# Systematic Literature Review on IoT Architectures and Smart Home

Aljuhara Alsadoun | Layan Aljabali | Sara Almashharawi | Shamaa Ben Elewa

## ABSTRACT:

Internet of things (IoT) enables the devices to communicate and exchange data through the network by connecting and controlling the devices. There are many applications for the IoT in different domains, to satisfy the aim of the IoT and provide an architecture design. Therefore, the architectural design process helps to establish a framework for the development of a computer system. Unfortunately, there are no specific comprehensive studies on IoT architectures and smart homes that effectively and systematically analyze them. We conducted this systematic literature review by searching IEEE, Wiley, Springer, and Hindawi online libraries between 2016 and 2022. We were able to find forty-seven studies based on inclusion and exclusion criteria. Only twenty out of forty-seven proposed and discuss the state of IoT architecture and IoT-based smart homes. However, we discuss the architecture for smart home privacy in different layers, including architectural patterns, models, tools, and platforms supporting IoT. We have found security domain is the most popular domain in the IoT architecture. There are other domains that we can classify the architectures upon them e.g., privacy, interoperability, scalability, load monitoring, energy consumption, and big data management.

*Research keywords:* Internet of Things (IoT), Smart Home, Systematic Literature Review (SLR), IoT architectures.

## I. INTRODUCTION:

Internet of Things (IoT) is an integration of the sensor, embedded, computing, and communication technologies. It is concerned as a network system in both wired and wireless connection that consists of many software and hardware entities [1].

The purpose of IoT is to create a system that connects and controls IoT devices, which can exchange data and communicate together through the network so that provides seamless services to anything, anytime at any place. We have many applications for the Internet of Things, such as Health, education, industry, and agriculture. As a reason for varying IoT applications, it is a must to provide an architecture that satisfied the aim of the IoT.

Architectural design is the process of defining a set of hardware and software components and their interfaces to establish the framework for the development of a computer system [2]. IoT architecture differs from each other depending on the goal that you want to achieve, whether you want to get high security, consume less electricity or manage big data, etc. After studying the architectures of IoT, it was found that each architecture has a combination of layers and technology to support the goal. However, one of the important applications of the IoT is the smart home. Smart home automation systems are integral in ensuring a high quality of life by monitoring and controlling the home environment. It helps control data storage and processing with cloud technology [3]. A typical smart home today contains a variety of consumer devices. Some consumer devices may also be connected to a smart home management system using a home area network. Many smart home devices interact with a consumer's mobile phone and use internet gateways to communicate with remotely hosted services offered by various commercials [4]. So, smart home architecture is an important concept of IoT. Since integrated architecture with different technologies would provide the main characteristics of the smart home environment.

In this work based on a systematic literature review (SLR), we review the previous research which points to the IoT architecture and smart homes. Which were published from 2016 to 2022. With the guide of an evidence-based method utilized, (number of our studies) studies were initially collected. Through the formulated inclusion and exclusion criteria, we selected twenty studies that are related to our defined research questions. The contributions of the study are stated as follows:

- To classify Internet of things architectures.
- To be aware of differences in layers and tools in each architecture.
- To see which architecture is suitable for IoT-based smart home.
- To be aware of the absence in the domain of IoT-based smart homes studies

The remainder of the paper is organized as follows: Section II the related work. Section III presents the search method. Section IV presents the result of the analysis and the discussion. While Section V concludes the paper.

## II. RELATED WORK:

This section presents the previous work on internet of thing architecture and smart home and there were a very few researchers have reviewed it, and this section discussed review and survey papers.

AlLifah *et al* [4] reviewed a Survey on Ranking Security of IoT-based Smart Home Consumer Devices. Additionally, they focused on security risks and security vulnerabilities to the consumer from the devices are exposed to mobile applications and cloud-based services, and they discussed AHP model for ranking commonly used home consumer devices.

Maswadi *et al [*5] provide an overview Systematic Literature Review of smart home for the Elderly using the monitoring Technologies in IoT. Then, they reviewed health monitoring technologies in smart home and different existing technologies utilizes. In addition, they provided the methodology used to undertake the current SLR of smart home technology implementation for the elderly.

Sarhan *et al [*6] presented a Survey on safety and security systems in smart home by using the Arduino platform. The survey reviewed research results that examined smart home safety and security systems using the Arduino platform. Then, He provided and described numbers of different system architectures in the design and implementation of smart home safety and security systems using Arduino.

