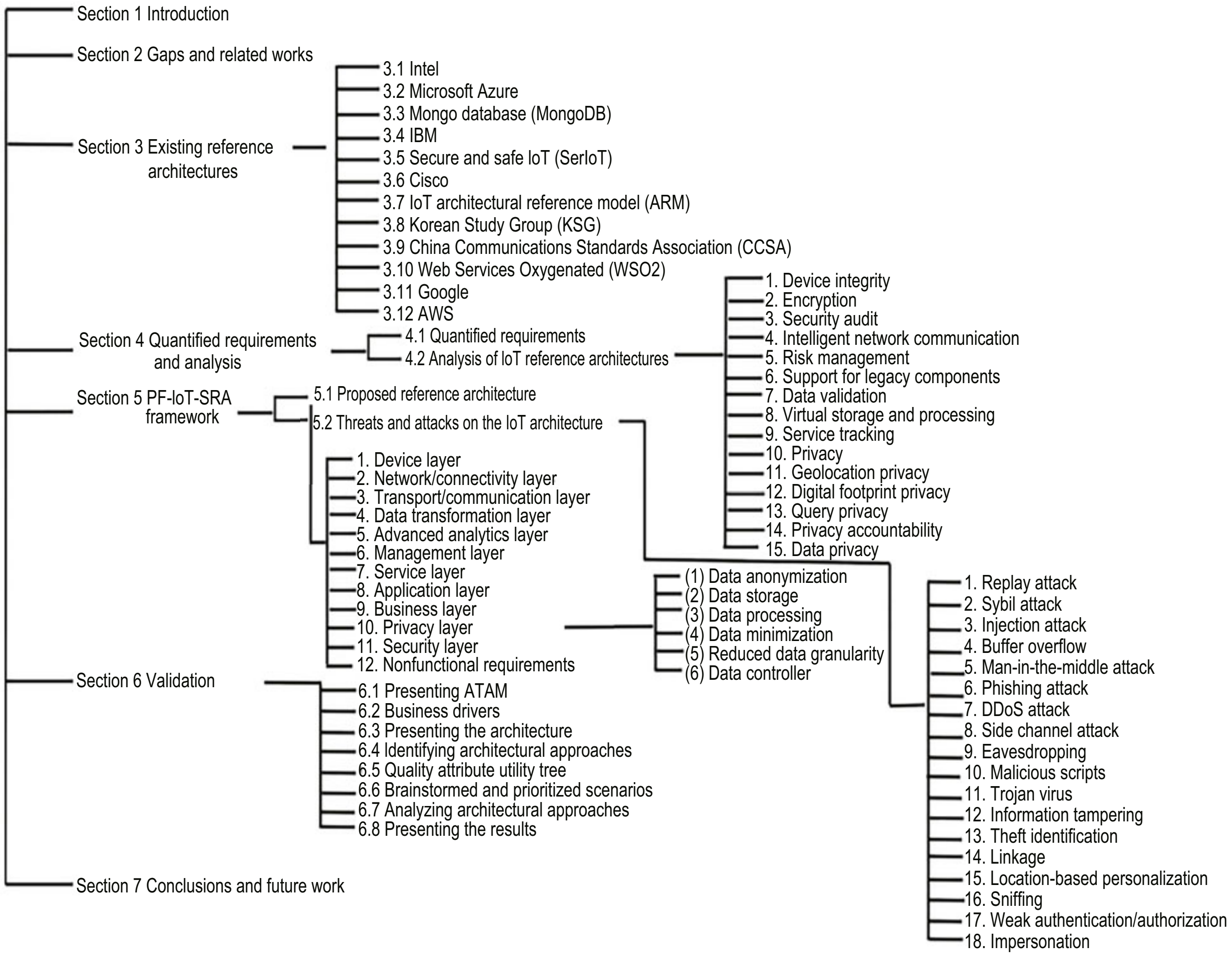
Section 1 Introduction
Section 2 Gaps and related works
Section 3 Existing reference architectures
3.1 Intel
3.2 Microsoft Azure
3.3 Mongo database (MongoDB)
3.4 IBM
3.5 Secure and safe IoT (SerIoT)
3.6 Cisco
3.7 IoT architectural reference model (ARM)
3.8 Korean Study Group (KSG)
3.9 China Communications Standards Association (CCSA)
3.10 Web Services Oxygenated (WSO2)
3.11 Google
3.12 AWS
Section 4 Quantified requirements and analysis
4.1 Quantified requirements
4.2 Analysis of IoT reference architectures
1. Device integrity
2. Encryption
3. Security audit
4. Intelligent network communication
5. Risk management
6. Support for legacy components
7. Data validation
8. Virtual storage and processing
9. Service tracking
10. Privacy
11. Geolocation privacy
12. Digital footprint privacy
13. Query privacy
14. Privacy accountability
15. Data privacy
Section 5 PF-IoT-SRA framework
5.1 Proposed reference architecture
5.2 Threats and attacks on the IoT architecture
1. Device layer
2. Network/connectivity layer
3. Transport/communication layer
4. Data transformation layer
5. Advanced analytics layer
6. Management layer
7. Service layer
8. Application layer
9. Business layer
10. Privacy layer
11. Security layer
12. Nonfunctional requirements
(1) Data anonymization
(2) Data storage
(3) Data processing
(4) Data minimization
(5) Reduced data granularity
(6) Data controller
1. Replay attack
2. Sybil attack
3. Injection attack
4. Buffer overflow
5. Man-in-the-middle attack
6. Phishing attack
7. DDoS attack
8. Side channel attack
9. Eavesdropping
10. Malicious scripts
11. Trojan virus
12. Information tampering
13. Theft identification
14. Linkage
15. Location-based personalization
16. Sniffing
17. Weak authentication/authorization
18. Impersonation
Section 6 Validation
6.1 Presenting ATAM
6.2 Business drivers
6.3 Presenting the architecture
6.4 Identifying architectural approaches
6.5 Quality attribute utility tree
6.6 Brainstormed and prioritized scenarios
6.7 Analyzing architectural approaches
6.8 Presenting the results
Section 7 Conclusions and future work

Fig. 1 Structure of the paper

the privacy and security of data collection, transmission, and usage. Psychoula et al. (2019) proposed a privacy-preserving architecture for IoT which converged to CC. An efficient privacy-preserving deep learning mechanism in a privacy layer was proposed, and physical unclonable functions (PUFs) were used for identity management and authentication. Farha et al. (2021) introduced a PUF-based authentication to access remote devices. The authentication is based on static random access memory PUF. The output of PUF is tested in different environmental conditions. Psychoula et al. (2018a) introduced a new method for privacy preservation and highlighted the lack of research on it using deep learning. Psychoula et al. (2018b) proposed a new encoding technique in ambient assisted living and health care data environments.

The abrupt development of microelectronic technology has made the size of IoT devices smaller. The size does not have any effect on its functionality as the range of functions is increasing. The increase of functions whereby these devices are interconnected everywhere in the IoT ecosystem has given rise to security and privacy challenges. Yao et al. (2021) introduced a security architecture for IoT, which divides the physical objects into three stages, i.e., pre-working, in-working, and post-working, to explain complicated security and privacy issues. This work does not incorporate the standard requirements of security and privacy for a secure IoT architecture.

IoT standardization bodies such as ISO/IEC Special Working Group-5 (SWG5) of the Joint Technical Committee-1 (JTC1) submitted a report on IoT reference architectures and frameworks (ISO/IEC, 2014). In this report, a layered IoT reference architecture was proposed by the Korean Study Group (KSG).

In general, IoT devices have limited computation power and storage capacity, but CC has catered to this limitation by increasing computational power and storage capacity by relying on the sharing of resources. Therefore, the integration of CC and IoT seems to be a promising solution. Pierleoni et al. (2019) compared the performance of three main cloud platforms: Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure. These cloud platforms have integrated CC into reference architectures of IoT. The study did not declare a winner among the three. The strategies applied for the data-driven IoT architecture guide us toward development and complexity and ensure that the IoT solutions remain scalable, robust, and flexible. These strategies enable us to achieve security by design and through the layered architecture approach (Gerber and Kansal, 2017).

The Seventh Framework Program (FP7) research project of the European Union (EU) has reinforced the reference architecture, paving way for the development of a concrete architecture. This reference architecture provides a high-level perspective to construct a solid building block architecture (Bassi et al., 2013).

In a previous paper (Li and Palanisamy, 2019), legal principle support was analyzed to implement privacy enhancing technologies (PETs) at the layer of an IoT architecture model to fulfill the requirements of users interacting with the IoT ecosystem.

3 Existing reference architectures

Existing reference architectures possess specific system designs and architectural patterns. Their structural frameworks and functions are highlighted below.

3.1 Intel

The reference architecture of Intel is shown in Fig. S1 (see the supplementary materials for Figs. S1–S14). It is a layered architecture (McKinney, 2015).

1. Communications and connectivity layer

For data ingestion and device control, the Intel IoT reference architecture uses broad protocol normalization and control systems. It uses multiprotocol data communication between the gateways and devices. It uses personal area network (PAN), local area network (LAN), and wide area network (WAN). PAN/LAN usually connects to the edge nodes of the sensors, actuators, devices, control systems, and assets (Iqbal et al., 2020). PANs are more constrained in comparison with LANs in terms of antenna distance and battery life. WAN can be the corporate network for the Internet, fourth/fifth-generation (4G/5G) mobile networks, or satellite networks.

2. Data layer with analytics

This layer provides customer value through data analytics and controlled closed-loop systems. These analytics are distributed across the cloud, gateways, and smart end-point devices. The advantage of this distribution is that it provides flexibility to provide time-critical and computation-intensive applications.

3. Management layer

This management layer comprises the managed devices, which consist of a management agent that executes management in the device. It has the main management functionality, which consists of updated applications, operating systems, discover registers, and provision of new devices. It manages data flow, destination, storage policy, uploading of stream data, alarms, notifications, organizations, and user access rights.

4. Control layer

This layer separates the management layer into the management and control planes (control objects, policies, and application programming interfaces (APIs)).

5. Security layer

The Intel IoT reference architecture provides a security software product portfolio for the developers to deliver interoperable and scalable solutions. This security is implemented at three phase end-points, i.e., device level, network level, and cloud level.

3.2 Microsoft Azure

The Microsoft Azure IoT reference architecture is as shown in Fig. S2. This architecture is based on the cloud-native and microservices. These IoT subsystems must be independently deployed and built as discrete services. This allows greater flexibility in updating the systems and choosing the right technology on a subsystem basis (Microsoft, 2018).

1. Devices, device connectivity, field gateway (edge devices), and cloud gateway

IoT edge devices are connected through the field gateway. This connection results in edge intelligent capabilities. Raw telemetry and aggregation of data are enabled. Connectivity patterns are direct devices connected to the cloud gateway via the field gateway. This option is very useful for devices that use industry standards such as the constrained application protocol (CoAP). Connectivity via a custom cloud gateway requires some form of custom processing for the devices that need a translation of the protocol.