Washizaki *et al* [7] presented an SLR on "Architecture and Design Patterns for IoT Systems ". This paper says that IoT architecture is in its early stage, due to the number of conferences accedes the number of journals. Also, it classifies architecture and design patterns based on abstraction level, domain specificity, and quality attributes. Also, they found 61 IoT architecture and design patterns.

This research focused on the architecture of IoT and smart home. Therefore, selecting a systematic literature review technique is appropriate because it relies on excellent quality scientific articles. However, on the internet of thing architecture and smart home there is no systematic literature review to the best of our knowledge; thus, this paper closes the gap.

## III. RESEARCH METHOD:

To organize the work, we have followed an iterative step that is as follows:

- Plan for the work.
- The formulation of key research questions and search keywords.
- The formulation of the search processes.
- Include / exclude the primary study.
- Extract the main idea from each study.
- Classify the studies.

### A) *RESEARCH QUESTIONS*

This research investigates how studies of IoT represent different architecture and which architecture is suitable for smart homes. Therefore, we formulated research questions that describe the research and break it down into smaller questions to be accurate. Our main research question is "What is the state of the art in the field of study of IoT architecture and IoT-based smart home ". The following questions are to achieve the objective of this study:

RQ1) What are the contributions of the primary studies that are related to IoT architecture?

RQ2) How do primary studies describe the architectural layers in IoT systems?

RQ3) What kind of models, tools, or platforms are supported IoT is mentioned in primary studies?

RQ4) What is the most suitable architecture for smart home?

## B) *SEARCH PROCESS*

In this study, each article was extracted from an electronic database using the conventional manual search process. We selected three data sources to extract essential information for the literature. These data sources are IEEE Xplore (https://ieeexplore-ieee-org), Wiley Online library (https://onlinelibrary-wiley-com), Springer (https://link.springer.com/) And Hindawi (www.hindawi.com ). The query to extract related information was filtering by the title or abstract. To search these electronic databases, we used advanced search and formulated the following search string: IoT OR Internet of Things AND Smart Homes, also IoT OR Internet of Things AND Architecture.

## C) *STUDY SELECTION*

Each study appearing in this SLR has been applied to inclusion / exclusion criteria that filter the forty-seven of studies to get twenty and helps us to find related information. TABLE 1 shows the data sources and number of primary studies after applying inclusion / exclusion criteria.

*The inclusion criteria:*

ICR1) Years between 2016 and 2022.

ICR2) The search study is written in English.

ICR3) The study that published in journal OR conference.

ICR4) The study that focuses on IoT architectures.

ICR5) The study that focuses on IoT-based smart homes.

ICR6) SLR that has a high rate and Signature.

*The exclusion criteria:*

ECR1) Years that are not in between 2016 and 2022.

ECR2) Any content other than English.

ECR3) The study that published in other than journal OR conference.

ECR4) The study does not relate to IoT architecture.

ECR5) The study does not relate to IoT-based smart home.

ECR6) The search study is not a scientific publication.

ECR7) The search study is not available in full text.

| Electronic Database | Number of Primary Studies |
|---|---|
| IEEE Xplore | 15 |
| Wiley Online Library | 3 |
| Springer | 1 |
| Hindawi | 1 |

TABLE 1. data sources and its related primary study after applying e inclusion / exclusion criteria.

## IV. RESULTS & DISSCUSSION:

In this section, we discuss the results of each research question in detail.

### *A. RQ1: What are the contributions of the primary studies that are related to IoT architecture?*

This section classifies the primary studies based on their contribution. When we analyzed the papers, we noticed all the contributions were based on non-functional capabilities such as security, privacy, availability, scalability, performance, and interoperability. On the other hand, there were contributions that support energy consumption, big data management, and appliance load monitoring. According to many literatures, we found these results:

There are studies focusing on software architectural patterns that are suitable for IoT:

According to Jacob *et al [*2] analyzed software architectural patterns based on non-functional capabilities. They suggested centralized cloud model -a form of client-server architecture- for scalability and availability. This model considered the cloud as a central server and devices used in IoT as client. However, this model does not support the performance. That can be solved by using a centralized hierarchical model. Also, suggested peer-to-peer architecture for scalability, availability, and performance as each system in IoT is considered as a server and client based on demand. For privacy and security, Jacob *et al* suggested Publisher–subscriber architecture. Here the consumer is interested only in receiving the data of their interest. Finally, Representational state transfer (REST) architecture is suggested for interoperability because of all systems share a uniform interface.

Gavrilović *et al* [8] suggested different architectures for different systems. These architectures are based on REST API to ensure interoperability between IoT devices. Gavrilović *et al* proposed software architecture based on cloud computing. By integrating on a cloud-based platform, IoT devices and uses middleware layer to hide implementation details and provide support for cloud application solution.

Whereas there are studies focusing on layered architecture and system architecture to achieve the privacy:

To achieve differential privacy, Zhang *et al* [9] proposed an architecture for smart home based on fog computing which is APDP model. APDP is guaranteed by differential privacy with Laplace noise. This model defeats the collusion attack under of multiple parties due to the properly decoupled noise generated by the modified Laplace mechanism.

Qashlan *et al* [10] proposed system architecture to provide privacy mechanism using blockchain. It consists of end users (home users, services accessors), IoT smart home devices, edge servers, and the cloud servers. All of them have unique Ethereum Address with public and private keys.

Furthermore, there are studies focusing on layered architecture and system architecture to achieve security:

Erfani *et al* [1] proposed IoT security management (IoTSMS). Here, the system is composed of three components, IoT layered architecture, layered of IoTSMS, and the IoT security management information base (IoTSMIB). That provides each layer of the IoT system with the needed security services.

On the other hand, Gupta *et al* [11] discussed the security architecture of IoT in detail which consists of three layers, these layers have been divided into sub-layers. Also, proposed protocols for each layer to achieve maximum security.

Likewise, Rahman *et al* [12] proposed a disseminated block building (DistBlockBuilding) architecture that enabled Blockchain-based SDN-IoT gateway. SDN is a gateway that filters IoT devices data and then produces the forwarding patterns using SDN-IoT gateway, and each pattern is grounded on the relating network communications protocol. Blockchain is P2P architecture technology that ignores the third-party interferer in smart communication and transaction system.

Additionally, Wang *et al* [13] proposed layered architecture of the IoT-Cloud system which was designed based on centralized hierarchical cloud model. This study focuses on edge computing to provide security mechanism for IoT. Here, edge computing is divided into two layers (edge network and edge platform). The edge network is spread over the IoT to ensure security.

Whereas there is a study focuses on layered architecture and the suitable software architecture to achieve the big data management:

Mokhtari *et al [*14] proposed layered architecture consisting of seven layers that support big data management. This layered architecture based on REST software architecture can be used to provide shared data-driven processing and decision-making.

Also, there are studies focusing on layered architecture and the suitable software architecture to reduce energy consumption in IoT:

Andrade *et al* [15] proposed an innovative HEMS model based on IoT services of interoperability by defining a middleware procedure based on REST API and Publisher–subscriber architecture. The architecture also allows the control of energy consumption using middleware layer services.

On the other hand, Tsai *et al* [16] proposed a schema to reduce energy consumption that uses smart socket and IoT which is residence energy control system (RECoS). Energy consumption is collected through smart socket in IoT appliances, not from the sensors. So, this architecture's sensor layer is the smart sockets.

In contrast, Paredes-Valverde *et al* [17] shows power saving mechanism using IoT and big data technology. It collects the data from IoT devices and sensors and then analyzes it in big data technology. So, they proposed IntelliHome system that lies on IoT layered architecture. This model adds home energy consumption monitor layer that allows users to monitor and reduce energy consumption in the home.

In addition, there is a study focuses on layered architecture that is supported by machine learning algorithm to achieve successful appliance load monitoring:

Franco *et al* [18] proposed hardware-based methods, including intrusive load monitoring (ILM) for load monitoring by defining the appliance using machine learning (ML) algorithm. So, it develops appliance parts in the architecture and suggests IoT architecture layers than can be used to implement appliance load monitoring.

Finally, we contrast each literature's contribution and show which contribution was focused on in this study in TABLE.2. We agree that security is a major concept in IoT environment, there were 38% of the literature that we found proposed architecture to ensure high security. After that comes the interoperability which is discussed in 30% of the studies. Then, privacy and energy consumption have an equal number of studies discussed in 23% of studies. Whereas scalability is discussed in 15% of the studies. However, we notice an absence in the domain of the performance, availability, big data management, and appliance load monitoring since there is only one study for each discussed these concepts which take 7% of the studies. furthermore, the architecture could be layered architecture, software architecture, or system architecture. These architectures could be composed of each other to achieve maximal utility for IoT.

| Contribution | Primary Study |
|---|---|
| Availability | [2] |
| Scalability | [2], [13] |
| Performance | [2] |
| Security | [2], [1], [11], [12], [13] |
| Privacy | [2],[9], [10] |
| Interoperability | [2], [15], [14], [8] |
| Energy consumption | [15], [16], [17] |
| Big data management | [14] |
| Appliance load monitoring | [18] |

TABLE.2 shows each literature with its corresponding contribution.