2. Data transformation

It manipulates and aggregates the telemetry stream either before or after it is received by the cloud gateway, i.e., the IoT hub. This is done by converting the binary stream data to JavaScript Object Notation (JSON). It integrates IoT hub and Azure functions for the translation of the telemetry data before they are received at the IoT hub.

3. Machine learning

This subsystem in the architecture is intelligent and learns from data and experience to respond without explicit programming. Predictive maintenance is programmed through machine learning (ML). Azure ML fulfills all such requirements.

4. User management

This subsystem allows user management and capabilities, such as command and control, upgrading the firmware, and user application capabilities.

5. Data flow and stream processing

Data records go through different stages: storage, routing, analysis, and action/display. Memory caches, temporary queues, and permanent archives included in storage routing involve the dispatching of data records to the end-points for analysis and actions. Analysis puts the data records through certain conditions that can result in different output data. These records are available for display and actions, such as emails, instant messages, incident tickets, customer relationship management (CRM) tasks, and device commands.

6. User interface and reporting

User interface (UI) and reporting, no matter whether it be a website, mobile, or desktop application, provides access and visualization for data analysis, discovery through registry, and command and control capabilities. It provides interaction with the live dashboards.

7. Business system integration

This layer is responsible for the downstream business such as CRM, enterprise resource planning (ERP), and line of business (LOB) applications. It includes service billing, customer support, dealers, service stations, third-party data sources, and job tracking.

8. Warm storage and cold storage

The data should be available in the database (DB) within seconds when they are absorbed into the cloud from the device. Warm storage stores the easily accessible data to the last known state per device. All the data are kept in warm storage with low latency, high throughput, and query capabilities. The cold storage might not be as quick or frequent, but can be very helpful for reporting, analysis, and ML.

3.3 Mongo database (MongoDB)

Apart from the DBs, storage, pre-aggregation, and advanced analytics using the aggregation framework, MongoDB plays an essential role in the IoT solution and presents a reference architecture (Mongo, 2019) for IoT as shown in Fig. S3.

1. Edge gateways

These are high-powered devices based on the same network as the sensors, which also communicate with them. These edge gateways are used for data collection, filtering, offline data storage, and local aggregation. These can also communicate with the backend systems for analytics and data storage. MongoDB realm software development kit (SDK) allows uni- or bi-directional sync between the edge gateway and the MongoDB realm.

2. Remote management

It monitors and manages the environment. Non-structured query language (NoSQL) DB is used for application development and object modeling. The management devices are abreast with the processed events so that the end users can see the alerts on the mobile devices and respond to them in a real-time environment.

3. Data storage

Things in IoT generate a huge amount of data, which requires storage for analysis and real-time usage. MongoDB, the best platform for IoT data storage, gives access to both real-time and batch-based workloads against the MongoDB cluster. This bypasses data extract, transform, and load (ETL) for batch analysis. MongoDB Atlas is a service that allows storing archived data in simple storage service (S3) buckets.

4. Real-time analytics

It processes high volumes of data connected to the assets in real time. It allows the organization to flag the event and follow up later whenever it is urgent.

5. Stream analytics and event processing

Stream analytics performs queries and actions on real-time data. MongoDB can be used as the data source and data destination for streaming platforms such as Apache Spark and MongoDB. MongoDB enables the applications to use event-driven processing to respond to the changes.

6. Advanced analytics

This layer prevents system failures. ML, which includes advanced analytics, prevents system failures by predicting the component failure. Apache Spark is a cluster computing system that provides API in Java, Scala, Python, and R. It supports libraries such as MLlib for ML and Graph X and Spark for graph processing and streaming.

7. Visualizing IoT data

MongoDB provides custom dashboard as well as third-party platform for visualization. MongoDB charts can visualize complex data, arrays, and subdocuments, providing a visual representation of performance.

8. Security

MongoDB Atlas has been incorporated and audited to meet the privacy and compliance standards such as service organization control (SOC) type-2 and privacy shield. This supports authentication mechanisms such as salted challenge response authentication mechanism (SCRAM), X.509 authentication, lightweight directory access protocol (LDAP) proxy, and Kerberos. For access control, it follows role-based access control. For network protection and encryption, it uses and supports transport layer security (TLS)/secure socket layer (SSL) network encryption.

3.4 IBM

The reference architecture presented by IBM with the respective cloud components is shown in Fig. S4. This is a three-tier architecture consisting of edge, platform, and enterprise tiers. The edge deals with data collection and transmission. The platform tier deals with analysis, API management, and visualization. The enterprise tier deals with enterprise data, enterprise user directory, and applications (dos Santos et al., 2020).

1. User layer

This layer consists of IoT users and end users. IoT users are persons or automated systems that allow user applications to achieve the goal. The end user application is an application that a user uses on smart-phones, tablets, and specialized IoT devices.

2. Physical entities

These are the things that are subject to sensor measurement and actuator behaviors. This layer differentiates the entities and devices that sense and act on them.

3. Device

The device layer consists of sensors, actuators, firmware, network connection, and UI. This includes an agent that supports the device management protocol that gives remote management capabilities through firmware.

4. IoT gateway

The gateway is an essential decoupling element that connects one or more devices with the network and the Internet. The local network allows the devices to communicate with the local IoT gateway.

5. Peer cloud

It is a third-party cloud system that provides services to bring data to the IoT platform. These peer clouds can contribute to IoT systems and also provide competence in the IoT architecture.

6. Edge services

These include a domain name system (DNS) that translates the uniform resource locator (URL) of the Web resource to the IP address of the system, which can then deliver the resource.

7. IoT transformation and connectivity

It enables secure connectivity from IoT devices and routes the high volumes of messages to the right components. The key capabilities in this domain are secure connectivity, scalable messaging, and scalable transformation.

8. Application logic

It is an event-based model that includes trigger, action, and rule-based programming of IoT application logic. It controls the workflow.

9. Analytics

Discovery and communication patterns in IoT data improve and predict business performance. Cognitive capabilities create intelligent systems, which themselves learn and adapt for augmented human intelligence. Actionable insight drives actions that are used by the business applications stored in the data repositories.

10. Transformation and connectivity

It enables secure connections to enterprise systems. It can filter, aggregate, and modify the data as they move among the cloud, IoT, and enterprise systems. It includes enterprise secure connectivity, transformation, and enterprise data connectivity.

11. Enterprise data

Enterprise data consist of the metadata about the data and system of record for enterprise applications. This sort of data flows directly to data integration or the repositories providing the feedback loop to the analyzed IoT system.

12. Enterprise applications

To address the business goals, enterprise applications consume cloud data and analytics. These consist of customer experience, new business models, financial performance, risk analytics, economics, and operations.

13. Security

It addresses the importance of the security layer in the reference architecture. Areas to consider are identity, access management, data protection, security monitoring, analysis, response, system application, and solution life cycle management.

3.5 Secure and safe IoT (SerIoT)

SerIoT (Domanska et al., 2018) is a project funded by EU's Horizon 2020 research and innovation program. The reference architecture presented by SerIoT is followed by the ISO/IEC 30141 standard. The architecture is as shown in Fig. S5. This architecture targets security-driven solutions to address the threats.

1. Physical entity domain

This domain consists of the sensed and controlled physical objects in the IoT system. It consists of the physical and virtual entities that are responsible for monitoring, sensing, and controlling.

2. Sensing and controlling domain

The sensing and controlling domain (SCD) provides critical information about the environment to other domains in the IoT system through proximity networks that use specialized protocols.

3. Operations and management domain

It contains a set of functions that manage, monitor, and optimize systems and their performance in real time. Managers and system operators maintain the health of the system.

4. Resource and interchange domain

In terms of resources, the domain interacts with entities, applications, services, and systems. The resources can be physical or monetary. The domain includes the processing of data, including data assurance, quality, transformation, distribution, and storage.

5. Application service domain

It consists of business services and service providers. These service providers interact with the users, as well as the sensors and actuators, to gain the data from physical objects.

6. User domain

It consists of stakeholders and actors in the IoT system. It can also be an individual, household, society, an organization, or government department.

3.6 Cisco

Cisco proposed a seven-layered reference architecture that can lead to standardization worldwide (Cisco, 2014). The architecture is as shown in Fig. S6.

1. Physical devices and controllers

This layer consists of sensors, devices, machines, and things in IoT. Physical devices and controllers generate data and convert analog data to digital.

2. Connectivity

The function of this layer is to transmit the information between the devices and the network, and across or between the networks.

3. Edge computing

This layer focuses on high-volume data analysis and transformation. This layer involves data evaluation, formatting, expansion, distillation, and assessment. It also deals with packet and content inspection, threshold, and event generation.

4. Data accumulation

This layer captures the data and puts them on rest in the memory or disk. These applications usually access the data when necessary. The event-based data are converted to query-based data for processing. It also reduces the data through filtering.

5. Data abstraction

It abstracts the data interface for applications. This layer creates schemas and views of the data according to the application's needs. It combines the data from multiple sources. To fulfill the client applications, it filters, projects, and reformats the data. It also reconciles differences in data shape, semantics, access control, and security.

6. Application

It varies based on device data and business needs. The example of the applications can be ERP or business applications, mobile applications, business intelligence reports, and analytic applications.

7. Collaboration and processes

It includes people and processes. People should be able to collaborate and communicate to make use of the information.

3.7 IoT architectural reference model (ARM)

The representation of IoT ARM (Bassi et al., 2013) is given in Fig. S7. This proposed architecture in FP7, a research project by the EU, helps us toward the construction of a concrete architecture.

1. Functional view

The functional view of IoT ARM is shown in Fig. S8. It consists of nine functional groups and components.

2. Information view

The smart objects interact with each other to exchange information among the external entities. Information between the entities is handled and stored to keep track of the life cycle.

3. Deployment and operation view

It investigates how components communicate with each other, encompassing quality, requirements, applicability, and architectural tactics.

3.8 Korean Study Group (KSG)

KSG has presented this reference architecture for IoT from two view points, i.e., functional and communication. Six blocks are present in the functional representation of the architecture (ISO/IEC, 2014). In Fig. S9, the functional view of the IoT reference architecture proposed by KSG is presented.

1. Communication viewpoint

This viewpoint consists of a connection method and interoperability. The connection method consists of IoT devices that are directly connected with the Internet. Due to implementation issues, some are connected through the gateways to avoid such errors even with the ability to connect directly. The other devices communicate indirectly through intermediate nodes.

2. Functional viewpoint

It consists of the following blocks:

(1) Infrastructure. It consists of the basic structure containing hardware, network, and system resources that are necessary for the core operations.

(2) Core functions. As shown in Fig. S9, this layer contains knowledge, semantics, resource management, connectivity, and network management, integrating security and privacy concerns.

(3) Application and services support functions. This layer provides an abstraction to the components and their core functions, making it easy for the upper layer.