### *B. RQ2: How do primary studies describe the architectural Layers in IoT systems?*

In this paper, we will discuss the most IoT architectures that help in smart homes, and how these architectures are divided. To answer this question, we will deduce the main IoT Architectures Layers, and we will discuss every paper in which there is a change in these layers, either by adding a layer or subtracting a layer.

After we read and discussed many papers, my colleagues and I agreed to divide the main architecture layers in IoT based on the importance of these layers and their presence in most papers, into three layers which most of them agreed on.

Which are: 1- Application Layer, 2- Network Layer, 3- Cloud Layer. Each of these layers has key features that we showed in TABLE.3.

| Layer | key features |
|---|---|
| Application Layer | Front for all applications that user used. |
| Network Layer | The communication between the devices. |
| Cloud Layer | intermediary for remote managements request. |

TABLE.3 shows layers and their key feature.

There is a paper focused on the architecture of smart home based on fog computing [9]. Which includes four Layers: 1- IoT Layer, 2- Fog Layer, 3- Public Cloud Layer, 4- Application Layer. So, they agreed with the Application Layer and Cloud Layer, and they added two more layers. IoT Layer includes smart devices at home, and Fog Layer for fog servers.

Another paper focused on security architecture [1]. This paper proposed IoTSMS that consist of three components: the IT reference model, the layered functional architecture of IoTSMS, and the IoTSMIB. the IoT reference model consists of element layers: 1- Network layer, 2- Service layer, 3- Application layer. Each layer in the reference model is integrated to the functional layers of IoTSMS they are IT security business policy management, IoT security service management IT security mechanism management, and IT fundamental security function. Whereas IoTSMIB corresponds to IoTSMS. IoTSMIB database will provide protection of the data from the bottom layer to the top layer of the IT reference model. By Our division of layers, which we agreed upon, they agreed with the Application Layer and Network Layer, but they have added one more layer which is Service Layer. Where the Service Layer responsible for service support function and data storage, and acts as home gateway between the Network layer and Application layer. FIGURE.1 is the system architecture that represents in the study [1].

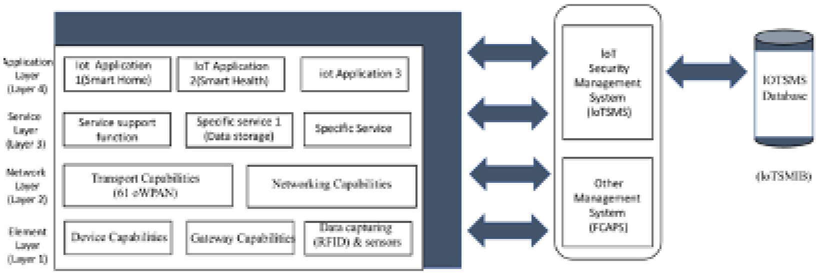
Application Layer (Layer 4)
Iot Application 1(Smart Home)
IoT Application 2(Smart Health)
iot Application 3
Service Layer (Layer 3)
Service support function
Specific service 1 (Data storage)
Specific Service
Network Layer (Layer 2)
Transport Capabilities (61 oWPAN)
Networking Capabilities
Element Layer (Layer 1)
Device Capabilities
Gateway Capabilities
Data capturing (RFID) & sensors
IoT Security Management System (IoTSMS)
Other Management System (FCAPS)
IOTSMS Database
(IoTSMIB)

FIGURE.1 The integration of IoT and IoTSMS

Whereas paper [11], focused on security architecture. So, they divided IoT architecture into three layers: 1- Perception Layer, 2- Transmission Layer, 3- Application Layer. So, they agreed on Application Layer and disagreed with the rest. They have added two layers which are Perception Layer and Transmission Layer. Perception Layer responsible for sensing, identification, actuation, and communication technologies. Transmission Layer responsible for connectivity establishment and information transmission.

Also, paper [12], discussed the DistBlockBuildind Architecture which is Distributed Blockchain-based Software-Defined Networking-IoT for Smart Building Management. this paper divided the IoT Architecture into two Layers: 1-Data Layer, 2- Control Layer. They added two layers, Data Layer and Control Layer. Data Layer responsible for communication between networks, and the Control Layer responsible for data OpenFlow control.

Another paper focused on the service architecture of the IoT-Cloud system [13]. This paper divided the IoT Architecture into three Layers: 1- Data Collection Layer, 2- Data Processing Layer, 3- Application Layer. They only agreed on the Application Layer. Where the Data Collection Layer for the edge network lies, the edge platform is in the Data Processing Layer and in the Application Data Layer.

In this paper [14], focused on different architectures which is the proposed Representational State Transfer (REST)-based architecture, by the (REST)-based architecture. It divided IoT Architecture into seven layers: 1- Physical Layer, 2- Fog-Computing Layer, 3- Network Layer, 4- Cloud Computing Layer, 5- Service Layer, 6- Session Layer, 7- Application Layer. So, they agreed on all Layers, but they added four layers which are Physical Layer, Fog-Computing Layer, Service Layer, and Session Layer. The Physical Layer includes types of sensing technologies and devices. Fog-Computing Layer provides the capability solution for Cloud Computing Layer. The Service Layer includes operational data and analytical data views. Session Layer provides standards and APIs to exchange data between smart home service and application layers.

Furthermore, these two papers [15] and [3] created and focused on a new Home Energy Management System (HEMS) architecture, this architecture can be divided IoT Architecture into three layers: 1- Application Layer, 2- Middleware Layer, 3- Cloud Layer. So, they agreed with Application Layer and Cloud Layer, but they added one more layer which is Middleware Layer. Middleware Layer can be used to switch to renewable energy sources for energy regulation.

This paper [16], discussed different Energy Saving System which is Residence Energy Control System (RECoS) Architecture, this paper divided IoT Architecture into three Layers: 1- Sensor Layer, 2-Network Layer, 3- Application Layer. So, they agreed with Application Layer and Network Layer, but they added one more layer which is Sensor Layer. Based on the architecture or the (RECoS), Sensor Layer is smart socket.

Another paper talked about Energy Saving System architecture [17]. It divided IoT architecture into three layers:  1- Presentations Layer, 2- Data Management Layer, 3- Network Layer. So, they agreed with Network Layer, but they added two more layers which are Presentations Layer and Data Management Layer. Presentations Layer is responsible for ensuring the communication between user and system, and the Data Management Layer is responsible for the management of all data collected from other home area networks.

Also, there is a paper focused on IoT Architecture for Intrusive Load Monitoring (ILM) [18]. they divided the IoT Architecture into five Layers: 1- Physical Layer, 2- Perception Layer, 3- Network Layer, 4- Middleware Layer, 5- Application Layer. So, they agreed with Network Layer and Application Layer, but they added three more layers. Where the Physical Layer responsible for collecting data flow and sending it to the upper layer, Perception Layer responsible for data acquisition of many sensors and actuators are gathering information, and Middleware Layer mediates the interaction between IoT devices and software applications.

Another paper discussed different layers of IoT Architecture based on a map the Cloud-IoT Platform [19]. So, they divided the IoT Architecture into five Layers: 1- Perception Layer, 2- Network Layer, 3- Middleware Layer, 4- Application Layer, 5- Business Layer. So, they agreed with Network Layer and Application Layer, but they added three more layers. The Perception Layer includes sensors, Middleware Layer response for processes received date and delivery the required service to Application Layer, and the Business Layer managing the overall IoT system actives and services.

In addition, another paper discussed the IoT protocol stack Architecture [20]. They divided the IoT Architecture into five mine Layers: 1- Perception Layer, 2- Transport Layer, 3- Service Layer, 4- Application Layer, 5- Business Layer. So, they agreed with only the Application Layer, and they added four more layers. Perception Layer serves as an intermediate between the environment and the digital world by using sensors, Transport Layer is aimed to connect in security way, Service Layer facilities the use of heterogeneous devices in IoT applications, and the Business Layer supervises the IoT system's operations and its various services.

### *C. RQ3: What kind of models, tools, or platforms are supported IoT is mentioned in primary studies?*

As we mentioned, there are many papers that talk about different models, platforms, and tools used to build and manage IoT systems.

Regarding to the model, we discussed papers used for communication in IoT. Also, there is a paper talks about model used in monitoring and activity recognition:

This paper [2], show us four communications model used by IoT devices: 1-Client–server architecture 2- Peer-to-peer is a variant of client–server architecture 3- Publisher–subscriber architecture 4-Representational state transfer (REST) architecture.