(4) Tools. This layer provides tools for the development of new applications.

(5) Test and deployment. It deals with the testing of the developed IoT system before it becomes available for the users.

The detailed core function representation of the reference architecture by KSG is shown in Fig. S10.

3.9 China Communications Standards Association (CCSA)

The representation of the IoT reference architecture proposed by CCSA (Chen SZ et al., 2014) is shown in Fig. S11.

1. Sensing layer

It consists of the sensors, controllers, RFID readers, and location-sensing devices of the network layer. This layer supports modularization, and its components can self-adapt, operate intelligently, and configure by themselves.

2. Network and service layer

It consists of the resource administration platform, application and support platform, and backbone network. This layer supports control functions such as access control, authorization, authentication, and mobility.

3. Application layer

This layer deals with the modularization of common functions that can be used in the development of applications by the developers.

3.10 Web Services Oxygenated (WSO2)

The reference architecture of the IoT presented by WSO2, shown in Fig. S12, consists of five horizontal and two vertical layers. The cross-cutting vertical layers consist of the device manager, identity, and access management (Fremantle, 2015).

1. Device layer

The device layer consists of the devices that can communicate with the Internet with a direct (Arduino with Arduino Ethernet, Raspberry pi-WiFi) or indirect (ZigBee through the gateway or Bluetooth connection through a mobile phone) connection. This architecture suggests having a unique, unmodifiable identifier, as well as Open Authorization 2.0 (OAuth2) Refresh and Bearer token, stored in electrically erasable programmable read-only memory (EEPROM).

2. Communications layer

This layer manages the connectivity of IoT devices. The most commonly used protocols for communication are the hypertext transfer protocol/hypertext transfer protocol secure (HTTP/HTTPS), message queuing telemetry transport (MQTT 3.1/3.11), and constrained application protocol (CoAP).

3. Aggregation/bus layer

It incorporates legacy protocols and correlates and maps the device identity (ID) to the user's ID. This layer incorporates the policy enforcement point (pep) for policy-based access.

4. Event processing and analytics layer

This layer processes events taken from the bus layer and stores data in the DB. It also performs analytics on the data coming from the aggregation layer.

5. Client/external communication layer

This layer uses all the functionalities such as Web-based portals, to communicate with the devices, dashboards, and APIs that need to communicate with the systems outside the network.

6. Device management

This layer communicates with the devices through protocols and gives control of devices at both individual and bulk levels. It works with the identity and access management layer and maintains the identities of the devices to map them to their users.

7. Identity and access management

This layer provides services such as OAuth2 token issuing and validation, identity services such as security assertion markup language-2 (SAML2), single sign-on (SSO), OpenID, and LDAP, policy management, and access control.

3.11 Google

GCP possesses tools to connect, store, process, and analyze data both at the edge and in the cloud. It has three essential components: device, gateway, and cloud (dos Santos et al., 2020). In this reference architecture, the device can be hardware or software and can connect directly or indirectly to the Internet. The reference architecture is shown in Fig. S13. The services of the gateway are for devices that are not directly connected to the Internet for cloud services. The gateway processes the data on behalf of a group of devices. The data are collected by the devices and sent to the cloud platform through the gateway. The data are transmitted to the cloud IoT core. The devices that are using the MQTT protocol send the data to the same global end-point regardless of the source region or location. The data are sent to the cloud publish/subscribe (Pub/Sub) after being received through the cloud IoT core. The data processed through the cloud IoT core or from the cloud Pub/Sub, message queue, and event broker can take several different paths. The cloud ML engine anonymizes the data stored on Google cloud storage. Control configuration in the Google IoT reference architecture allows the data to be sent back to IoT devices by the cloud IoT core.

This reference architecture incorporates edge computing with rapid response, thus reducing latency and the number of round trips. Unconstrained by connectivity limitations, edge devices locally store and process the data to maintain reliability in the operations.

The cost of network bandwidth, data storage, and computational power can hinder the deployment of solutions by the customers. The use of edge computing can help businesses spread the computational load to the cloud and edge devices for cost-effectiveness and good return on investment (ROI).

The cloud IoT core in the context of Google cloud consists of subsystems, i.e., protocol bridge and device manager. The data are transmitted to the cloud IoT core using TLS and protocol bridge using secure MQTT port and HTTP/S port.

3.12 AWS

The IoT reference architecture presented by AWS (dos Santos et al., 2020) is shown in Fig. S14. This architecture provides secure bidirectional communication between the Internet and the devices.

1. Device gateway

This layer helps the devices securely and efficiently communicate with AWS IoT.

2. Message broker

The communication between the devices and AWS IoT is usually done by a message broker that distributes data to the devices and core AWS services.

3. Device shadow

This layer maintains the states of online or offline devices. The applications should communicate with the devices. The data are maintained for the connected applications when offline and are synchronized back to their states when online to the device shadow service.

4. Rule engine

For storage and processing, the data are transferred from the message broker to AWS services through the rule engine. The expressions defined in the rule engine can be used to update, insert, or query a DynamoDB table.

5. Security and identity

The communication is secured by X.509 certificates for authentication. The credentials should be secured. Both the message broker and rule engine use the AWS security and identity layer to send the data securely to the devices and AWS services. The core IoT rule engine can connect to the following AWS services:

(1) Amazon DynamoDB. This is a scalable and NoSQL DB service that gives us good and predictable DB performance.

(2) Amazon Kinesis. It collects, processes, and analyzes the streaming data to know the new information. This layer uses audio, video, and application logs for ML, data analytics, and applications.

(3) AWS Lambda. This executes the code without servers. The mobile application and Web can be used to directly execute the code from AWS IoT data automatically.

(4) Amazon simple storage service (S3). In Amazon S3, the data can be stored and retrieved anytime from anywhere through the Web. These data can also be sent for storage purposes.

(5) Amazon simple notification service (SNS). Amazon SNS is a Web service that enables applications, users, and devices to send information to and receive information from the cloud.

(6) Amazon simple queue service (SQS). This is a message queuing service used to decouple and scale services, distributed systems, and applications.

4 Quantified requirements and analysis

4.1 Quantified requirements

There are some specific and unique requirements of the IoT network, which need to be met while designing an IoT network. Reference architectures have been analyzed based on the requirements quantified through the standards. Twenty-two requirements with metrics have been identified. These are divided into two categories, i.e., functional and nonfunctional requirements. The functional requirements are further expanded into metrics. This is done to extract a tangible meaning out of the requirements and make its deployment to the network easy. It must adhere to the nonfunctional requirements. The quantifiable metrics are shown in Fig. 2.

4.2 Analysis of IoT reference architectures

We have analyzed 12 reference IoT architectures based on the quantifiable requirements and metrics. We have extracted these requirements from the standards. We have evaluated, through detailed literature study, whether a reference architecture from a particular vendor or organization addresses that particular metric. The analysis is shown in Table 1. Through this analysis, we have identified the shortcomings of the reference architectures and identified the metrics that have been excluded from a particular reference architecture. The following requirements are absent in most of the reference architectures analyzed.

1. Device integrity

The reference architecture of the IoT proposed by various organizations, research projects, and vendors must incorporate the integrity of the devices, so that the data cannot be altered or destroyed by unauthorized users. The integrity of data is very important for the reliability of IoT systems. Data of IoT applications must not be altered through any sort of malicious activity, and the reference architectures must support such a requirement in IoT systems. This ensures the security of the system.

2. Encryption

To improve the security of IoT systems, encryption algorithms and techniques could be applied and analyzed, no matter whether the mechanism is present in the architecture or not. The storage and communication of the data must be encrypted, with private data communication in the form of hidden

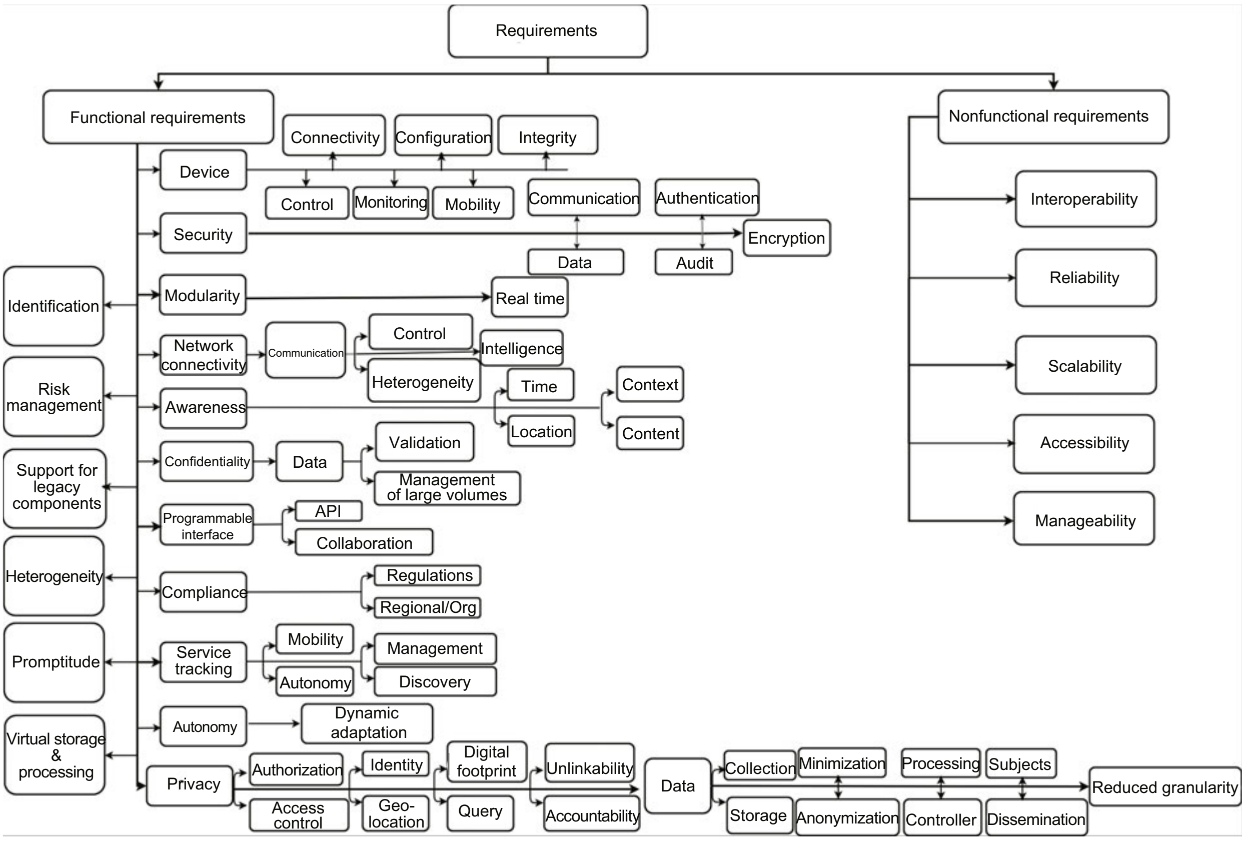

Fig. 2 Quantifiable metrics (API, application programming interface)