Also, this paper [20] discusses the model used for communication in IoT:

- Edge-to-Edge communication model (E2EC): In this model, devices communicate directly with other devices.
- Edge-to-Gateway communication model (E2GCM): In this model, the gateways are loaded with the application layer software and serves as an intermediate between the devices and application service providers.
- Edge-to-Cloud communication model (E2CC): In this communication standard, devices are directly connected to the cloud. Devices read and write data from and to the cloud, respectively. Applications like Smart Grids, FMS, Connected Labs, etc. use this communication model.
- Back-end data sharing model (BDS): This model allows trusted third parties to obtain the sensory data from the cloud for aggregation and analysis.

This primary study [18] discussed the Machine learning models help to monitor and Activity Recognition in Smart Homes models, such as FFNN, LSTM networks, and SVMs allow labeling of the data and contribute to the correct classifier generalization. Three different classifier models are tested using real data from the UK-DALE dataset: feed-forward neural network (FFNN), long short-term memory (LSTM), and support vector machine (SVM). They are listed in TABLE.4.

| FFNN | LSTM | SVM |
|---|---|---|
| is a machine learning model that involves passing input data through intermediate computations in order to arrive at its output? A layer's outputs are not fed back into itself, because there are no feedback connections. | A long short-term memory network is a type of recurrent neural network (RNN) model An architecture comprised of gated inputs, outputs, and feedback loops. Its main contribution is that it addresses the vanishing gradient problem, common in RNN models, | Based on the principle of structure risk minimum in statistical theory, support vector machines are an ML technique. Both classification and regression problems can be solved with it, and its main advantage is its principle of operation. An infinite-dimensional hyper-plane is constructed |

| | | |
|---|---|---|
| | by allowing gradient information to disappear or explode over time, and to propagate backward as well. | by creating a set Of hyperplanes |

TABLE.4 classifier Machine learning models.

Here, we discuss platforms that are used in IoT. There are platforms for storage and their types:

This paper [8], talk about how system platform are used for resource storage in IoT:

- NET platform (PaaS), Cloud computing, and storage resources are available on public and private clouds.
- The City Data and Analytics Platform (CiDAP) is a Big Data-based platform that stores a large amount of data, IoT middleware is used to process data sets It consists of IoT agents, IoT brokers, Big Data Repository, City Model server.
- ITU platform using an Internet-of-Things platform, data can be collected from IoT devices, transmitted to city infrastructure, analyzed, and transmitted to all applications on the surface of the city.

This paper [13] talks about edge platform. The edge platform consists of four primary functions:

- Creating virtual devices from physical ones.
- The template parameter is created in the edge platform, as well as the template parsing is created in the edge platform.
- Dynamic cloud load balancing by providing an on the edge platform.
- Cooperating with the edge network to ensure IoT reliability at the data level.

This paper [19] talks about comparing the three main Cloud Platforms (Amazon Web Services, Google Cloud Platform, and Microsoft Azure) and shows the result of the test of the platforms in keys that we consider performing the analysis. Cloud-IoT platforms provide middleware to connect and manage hardware devices and the data collected by them. The keys that we consider performing the analysis are device management, data communication protocols, rules, data storage, integration, security, and costs.

Also, we found a paper that mentioned the tools that are used in IoT:

This paper [11] mentioned open-source tools, but we will focus on the most suitable tools for the smart home from our point of view.

- IoT Development Tools: An open-source electronics platform based on easy-to-use hardware and software. Provides the technology needed to build IoT devices, gateways, and Cloud platforms. Example: Arduino 90

- Middleware: Open-Source middleware for getting information from sensor Clouds and offers utility-based IoT services. Integration middleware for IoT which provides a communication stack for embedded devices based on IPv6 and web services to establish interoperable interfaces for smart objects. Example: IoTSys 96
- Platform & Integration Tools: Tools for integrating multiple IoT-related sensor networks and protocols. Provides an M2M communication framework for connecting devices to applications in IoT environment and enables users to visualize data from the devices. Example: DeviceHive 101

We summarize the models, platforms, and tools in TABLE.5.

| Models: | Platforms: | Tools: |
|---|---|---|
| used in IoT to communication:<br>1-Client–server architecture 2- Peer-to-peer is a variant of client–server architecture 3- Publisher–subscriber architecture 4-Representational state transfer (REST) architecture<br>5-Edge to edge communication model (E2EC) 6-edge to getaway communication model (E2GCM)<br>7- edge to cloud communication model (E2CC) 8- back-end data sharing model (BDS) | platform used to resource storage in IoT:<br>1-NET platform (PaaS) 2-The City Data and Analytics Platform (CiDAP)<br>3- ITU platform4- edge platform | open-source tools:<br>1-IoT Development Tools<br>2- Middleware<br>3-The platform & integration tools |
| Model used in monitor and Activity Recognition:<br>feed-forward neural network (FFNN), long short-term memory (LSTM), and support vector machine (SVM). | Cloud Platforms: (Amazon Web Services, Google Cloud Platform, and Microsoft Azure) | |

TABLE.5 classification of models, tools, platforms we mentioned

After many papers were taken, it became clear to us what was coming: All the models mentioned are used based on the purpose of the IoT system.

We notice the most suitable model for communication in IoT smart home is a centralized hierarchical model-form of Client–server architecture -. it upgrades performance, scalability, and availability.  Also, this model of communication should be integrated with Edge-to-Edge communication model (E2EC) since it is a wireless communication standard.

Since there is a hierarchical model, so we suggest edge platform to be used as a resource storage in IoT.

Edge networks have the following advantages:

- They replace recommendations and indirect trust.
- By establishing the entire trust state of the IoT, we can dynamically balance the IoT load while selecting trusted devices to perform the service.
- Meeting specific user requirements like delays, integrity, and precision.

Also, we suggest using DeviceHive 101 tool because it provides M2M communication for connecting devices in the IoT environment and allowing users to view data from the devices.

### *D. RQ4: What is the most suitable architecture for smart home?*

According to many papers, this section provides the suitable software architecture and layered architecture for smart home.

Paper [1] was the only study done for smart homes focused on security. Also, papers [8], [14] and [15] are studies done on smart home's interoperability. The papers [9] and [10] were done for smart home's privacy. Also, the paper [17] is done for smart home energy consumption. Finally, paper [18] was done for smart home appliance load monitoring.

From all literature we have discussed, we see interoperability and privacy are the main characteristic of IoT architecture for the smart home. Interoperability is achieved by using REST API, whereas the privacy is achieved using cloud-based architecture. For explanation, most of the literatures were dividing the cloud layer into two separate layers (fog computing layer – same as edge server–, cloud computing layer). Fog computing layer can achieve the privacy for smart home residents because it acts as a local cloud. So, the processing and sensitive data storing is applied in this layer. We see the most suitable architecture for smart home is 1- IoT Layer, 2- Fog Layer, 3- Public Cloud Layer, 4- Application Layer. Also, IoT devices should communicate using REST API and support its technology.

## V. CONCLUSION:

In our Systematic literature review (SLR), we focused on the architecture for IoT and smart home. We did this SLR with many scientific papers. In this SLR, we classify the architectures based on their contribution. The contributions we have found are availability, scalability, performance, security, privacy, interoperability, energy consumption, big data management, and appliance load monitoring. However, most of the papers we found were talk about security. We notice an absence in the domain of availability, performance, big data management, and appliance load monitoring. Furthermore, we have found twelve different software, system, and layered architectures. The layered architectures share these layers Application Layer, Network Layer, and Cloud Layer. In addition, IoT has various models, platforms, and tools. Regarding to models, there are models used for communication, and other for monitoring and activity recognition. For platform, there are platforms used for resource storage. Also, we have found different tools for different purpose e.g., IoT Development Tools which is an open-source electronics platform based on easy-to-use hardware and software. Provides the technology needed to build IoT devices. Also, the Middleware tool is an open-source middleware for getting information from sensor clouds and offers utility-based IoT services. Integration middleware for IoT which provides a communication stack for embedded devices based on IPv6 and web services to establish interoperable interfaces for smart objects. Finally, Platform & Integration Tools are used for integrating multiple IoT-related sensor networks and protocols. Provides an M2M communication framework for connecting devices to applications in IoT environment and enables users to visualize data from the devices.

Also, the SLR proposes an architecture for IoT-based smart home which is IoT Layer, Fog Layer, Public Cloud Layer, and Application Layer. This combination of layers provides privacy since the cloud layer is divided into fog computing and cloud computing. Also, we see the REST API is the most suitable software architecture for smart home, since it provides interoperability for IoT devices.

Finally, we are looking to increase the studies in IoT architectures and smart home architecture and their platforms and models.

# BIBLIOGRAPHY

[1] S. Erfani, M. Ahmadi, and L. Chen, “The Internet of Things for smart homes: An example,” in *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)*, 2017, pp. 153–157. doi: 10.1109/IEMECON.2017.8079580.

[2] P. M. Jacob and P. Mani, “Software architecture pattern selection model for Internet of Things based systems,” *IET Software*, vol. 12, no. 5, pp. 390–396, Oct. 2018, doi: https://doi.org/10.1049/iet-sen.2017.0206.