Table 1 Analysis of existing IoT reference architectures

Requirement			Intel	Microsoft Azure	Mongo database	IBM	SerIoT	Cisco	IoT ARM	KSG	CCSA	WSO2	Google	AWS
Functional	Device	Connectivity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Control	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
		Configuration	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓
		Monitoring	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
		Integrity	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
		Mobility	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓
	Security	Communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Data	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓
		Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Audit	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓
		Encryption	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
	Modularity	Real time	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
	Identification		✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
	Network connectivity communication	Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Heterogeneity	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Intelligence	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗
	Risk management		✗	✓	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗
	Awareness	Time	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
		Location	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
		Context	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✓	✗
		Content	✓	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗
	Support for legacy components		✓	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓	✓
	Confidentiality data	Validation	✗	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗	✓
		Management of large volumes	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗
	Heterogeneity		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Programmable interface	API	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Collaboration	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Promptitude		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Compliance	Regulations	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
		Regional/ organizational	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓
	Virtual storage and processing		✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓
	Service tracking	Mobility	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓
		Autonomy	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓
		Management	✓	✓	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓
		Discovery	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓
	Autonomy	Dynamic adaptation	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓
	Privacy	Authorization	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Identity	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓
		Geolocation	✗	✓	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗
		Digital footprint	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
		Query	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
		Unlinking ability	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
		Accountability	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
	Privacy data	Collection	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗
		Storage	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓
		Minimization	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
		Anonymization	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✗
		Processing	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
		Controller	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓
		Subjects	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
		Dissemination	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
		Reduced granularity	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
Nonfunctional		Interoperability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Reliability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Scalability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Accessibility	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Manageability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

✓and ✗ represent the presence and absence of a particular metric, respectively

data routing. Encryption encodes a message from the sender to the intended recipient. No user other than the intended user can read it. It consists of a secret key or password that allows the user to decrypt the message.

3. Security audit

The analysis indicates the lack of auditing mechanisms adopted by IoT reference architectures. Most of the architectures do not audit the security mechanisms implemented or conform to the information security standards. The data access, processing, and storage must have a proper purpose defined under the laws and regulations. The vulnerabilities get exposed in the form of cyber attacks such as DDoS and eavesdropping in IoT systems. These devices, when hacked or exposed, can be used as a helping hand to disrupt the services of the server. The IoT architecture must incorporate security audit.

4. Intelligent network communication

IoT devices must be intelligent in communication, and the architecture must include this particular metric, but our analysis indicates that most of the reference architectures lack this particular metric. Intelligent, autonomic, and redundant networking is required to possess the capabilities of self-healing, self-rectification, and self-selection of the path and direction of traffic. Path selection redundancy and routing of content-aware communication are required. Network flow analytics helps us come up with better efficiency and results, without any delay in communication. Congestion in network traffic can be avoided through this intelligent network communication.

5. Risk management

IoT devices have vulnerabilities and can be exposed to cyber attacks; e.g., a car that consists of sensors can be compromised and involved in a lethal accident. The risks can be calculated and avoided through risk management to counter vulnerabilities in the IoT system.

6. Support for legacy components

Outdated components need support in IoT systems, along with the updated technologies. The analysis shows a deficiency in the support of such components in the IoT reference architecture. The integration of updated and legacy components is beneficial for systems. It is good to come up with new components without completely abandoning legacy devices.

7. Data validation

Integrity is one of the major concerns in terms of security. Tampering of the data must be avoided as it affects the reliability and functionality of the system. Data validation must be incorporated in the IoT building block. Without validation, the data can be corrupted or tampered, affecting the efficiency of the system.

8. Virtual storage and processing

Large numbers of things in IoT systems collect and process a large amount of data. However, IoT devices are resource-constrained due to low power and processing capability. Since big data analytics is an essential component of an IoT reference architecture, overcoming such constraints and integrating big data require CC support in the form of virtual storage and processing.

9. Service tracking

Services such as mobility, autonomy, management, and discovery are important to be incorporated in IoT systems. The awareness of time, context, content, and location is essential for mobile services. The services must start automatically on the expiry of one service and also warn the user before its expiry. The services must start without human intervention and must not be required to start only through human command and control.

10. Privacy

Privacy of users is one of the important aspects with regard to the nature of IoT. Protection of the privacy of users must be guaranteed. As privacy is a basic right of an individual, the identities of users must not be traced back to them. Information related to them must be stored and processed under the defined purpose. These privacy principles must be applied in data collection, storage, and processing. Data anonymization and minimization techniques must be incorporated in the privacy-federated reference architecture. Authentication, encryption, access control, and authorization must also be included in the protection of users' privacy. Privacy can be achieved through confidentiality. To prevent the leakage of data, privacy requirements must be applied for data removal, requisition, and encryption.

11. Geolocation privacy

The geolocation of the user can be traced through user identities. The data must be concealed, as this type of information can be used for illegal purposes. The analysis highlights that most of the reference architectures do not value the privacy of users in terms of their geolocation. Data must not be profiled based on geolocation.

12. Digital footprint privacy

Digital footprint privacy promotes the use of privacy settings and private data communication. IoT devices are connected to the Internet all the time. Such a scenario can lead to vulnerabilities as the devices are continuously exposed to cyber attacks. Data can be traced through devices that must be secured through effective lightweight security protocols to prevent the gathering of digital footprints of the devices and their owners. Surveillance of linking accounts and private data communication, including encrypted data communication and hidden data routing, must be embedded in digital footprint privacy.

13. Query privacy

By tracking the IP address, search queries can reveal the identity of the user. Search query privacy is supposed to answer high-level data instead of raw data. Giving raw data can lead to privacy violations of users due to its secondary usage. Search query can overcome raw data through open personal data store (PDS). It gives a high-level answer to the queries instead of raw data, protecting the privacy of end users. Through analysis, we can block repeated queries that can lead to a malicious activity that discloses the data from users.

14. Privacy accountability

The data controller is responsible for the accountability of privacy in an IoT system through data collection, by defining the purpose of data collection, limiting the required data, and data dissemination. Only required data must be collected, with no trade-offs that can compromise the privacy of users. Access controls should be defined in the form of access control list (ACL) and a digital certificate. Privacy impact assessment can be done through privacy safety data sheets (SDSs) and privacy control record (PCR). The analysis shows that none of the reference architectures of IoT incorporate privacy accountability.

15. Data privacy

Data privacy must be embedded in the form of data subjects, collection, storage, minimization, anonymization, and processing. In privacy design, the data provider manages privacy.

5 PF-IoT-SRA framework

5.1 Proposed reference architecture

In this work, we propose a novel PF-IoT-SRA framework that is secured from the risks associated with IoT in terms of privacy and security. It consists of a dedicated, separate layer for privacy, with metrics that are not incorporated in previous works. The architecture, i.e., a modular and interoperable reference architecture of IoT, covers some new features at both individual and system levels. It consists of nine horizontal and two vertical layers, along with a layer that addresses the nonfunctional requirements of IoT. The new features are implemented based on the standards and shortcomings identified in the analysis of existing reference architectures. These features are described below in their respective layers. Each layer is interrelated and addresses specific metrics and functionality. It is a step toward a standard architecture as we incorporate a combined list of standards including ISO/IEC, ITU-T, and NIST. The proposed architecture is shown in Fig. 3.

1. Device layer

Edge gateway and autonomy are embedded as new features in the first layer. The devices have their unique identification and are autonomous. In case of malfunction and errors, these devices are able to configure and rectify themselves without human intervention. Rectification is done in the real-time environment supporting dynamic adaptation. Protocols used for unique identification are electronic product code (EPC), ubiquitous code (uCode), IP version 6 (IPv6), and uniform resource identifier (URI). This layer supports the edge gateway, present on the same layer with sensors and actuators. These are high-powered devices capable of initial data collection, filtering, local aggregation, analysis, and offline data storage.

2. Network/connectivity layer

The network/connectivity layer incorporates a new feature of CC. It is a serverless platform and can support many connected devices. The dispersed data of many IoT devices can be converted to the cloud IoT platform. It contains a computer network, a mobile communication network, a low-power WAN, and a CC. This layer helps in connectivity of the things with the network using connectivity protocols. The computer network uses a wired or wireless medium for connectivity, which contains the protocols shown in Table 2.

3. Transport/communication layer

Private communication and error control communication are the new features added in the third layer, which incorporates backend data sharing from the devices. Automatic communication modes are required between users and devices. Error control is important to handle the interference with the devices regarding communication and to minimize errors. Private communication helps prevent cyber

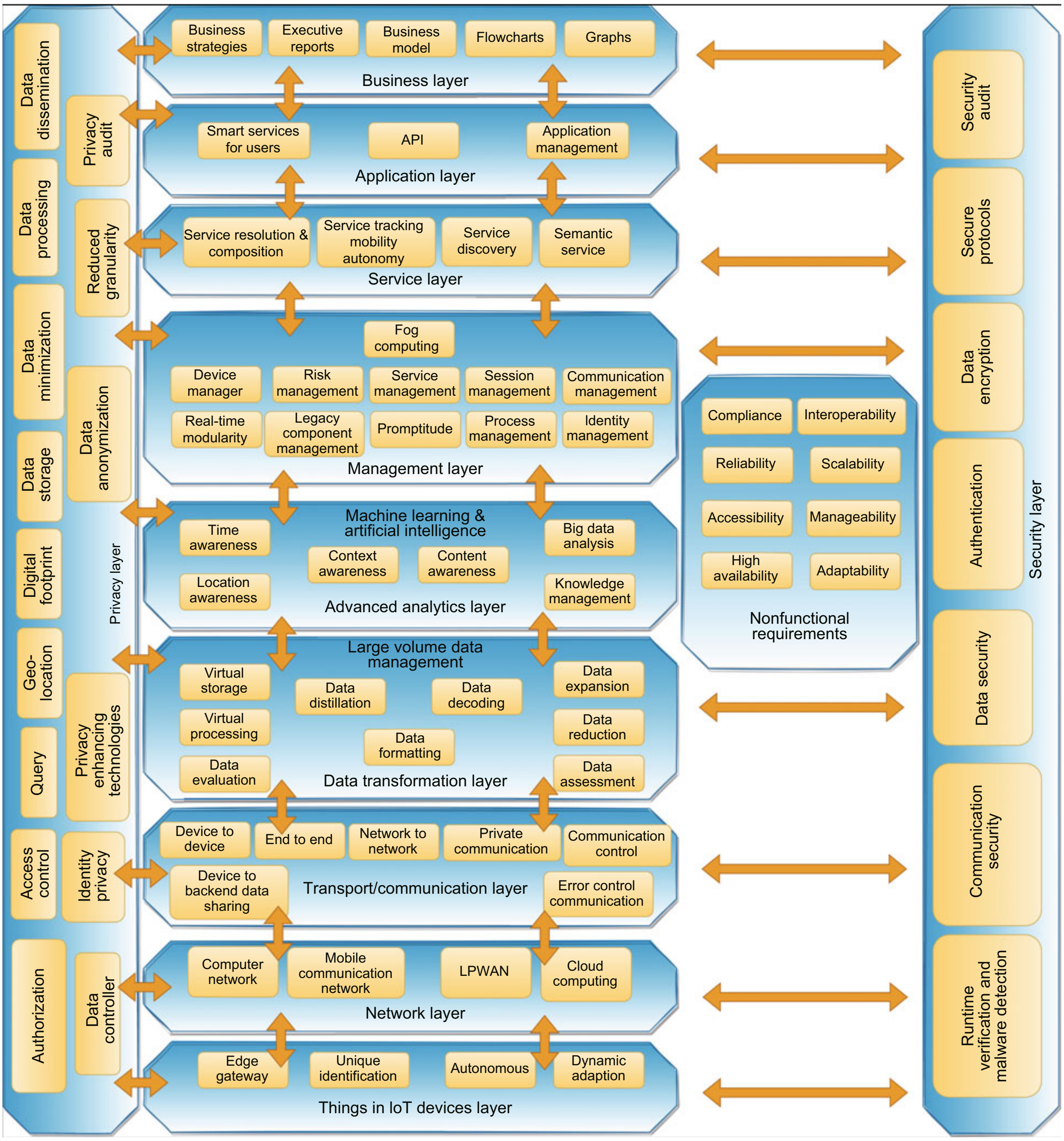

Fig. 3 Proposed reference architecture (API, application programming interface; LPWAN, low-power wide area network)

attacks through encryption. The protocols for communication are shown in Table 3.

4. Data transformation layer

Virtual storage and virtual processing are the new features introduced in the proposed architecture. The fourth layer transforms data for the upper layers through data assessment, data reduction, data decoding, data formatting, data distillation, and data evaluation. The data are evaluated and checked regarding whether they are in a suitable format for the upper layer. It handles a large amount of data; therefore, virtual storage and processing are also embedded. Big data are managed through virtual storage and processing.

Table 2 Protocols

Ethernet	LPWAN	Cellular
WiMAX	LoRaWAN	GPRS
CAN bus	LTE-MTC	2G
Wi-Fi	NB-IoT	3G
ZigBee	RPMA	4G
ANT	EC-GSM-IoT	5G
EnOcean	Weightless	
Eddy stone		
NFC		
Bluetooth		
DigiMesh		
ISA 100.11a		
IEEE 802.15.4		
WirelessHart		

2G/3G/4G/5G, second/third/fourth/fifth-generation; CAN, controller area network; EC, extended coverage; GPRS, general packet radio services; GSM, global system for mobile communications; IEEE, Institute of Electrical and Electronics Engineers; ISA, International Society of Automation; LPWAN, low-power WAN; LTE, long-term evolution; MTC, machine type communication; NB, narrow band; NFC, near-field communication; RPMA, random phase multiple access; WAN, wide area network; Wi-Fi, wireless fidelity; WiMAX, Worldwide Interoperability for Microwave Access; WirelessHART, Wireless Highway Addressable Remote Transducer Protocol

Table 3 Communication protocols

Abbreviation	Full name
IPv6	Internet protocol version 6
TSMP	Time synchronized mesh protocol
UDP	User datagram protocol
CCN	Content-centric networking
6LoWPAN	IPv6 over low-power wireless personal area network
Nano-IP	Nano-IP
Aeron	Aeron
RPL/ROLL	Routing protocol for low-power and lossy networks/routing over low-power and lossy networks
DTLS	Datagram transport layer security
uIP	Micro IP
QUIC	Quick UDP Internet connection

5. Advanced analytics layer

Location awareness is embedded as a new feature in the fifth layer. ML and artificial intelligence algorithms are applied to the data collected from the below layers to obtain the best results from the upcoming data. This includes big data analysis, content awareness, knowledge management, time awareness, and location awareness. Advanced analytics can be achieved through knowledge management, which consists of information gathering and intelligent learning. This incorporates deep business insights to predict the failure of a component through analytics.

6. Management layer

The new features of promptitude and legacy component management are incorporated in the sixth layer. After the advanced analytics layer, data will go to the management layer, which provides management services including risk management through asset categorization and risk value. Fog computing, promptitude, service management, session management, communication management, and identity management are included.

7. Service layer

Semantic service is incorporated as a new feature in layer 7. It is responsible for service resolution, composition, tracking, mobility, autonomy, discovery, and semantic service. Multicast domain name system (mDNS), universal plug and play (UPnP), physical Web, and HyperCat are some protocols used in service discovery.

8. Application layer

It incorporates smart services for users and application management as new features. Smart services are in the form of applications for the users. The management of the applications is also done in this layer.

9. Business layer

Executive reports and business strategies are new features incorporated in this layer. It provides business insights of an IoT system through graphs, flowcharts, and executive reports for the top management. These reports play a vital role in development. Strategies are also developed to capture the market. The business layer carries the profit models for the system.

10. Privacy layer

Previous works focus on assisting users with mobile application permissions, protecting data and privacy-aware video streaming. Our goal is to design an architecture that will allow the users to store and manage data according to the level of privacy they want, trading the data for services rather than allowing the individuals to view, control, and disclose their data.

Privacy of users can be ensured through the integration of privacy by design metrics to the reference architecture of IoT. This includes the privacy validation chain (PVC), which acts among the data owner, data controller, and data processor to define the purpose of the usage of user data. This acts between the data provider and data controller, which manage and assess privacy protection, respectively.

Privacy-enhancing technologies (PETs) enhance the privacy of the system. PVC answers the most important question about who is collecting the data and under what defined purpose. User authorization is required according to the predefined security policies to access IoT, followed by ACL and digital certificates.

(1) Data anonymization. This technique can remove personally identifiable information before it is used by IoT applications. It leads the data to be anonymous. This reduces the risk of identification of personal information and privacy violations. It can include the secret key encryption mechanism and k-anonymity with a large value of k, which exploits quasi-identifier attributes to preserve sensitive data. Strong identities without unique identifiers in the DB can lead to protection of privacy for the users.

(2) Data storage. To ensure minimum data storage, raw data must be deleted after deriving secondary contexts. Privacy can be enhanced by preventing the storage of long-term personal characteristics. It includes distributed data storage, limiting storage data and defining legal needs to store the user's data, purpose of storage, and encrypted data storage.

(3) Data processing. The processing of the data must be distributed and encrypted to prevent data tampering by malicious attacks. Encryption is the encoding of data in such a way that only authorized users can read the data. Those who are processing the data must not be allowed to read the data.

(4) Data minimization. It incorporates minimum knowledge discovery. Discovering the data is needed to achieve the primary objectives of an IoT application. However, the remainder of the detailed information must not be collected. Minimizing raw data intake will prevent privacy violation through secondary usage of the data. Since a long retention period can enhance the chance of malicious activity, which may breach the privacy of the user, minimization of the data retention period is an effective approach.

(5) Reduced data granularity. IoT technologies should implement a lower level of granularity because if a higher level is implemented, fine-grained data and information will result in high privacy risk.

(6) Data controller. Data subjects must be controlled through a mechanism. The data controller is accountable for the protection of privacy, including privacy auditing through systematic checking of the logs and procedures.

11. Security layer

It incorporates the new features of runtime verification, malware detection, and security audit. It consists of lightweight authentication mechanisms with communication and data security. Security audits should be done in the form of fair, clearly informed, and transparent data access. Data access must abide by laws and regulations. This layer performs runtime verification, malware detection, and data encryption. Lightweight data security protocols are shown in Table 4.

Table 4 Lightweight data security protocols

Abbreviation	Full name
ONS 2.0	Object name service 2.0
–	Reactive streams
SSI	Simple sensor interface
MQTT	Message queuing telemetry transport
CoAP	Constrained application protocol
STOMP	Simple text oriented messaging protocol
AMQP	Advanced message queuing protocol
XMPP	Extensible messaging and presence protocol
REST	Representational state transfer
LWM2M	Lightweight machine-to-machine
LLAP	Lightweight local automation protocol
DDS	Data distribution service for a real-time system
JMS	Java message service
–	Mihini/M3DA

12. Nonfunctional requirements

This layer incorporates high availability, adaptability, accessibility, manageability, reliability, scalability, interoperability, and compliance as nonfunctional requirements.

5.2 Threats and attacks on the IoT architecture

We know that IoT-based systems are vulnerable to various types of attacks. Fig. 4 shows the threats and attacks in the IoT communication environment, along with their countermeasures, as present in our proposed architecture (PF-IoT-SRA). This identifies which layer and metric will prevent these threats and attacks (Karale, 2021).

1. Replay attack

It is a network attack in which attackers analyze the traffic and use it for their own benefit (Chen KJ