[3] O. Taiwo and A. E. Ezugwu, “Internet of Things-Based Intelligent Smart Home Control System,” *Security and Communication Networks*, vol. 2021, p. 9928254, 2021, doi: 10.1155/2021/9928254.

[4] N. M. Allifah and I. A. Zualkernan, “Ranking Security of IoT-Based Smart Home Consumer Devices,” *IEEE Access*, vol. 10, pp. 18352–18369, 2022, doi: 10.1109/ACCESS.2022.3148140.

[5] K. Maswadi, N. B. A. Ghani, and S. B. Hamid, “Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly,” *IEEE Access*, vol. 8, pp. 92244–92261, 2020, doi: 10.1109/ACCESS.2020.2992727.

[6] Q. I. Sarhan, “Systematic Survey on Smart Home Safety and Security Systems Using the Arduino Platform,” *IEEE Access*, vol. 8, pp. 128362–128384, 2020, doi: 10.1109/ACCESS.2020.3008610.

[7] H. Washizaki, S. Ogata, A. Hazeyama, T. Okubo, E. B. Fernandez, and N. Yoshioka, “Landscape of Architecture and Design Patterns for IoT Systems,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10091–10101, 2020, doi: 10.1109/JIOT.2020.3003528.

[8] N. Gavrilović and A. Mishra, “Software architecture of the internet of things (IoT) for smart city, healthcare, and agriculture: analysis and improvement directions,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1315–1336, 2021, doi: 10.1007/s12652-020-02197-3.

[9] Y. Zhang *et al.*, “APDP: Attack-Proof Personalized Differential Privacy Model for a Smart Home,” *IEEE Access*, vol. 7, pp. 166593–166605, 2019, doi: 10.1109/ACCESS.2019.2953133.

[10] A. Qashlan, P. Nanda, X. He, and M. Mohanty, “Privacy-Preserving Mechanism in Smart Home Using Blockchain,” *IEEE Access*, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[11] B. B. Gupta and M. Quamara, “An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols,” *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, p. e4946, Nov. 2020, doi: https://doi.org/10.1002/cpe.4946.

[12] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. S, and B. Minaei-Bidgoli, “DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management,” *IEEE Access*, vol. 8, pp. 140008–140018, 2020, doi: 10.1109/ACCESS.2020.3012435.

[13] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, “A Secure IoT Service Architecture With an Efficient Balance Dynamics Based on Cloud and Edge Computing,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4831–4843, 2019, doi: 10.1109/JIOT.2018.2870288.

[14] G. Mokhtari, A. Anvari-Moghaddam, and Q. Zhang, “A New Layered Architecture for Future Big Data-Driven Smart Homes,” *IEEE Access*, vol. 7, pp. 19002–19012, 2019, doi: 10.1109/ACCESS.2019.2896403.

[15] S. H. M. S. Andrade, G. O. Contente, L. B. Rodrigues, L. X. Lima, N. L. Vijaykumar, and C. R. L. Francês, “A Smart Home Architecture for Smart Energy Consumption in a Residence With Multiple Users,” *IEEE Access*, vol. 9, pp. 16807–16824, 2021, doi: 10.1109/ACCESS.2021.3051937.

[16] K.-L. Tsai, F.-Y. Leu, and I. You, “Residence Energy Control System Based on Wireless Smart Socket and IoT,” *IEEE Access*, vol. 4, pp. 2885–2894, 2016, doi: 10.1109/ACCESS.2016.2574199.

[17] M. A. Paredes-Valverde, G. Alor-Hernández, J. L. García-Alcaráz, M. del P. Salas-Zárate, L. O. Colombo-Mendoza, and J. L. Sánchez-Cervantes, “IntelliHome: An internet of things-based system for electrical energy saving in smart home environment,” *Computational Intelligence*, vol. 36, no. 1, pp. 203–224, Feb. 2020, doi: https://doi.org/10.1111/coin.12252.

[18] P. Franco, J. M. Martínez, Y.-C. Kim, and M. A. Ahmed, “IoT Based Approach for Load Monitoring and Activity Recognition in Smart Homes,” *IEEE Access*, vol. 9, pp. 45325–45339, 2021, doi: 10.1109/ACCESS.2021.3067029.

[19] P. Pierleoni, R. Concetti, A. Belli, and L. Palma, “Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison,” *IEEE Access*, vol. 8, pp. 5455–5470, 2020, doi: 10.1109/ACCESS.2019.2961511.

[20] S. N. Swamy and S. R. Kota, “An Empirical Study on System Level Aspects of Internet of Things (IoT),” *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.