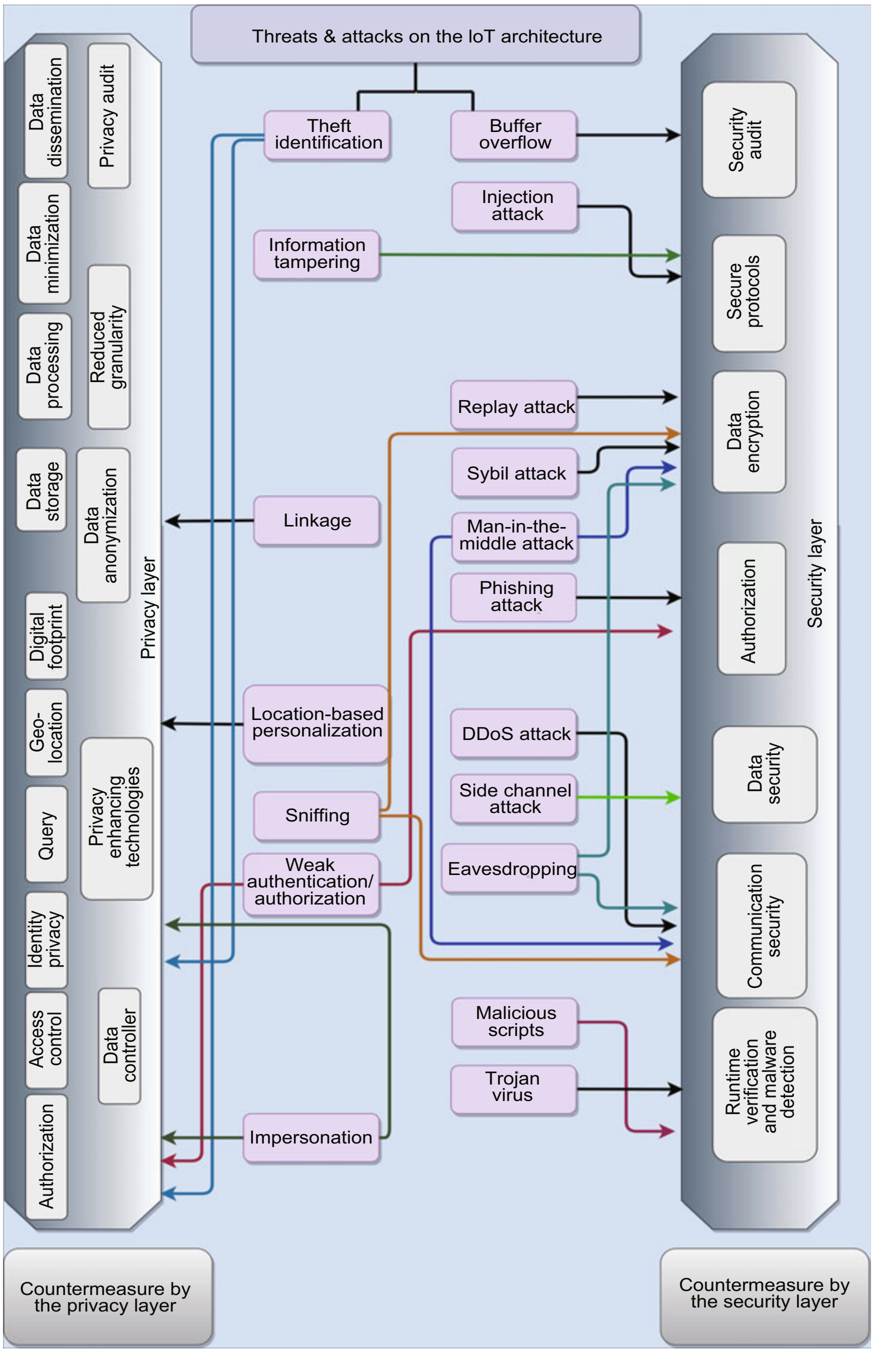

Fig. 4 Threats and attacks on the IoT architecture (DDoS, distributed denial of service)

et al., 2018). The proposed architecture has the security layer with data encryption embedded to counter such a type of attack.

2. Sybil attack

It is a network attack in which the attacker creates a bottleneck to decrease the performance of devices. Our proposed architecture has the security layer with a data encryption metric to prevent such attacks.

3. Injection attack

This attack injects a malicious code into the sensors and the network. To prevent such attacks, our proposed architecture possesses a security layer with a secure protocol metric.

4. Buffer overflow

It is a type of software-coding vulnerability that an attacker exploits. We can prevent such attacks by auditing the code. The proposed architecture possesses a security audit metric in the security layer to counter it.

5. Man-in-the-middle attack

It is a real-time network attack in which an attacker disguises himself/herself as a legitimate user. Our proposed architecture possesses a communication security and data encryption metric in the security layer to counter this attack.

6. Phishing attack

It is an application layer attack in which an attacker sends fraudulent messages to trick the user into revealing sensitive information. Our proposed architecture possesses an authentication metric embedded in the security layer to counter such an attack.

7. DDoS attack

It blocks the access of application for legitimate users through flooding. Our proposed architecture has communication security integrated in the security layer to counter this attack (Frustaci et al., 2018).

8. Side channel attack

This type of attack does not rely on the vulnerabilities of a system; rather, its attacks originate from system implementation. The data security metric in the security layer can prevent such attacks.

9. Eavesdropping

It is a type of attack in which an attacker listens, interprets, and reads the user's communication. Communication security and data encryption metrics in the security layer can counter this type of attack.

10. Malicious scripts

This type of attack exploits the vulnerabilities in a system. It is a software attack that modifies the code. Our proposed architecture has a runtime verification and malware detection metric embedded in the security layer to counter such an attack.

11. Trojan virus

It is a software attack in which an attacker steals data by disguising as a legitimate program. A runtime verification and malware detection metric in the security layer can counter such an attack.

12. Information tampering

This attack manipulates and destroys data. Secure protocols embedded in the security layer can counter information tampering.

13. Theft identification

It is a privacy breach threat that steals personal information. Our proposed architecture has identity privacy and authorization metrics in the privacy layer to counter it.

14. Linkage

Data linkage identifies records and data belonging to the same person. It is a privacy breach threat, and we have identity privacy and data anonymization metrics in the privacy layer to counter this privacy threat.

15. Location-based personalization

This privacy threat associates an identifier with the user and records the user's location. It is a privacy threat, and our proposed architecture has geolocation integrated in the privacy layer to prevent such threats.

16. Sniffing

It is a network attack that captures network traffic using packet sniffers. Our proposed architecture possesses communication security and data encryption in the security layer to counter it.

17. Weak authentication/authorization

The attacker accesses the system with brute force attack and uses default passwords against weak authentication. Our proposed architecture has authentication and authorization metrics in the security and privacy layers, respectively, to counter it.

18. Impersonation

The attacker impersonates a legitimate user to gain sensitive information. Our proposed architecture has authorization and identity privacy metrics in the privacy layer to counter it.

6 Validation

To validate the proposed PF-IoT-SRA, we have followed the industry-recognized scenario-based approach. Researchers have termed this approach better, in comparison to the questionnaire-driven and decision-based approaches. We have adopted ATAM to validate the proposed architecture. This method provides us insight into how the quality goals interact with each other and how they can trade-off each other. ATAM is the leading methodology to evaluate and validate architectures. This methodology consists of the following steps.

6.1 Presenting ATAM

ATAM evaluation can identify and expose the risks that inhibit the achievement of an organization's business goals. It is a scenario-based approach in which the proposed reference architecture is evaluated and validated through quality attributes in brainstormed scenarios. It evaluates whether an architecture meets the functional requirements addressed in the standards of NIST, ISO/IEC, and ITU-T. This results in the identification of the tradeoffs, sensitivity points, and risks associated with the architecture.

6.2 Business drivers

The following are the business drivers for IoT: (1) revenue and innovation, large investments on IoT, (2) low cost of sensors and shift from traditional to smart sensors, which have contributed to the growth of IoT businesses, (3) better customer service and support, and improved customer experience, (4) high mobile adaptation ratio, (5) product service improvement and innovation, (6) supply chain and logistics, (7) new consumer demands, (8) diverse and expanded Internet connectivity, and (9) asset tracking, utilization, and inventory management.

However, despite business growth, problems relevant to implementation and security may also arise. Therefore, it is crucial to identify how we can deploy the IoT architecture to connected devices and services. Lack of standardization is also a major factor that can hinder business growth.

6.3 Presenting the architecture

The architecture is presented in Section 5.

6.4 Identifying architectural approaches

PF-IoT-SRA is a layered, scalable, secure, and flexible architecture that has no restrictions in terms of numbers and types of layers. It consists of nine horizontal and two vertical layers, along with a layer with nonfunctional requirements. We have followed the ITU-T Y.2066 and ISO/IEC 30141 standards for the proposed IoT reference architecture. The other standards are ITU-T Y.2060 and NIST, but these focus on the device and physical object communication. They do not completely address the end-to-end IoT systems reference architecture model. ISO/IEC 30141 elaborates more on the system architecture of IoT in terms of the conceptual, system, domain, network, functional, and cross-sectional service views of the ecosystem. It is a modular and scalable architecture that provides an understanding of the key aspects of an IoT architecture. Two vertical layers integrate the security and privacy concerns of end users. The metrics embedded are incorporated through the requirements defined in standards.

6.5 Quality attribute utility tree

The utility tree identifies the quality attributes needed to achieve the most important quality goals in the architecture and validates the architecture based on the requirements. This follows the top-down approach. The quality factors that determine system utility are performance, usability, reliability, installing ability, functionality, security, portability, and privacy. In the next level, there are refinements of the quality attributes, specified down to the scenarios, which are also called the leaves of the trees. The architecturally significant requirement (ASR), provided by business drivers for the quality attributes, has been mapped in the quality attribute tree.

Scenarios are generated through brainstorming events in real-time scenarios. Day-to-day usage of IoT applications and utilization of the proposed reference architecture metrics can generate the scenarios for validation. We have then validated, through mapping, whether the proposed architecture's significant metrics meet the defined quality attributes and their refinements. The utility tree along with the scenarios is shown in Fig. 5 in accordance with the quality attributes.

6.6 Brainstormed and prioritized scenarios

Based on the scenarios generated in the utility tree, a larger set of scenarios is elicited from stakeholders. These real-time scenarios are prioritized by stakeholders, using the ASR collected previously. The characterization and prioritization of the quality attribute indicate the success of the system, and difficulty in achieving it can be the architect's assessment. This will be prioritized as high, medium, and low. The scenarios and their priorities are described in Table 5.

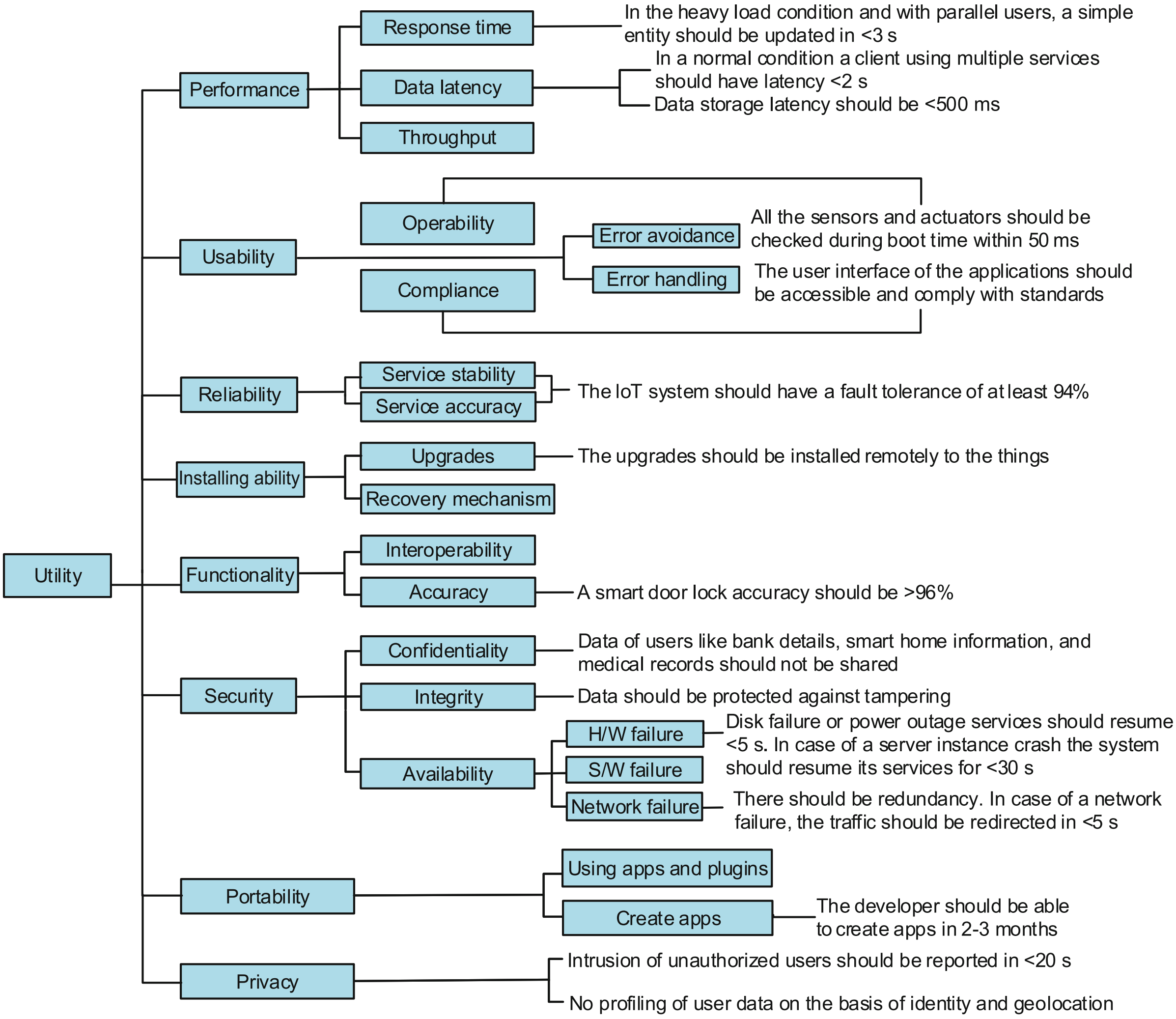
Utility
Performance
Response time
In the heavy load condition and with parallel users, a simple entity should be updated in <3 s
Data latency
In a normal condition a client using multiple services should have latency <2 s
Data storage latency should be <500 ms
Throughput
Usability
Operability
Compliance
Error avoidance
All the sensors and actuators should be checked during boot time within 50 ms
Error handling
The user interface of the applications should be accessible and comply with standards
Reliability
Service stability
Service accuracy
The IoT system should have a fault tolerance of at least 94%
Installing ability
Upgrades
The upgrades should be installed remotely to the things
Recovery mechanism
Functionality
Interoperability
Accuracy
A smart door lock accuracy should be >96%
Security
Confidentiality
Data of users like bank details, smart home information, and medical records should not be shared
Integrity
Data should be protected against tampering
Availability
H/W failure
S/W failure
Network failure
Disk failure or power outage services should resume <5 s. In case of a server instance crash the system should resume its services for <30 s
There should be redundancy. In case of a network failure, the traffic should be redirected in <5 s
Portability
Using apps and plugins
Create apps
The developer should be able to create apps in 2-3 months
Privacy
Intrusion of unauthorized users should be reported in <20 s
No profiling of user data on the basis of identity and geolocation

Fig. 5 Quality attribute utility tree

6.7 Analyzing architectural approaches

We map the brainstormed scenarios in the quality attribute tree to see whether the architecture responds to the stimulus of the scenario. End user input sends a stimulus about the failure of a particular system. The environment is the mode or state of the system while receiving a stimulus. It could be starting up the system, shutting down the system, recovering from a failure, or normal operations. This will identify the risks, sensitivity points, and trade-offs. The architecture's decisions are specified. Through mapping, we evaluate our proposed reference architecture regarding whether it responds against a particular stimulus in the prioritized scenarios. We also evaluate the architecture against quality goals.

Table 6 evaluates scenario 1. The success of the system is high, and the difficulty in achieving it is medium. To validate the architecture in terms of decision-making capability in a particular scenario, we generate a stimulus in normal operating conditions to evaluate the response and architecture decision. In this scenario, we evaluate the functionality of our proposed architecture and the trade-off that can be made.

Table 7 evaluates scenario 2. The success of the system is high, and the difficulty in achieving it is medium. The quality attribute evaluated is reliability under normal operating conditions. We generate a stimulus about the failure of the system to check what will be the decision of our proposed architecture to handle the failed state of the system.

Table 8 evaluates scenario 3. The success of the system is medium, and the difficulty in achieving it is medium. A scenario is generated to evaluate the usability attribute while starting up the system. We check the architecture's decision in a particular stimulus, i.e., failure of the system.

Table 9 evaluates scenario 4. The success of the system is high, and the difficulty in achieving it is high. The system is recovering from a failure, and the quality attributes addressed are security and availability. The scenario addresses whether the system has the response to the state of the system and which particular metric addresses the response to the stimulus.

Table 10 evaluates scenario 5. The success of the system is medium, and the difficulty in achieving it is low. The quality attribute evaluated in this scenario is the performance of the system in extreme working conditions. The risk attached to this scenario is that

Table 5 Brainstormed scenarios and their priorities

Scenario	Description	Priority
1	A smart home where all the appliances are connected to the Internet. A user requests to unlock the door through a mobile application rather than just normal keys (functionality: a smart door lock; accuracy should be >96%)	(H, M)
2	A connected self-driven car can optimize its operation and maintenance driving on the road without a driver (reliability: IoT system should have a fault tolerance of no less than 94%)	(H, M)
3	Industrial IoT, also known as Industry 4.0, the revolution of industry; production units highly rely on sensors, actuators, and controllers; temperature, voltage, frequency, seismic sensors not giving correct readings to PLCs; giving false negatives (usability: all the sensors and actuators should be checked during boot time within 50 ms)	(M, M)
4	In smart health care, patients use a connected battery-powered pacemaker to control abnormal heart rhythms (security: hardware disk failure or power outage; the services should resume <5 s)	(H, H)
5	In smart retail, a large number of users request for transaction checkout at the same time using mobile POS (performance: in heavy load conditions and with parallel users, a simple entity should be updated in <3 s)	(M, L)
6	IoT medical devices collect health care data, including blood pressure, sugar level, oxygen, and weight; the data of users are stored online (privacy: no profiling of user data based on identity and geolocation)	(M, H)
7	The developer should be able to create new applications in an IoT ecosystem (portability: the developer should be able to create applications in 2–3 months)	(M, L)
8	The patches should be installed on the software and operating systems of things (installing ability: the upgrades should be remotely installed to the things)	(H, M)

H, high; L, low; M, medium; PLC, programmable logic controller; POS, point of sale

Table 6 Scenario 1

Item	Description
Attribute	Functionality
Environment	Normal operations
Stimulus	The mobile application fails to unlock the door using communication protocols Z-Wave, Wi-Fi, and ZigBee
Response	Will not affect the overall system functionality and accuracy
Architecture decision	(Layer 3) Transport/communication layer: error control communication
Sensitivity	This layer should be able to control communication and errors from multiple IoT devices with the capability of intelligent networking
Trade-off	Performance, reliability
Risk	The interoperability in the functionality could result in security vulnerabilities, and the smart home could be compromised by unauthorized users

it can affect the goodwill of the consumers and halt the sales.

Table 11 evaluates scenario 6. The success of the system is medium, and the difficulty in achieving

Table 7 Scenario 2

Item	Description
Attribute	Reliability
Environment	Normal operations
Stimulus	A self-driven car has failed to sense a hurdle on the road component failure
Response	Will not affect the reliability of the self-driven car
Architecture decision	(Layer 5) Advanced analytics layer: machine learning and artificial intelligence
Sensitivity	IoT devices should be autonomous to detect any failure, change, and adjust themselves according to the environment
Trade-off	No trade-off
Risk	If there is less fault tolerance, the system cannot be termed reliable and can lead to a major hazard such as an accident in this scenario

Table 8 Scenario 3

Item	Description
Attribute	Usability
Environment	Starting up the system
Stimulus	Failure of boot time check of sensors and actuators within 50 ms
Response	Will not affect the overall system operations
Architecture decision	(Layer 1) Devices layer: things in IoT
Sensitivity	The devices such as sensors, actuators, and wearables should be able to check, protect, and configure themselves within the specified boot time
Trade-off	Portability, reliability, and functionality
Risk	Could result in false negatives; can halt the production units, resulting in financial loss

Table 9 Scenario 4

Item	Description
Attribute	Security, availability
Environment	Recovering from a failure
Stimulus	The hardware or battery of the pacemaker fails during the operation
Response	The recovery mechanism supported will not affect the security and availability of the system
Architecture decision	(Layer 6) Management layer: risk management
Sensitivity	There should be no common mode of failure; to ensure different types of hardware and operating systems
Trade-off	Installing ability, reliability
Risk	This could result in fatal hazards; the management layer might be helpful in risk minimization; might not address hardware redundancy

Table 10 Scenario 5

Item	Description
Attribute	Performance
Environment	Extreme operations
Stimulus	Due to the increased number of processing operations at the same time, the POS system gets hung
Response	Heavy load and parallel processing will not affect the response time of the smart retail system
Architecture decision	(Layer 5) Advanced analytics layer; (layer 6) management layer big data analysis, process management
Sensitivity	Virtual storage and processing using cloud computing should be secure and reliable
Trade-off	Portability, reliability, security, and privacy
Risk	Could damage the goodwill of the consumer experience and halt sales

POS, point of sale

it is high. The quality attribute evaluated in this scenario is privacy under normal operating conditions. The architecture proposed should mitigate the risk associated with the specific scenario.

Table 12 evaluates scenario 7. The success of the system is medium, and the difficulty in achieving it is low. This scenario evaluates the portability quality attribute from the utility tree. The response of the system identifies the architecture decision.

Table 13 evaluates scenario 8. The success of the system is high, and the difficulty in achieving it is medium. The installing ability attribute is evaluated in terms of whether it is achieved or not and which layer or particular metric responds to the system.

6.8 Presenting the results

ATAM gives us the trade-offs, sensitivity points, and risks associated with the proposed IoT reference architecture. It gives us a clear sight of how the reference architecture should perform under the brainstormed real-time scenarios. We generate the stimulus in brainstormed scenarios of the failures of the system, evaluate and map it with our proposed architecture. It has been derived that the architecture addresses and responds to a particular stimulus in the given environment. The trade-offs provide insight into which quality attribute could be given up to gain the other. The achievement of the quality goals and attributes refines, evaluates, and validates the proposed reference architecture.

7 Conclusions and future work

IoT has made our world smarter through communication between objects and humans. In the form of its applications such as smart devices and technologies, it has found its path in our daily lives. However, there are different standardization bodies for IoT, which have not embedded privacy metrics, and IoT still lacks a standard architecture. In this study, we have identified the core requirements from the standards and thereafter federated privacy and security to the reference architecture of IoT. Based on these requirements and metrics, we have analyzed 12 existing reference architectures. We have identified their shortcomings and proposed PF-IoT-SRA, which will help make a concrete and standard architecture. PF-IoT-SRA will counter major threats and attacks in IoT communication and address all

Table 11 Scenario 6

Item	Description
Attribute	Privacy
Environment	Normal operations
Stimulus	Medical records of the patients get profiled based on unique identifiers
Response	Will not disclose or profile the data based on identities in the database
Architecture decision	(Vertical layer 1) Privacy layer: identity privacy, geolocation privacy, privacy audit
Sensitivity	Health care IoT devices should have a privacy validation chain and a defined purpose of collection and profiling of data
Trade-off	Security, reliability
Risk	Unauthorized data collection and profiling of health care records could lead to exposure

Table 12 Scenario 7

Item	Description
Attribute	Portability
Environment	Normal operations
Stimulus	A new application or version of an operating system fails to configure with things, sensors, actuators, and devices
Response	Will not affect the software's ability to get transferred from one piece of hardware to another
Architecture decision	(Layer 4) Data transformation layer; (layer 8) application layer: data assessment, data expansion, API
Sensitivity	The things in IoT should be open source and be able to create and modify applications in case of any incompatibility or failure
Trade-off	Functionality, usability, and security
Risk	The new applications could lead to major security vulnerabilities which could result in exposure

API, application programming interface

Table 13 Scenario 8

Item	Description
Attribute	Installing ability
Environment	Normal operations
Stimulus	It fails to connect a mobile device to the target controller to install updates
Response	Will not affect the communication network of low-power resource-constrained IoT devices
Architecture decision	(Layer 2) Network layer mobile communication network, LPWAN
Sensitivity	Things should be autonomous to carry on, and managing legacy components will become difficult
Trade-off	Security, usability
Risk	This could result in bugs and viruses and loss of data while upgrading the things' firmware or OS; potential downtime while upgrading

LPWAN, low-power wide area network; OS, operating system

the concerns for the domain system and functional point of view. We have validated our proposed reference architecture through an industry-recognized scenario-based technique known as ATAM, which will support the proposed reference architecture from a business perspective.

The IoT ecosystem can face security and privacy challenges. For future work, we recommend studying each layer in detail to identify which protocol mix is the best to optimize the IoT network. We recommend proposing PETs to be embedded within smart IoT devices, incorporating all the metrics in the privacy layer. Considering the resource-constrained environment of IoT, lightweight protocols should be introduced, and the IoT network should be optimized in federation to privacy and security. Complex encryption and authentication algorithms consisting of less latency and fewer computing resources on tiny IoT devices could be a great breakthrough in the future. We recommend coming up with a lightweight trust management system to address hardware insecurities of IoT devices.

Contributors

Musab KAMAL and Imran RASHID initiated the idea. Musab KAMAL, Imran RASHID, and Waseem IQBAL drafted the paper. Muhammad Haroon SIDDIQUI, Sohaib KHAN, and Ijaz AHMAD revised and finalized the paper.

Compliance with ethics guidelines

Musab KAMAL, Imran RASHID, Waseem IQBAL, Muhammad Haroon SIDDIQUI, Sohaib KHAN, and Ijaz AHMAD declare that they have no conflict of interest.

References

Alaba FA, Othman M, Hashem IAT, et al., 2017. Internet of Things security: a survey. *J Netw Comput Appl*, 88:10-28. https://doi.org/10.1016/j.jnca.2017.04.002

Al-Fuqaha A, Guizani M, Mohammadi M, et al., 2015. Internet of Things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutor*, 17(4):2347-2376. https://doi.org/10.1109/COMST.2015.2444095

Al-Qaseemi SA, Almulhim HA, Almulhim MF, et al., 2016. IoT architecture challenges and issues: lack of standardization. Future Technologies Conf, p.731-738. https://doi.org/10.1109/FTC.2016.7821686

Alshohoumi F, Sarrab M, AlHamadani A, et al., 2019. Systematic review of existing IoT architectures security and privacy issues and concerns. *Int J Adv Comput Sci Appl*, 10(7):232-251. https://doi.org/10.14569/IJACSA.2019.0100733

Bassi A, Bauer M, Fiedler M, et al., 2013. Enabling Things to Talk. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40403-0

Cisco, 2014. Internet of Things Reference Model. https://www.cisco.com [Accessed on Aug. 10, 2021].

Chen KJ, Zhang S, Li ZK, et al., 2018. Internet-of-Things security and vulnerabilities: taxonomy, challenges, and practice. *J Hardw Syst Secur*, 2(2):97-110. https://doi.org/10.1007/s41635-017-0029-7

Chen LM, Nugent CD, Wang H, 2012. A knowledge-driven approach to activity recognition in smart homes. *IEEE Trans Knowl Data Eng*, 24(6):961-974. https://doi.org/10.1109/TKDE.2011.51

Chen SZ, Xu H, Liu DK, et al., 2014. A vision of IoT: applications, challenges, and opportunities with China perspective. *IEEE Int Things J*, 1(4):349-359. https://doi.org/10.1109/JIOT.2014.2337336

Dhelim S, Ning HS, Farha F, et al., 2021. IoT-enabled social relationships meet artificial social intelligence. *IEEE Int Things J*, 8(24):17817-17828. https://doi.org/10.1109/JIOT.2021.3081556

Domanska J, Gelenbe E, Czachorski T, et al., 2018. Research and innovation action for the security of the Internet of Things: the SerIoT project. 1st Int ISCIS Security Workshop, p.101-118. https://doi.org/10.1007/978-3-319-95189-8_10

dos Santos MG, Ameyed D, Petrillo F, et al., 2020. Internet of Things architectures: a comparative study. https://arxiv.org/abs/2004.12936

Fallmann S, Chen LM, 2019. Computational sleep behavior analysis: a survey. *IEEE Access*, 7:142421-142440. https://doi.org/10.1109/ACCESS.2019.2944801

Farha F, Ning HS, Ali K, et al., 2021. SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE Int Things J*, 8(7):5904-5913. https://doi.org/10.1109/JIOT.2020.3032518

Fremantle P, 2015. A Reference Architecture for the Internet of Things. WSO2 White Paper 02-04.

Frustaci M, Pace P, Aloi G, et al., 2018. Evaluating critical security issues of the IoT world: present and future challenges. *IEEE Int Things J*, 5(4):2483-2495. https://doi.org/10.1109/JIOT.2017.2767291

Gerber A, Kansal S, 2017. Simplify the Development of Your IoT Solutions with IoT Architectures. https://www.ibm.com/developerworks/library/iot-lp201-iot-architectures/index.html [Accessed on Mar. 22, 2021].

Hu PF, Ning HS, Chen LM, et al., 2019. An open Internet of Things system architecture based on software-defined device. *IEEE Int Things J*, 6(2):2583-2592. https://doi.org/10.1109/JIOT.2018.2872028

Iqbal W, Abbas H, Daneshmand M, et al., 2020. An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Int Things J*, 7(10):10250-10276. https://doi.org/10.1109/JIOT.2020.2997651

ISO/IEC, 2014. Study Report on IoT Reference Architectures/Frameworks. Kate Grant AHG, SWG5, JTC1.

Javed B, Iqbal MW, Abbas H, 2017. Internet of Things (IoT) design considerations for developers and manufacturers. IEEE Int Conf on Communications Workshops, p.834-839. https://doi.org/10.1109/ICCW.2017.7962762

Karale A, 2021. The challenges of IoT addressing security, ethics, privacy, and laws. *Int Things*, 15:100420. https://doi.org/10.1016/j.iot.2021.100420

Kraijak S, Tuwanut P, 2015. A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. 11th Int Conf on Wireless Communications, Networking and Mobile Computing, p.1-6. https://doi.org/10.1049/cp.2015.0714

Li C, Palanisamy B, 2019. Privacy in Internet of Things: from principles to technologies. *IEEE Int Things J*, 6(1):488-505. https://doi.org/10.1109/JIOT.2018.2864168

McKinney D, 2015. Intel IoT Platform Architecture Specification White Paper.

Microsoft, 2018. Microsoft Azure IoT Reference Architecture V 2.1 26/09/2018. https://download.microsoft.com/Microsoft_Azure_IoT_Reference_Architecture [Accessed on June 10, 2021].

Mongo, 2019. IoT Reference Architecture. https://www.mongodb.com/collateral/iot-reference-architecture [Accessed on June 10, 2021].

O'Donnell L, 2019. Researchers Allege 'Systemic' Privacy, Security Flaws in Popular IoT Devices. https://threatpost.com/researchers-allegesystemic-privacy-security-flaws-in-popular-iotdevices/141244 [Accessed on Mar. 17, 2021].

Okeyo G, Chen LM, Wang H, et al., 2011. Ontology-based learning framework for activity assistance in an adaptive smart home. In: Chen LM, Nugent CD, Biswas J, et al. (Eds.), Activity Recognition in Pervasive Intelligent Environments. Atlantis Press, Paris, France, p.237-263. https://doi.org/10.2991/978-94-91216-05-3_11

Pan QQ, Wu J, Bashir AK, et al., 2022. Joint protection of energy security and information privacy for energy harvesting: an incentive federated learning approach. *IEEE Trans Ind Inform*, 18(5):3473-3483. https://doi.org/10.1109/TII.2021.3105492

Pierleoni P, Concetti R, Belli A, et al., 2019. Amazon, Google and Microsoft solutions for IoT: architectures and a performance comparison. *IEEE Access*, 8:5455-5470. https://doi.org/10.1109/ACCESS.2019.2961511

Psychoula I, Singh D, Chen LM, et al., 2018a. Users' privacy concerns in IoT based applications. IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), p.1887-1894. https://doi.org/10.1109/SmartWorld.2018.00317

Psychoula I, Merdivan E, Singh D, et al., 2018b. A deep learning approach for privacy preservation in assisted living. IEEE Int Conf on Pervasive Computing and Communications Workshops, p.710-715. https://doi.org/10.1109/PERCOMW.2018.8480247

Psychoula I, Chen LM, Yao XX, et al., 2019. A privacy aware architecture for IoT enabled systems. IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), p.178-183. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00073

Psychoula I, Chen LM, Amft O, 2020. Privacy risk awareness in wearables and the Internet of Things. *IEEE Perv Comput*, 19(3):60-66. https://doi.org/10.1109/MPRV.2020.2997616

Solapure SS, Kenchannavar H, 2016. Internet of Things: a survey related to various recent architectures and platforms available. Int Conf on Advances in Computing, Communications and Informatics, p.2296-2301. https://doi.org/10.1109/ICACCI.2016.7732395

Torkaman A, Seyyedi MA, 2016. Analyzing IoT reference architecture models. *Int J Comput Sci Softw Eng*, 5(8):154.

Yao XX, Farha F, Li RY, et al., 2021. Security and privacy issues of physical objects in the IoT: challenges and opportunities. *Dig Commun Netw*, 7(3):373-384. https://doi.org/10.1016/j.dcan.2020.09.001

Zhou W, Jia Y, Peng AN, et al., 2019. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. *IEEE Int Things J*, 6(2):1606-1616. https://doi.org/10.1109/JIOT.2018.2847733

List of supplementary materials