Classification and Analysis of Internet-of-Things Architecture Based on Scalability, Security and Energy Efficiency

Dr. Shalini Aggarwal[1]
Mr. Karan Singh bisht[2]

ABSTRACT

Internet of Things (IoT) comprises things that have unique identities and are connected to the internet. IoT is a new revolution in the capabilities of the devices that are connected via the internet, and is being driven by the advancement in capabilities (cost-effective) in sensor networks, mobile devices, wireless communications, networking and cloud technologies with minimum or no human intervention. The scope of IoT is not limited only to connecting devices to the internet but also allows communication and exchange of data among themThe Internet of Things (IoT) represents a significant evolution in internet technology, enabling the connection and communication of billions of devices worldwide. This paper aims to provide a comprehensive review and classification of IoT architectures. We examine the various layers, models, and frameworks proposed in the literature, identifying common themes and differences. By analyzing these architectures, we aim to offer insights into their design principles, strengths, and weaknesses. Our review highlights the critical role of architecture in IoT deployment and suggests directions for future research to address current challenges and enhance IoT system efficiency and security. This paper presents a review and classification on architecture of IoT based on the challenges in application of IoT. It provides an overview of the classification of the architecture based on scalability, security and energy efficiency. This paper evaluates various contributions of researchers in different areas of IoT architecture. It will give good comprehension for the new researchers, who want to do research in this field of Internet of Things.

Keywords: *Internet of Things (IoT), Three-layer architecture, Scalability, Security, Energy-efficiency.*

I. Introduction

Internet of Things (IoT) is a smart technology through which many smart devices can be connected seamlessly. IoT has been defined by different authors in many different ways. The most popular definitions define the Internet of Things as simply an interaction between the physical and digital worlds [1]. The digital world interacts with the physical world using a plethora of sensors and actuators. Another definition by [2] defines the Internet of Things as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object. The IoT technology has introduced a new world where almost all the devices and appliances that we use are connected to each other via network. With this technology, the connecting devices require none or very little human intervention to communicate with each other. IoT devices are well equipped with embedded sensors, actuators, processors, and transceivers.

Sensors and actuators are devices, which help in

[1]*Associate Professor, Institute of Professional Excellence & Management, Ghaziabad, India, Dr.shaliniaggarwal@ipemgzb.ac.in, ORCHID ID – 0000-0001-9172-3420*

[2]*Student, Graphic Era Hill University, Dehradun, India, karansbhist01@gmail.com*

interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it. An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner [3]. The storage and processing of data can be either done on the edge of the network or on a server at a remote location. In the possibility of preprocessing of data, then it is done either by the sensor or some other device in proximity. The storage and processing capabilities of an IoT device are restricted by the resources available, energy, power, and computational capability.

With the advent of ubiquitous computing, IoT has witnessed manifold advancement in nearly all the applications such as augmented reality, high-resolution video streaming, smart environment, smart transportation, self-driving vehicles, advanced health care equipment etc. All these applications require high bandwidth, high frequency data rate, low end-to-end delay and high throughput. Many architectures for IoT have been proposed recently, they all attempt to cover the main characteristics of IoT which are [4]

Distributive: IoT model is probably developed in an enormously distributed environment, where data can be collected from various sources and consequently can be processed via distinctive smart entities in a distributed procedure.

Interoperability: IoT devices that belong to distinct vendors have to communicate with each other to obtain mutual goals. Protocols and systems must be also designed in a manner that permits smart devices from numerous manufacturers to exchange their sensed data in an interoperable manner.

Scalability: Billions of objects are expected to join the network of any IoT environment. Thus, applications and systems that run on these environments must be able to manage and process a tremendous amount of data.

Resources scarcity: Both computation units and energy are considered to be highly scarce resources.

Security: Users' feelings of being helpless and exposed under the control and dominant of an unknown external device could sorely handicap IoT deployment.

There are three components of IoT architecture:

Hardware: It comprises nodes with sensing technology, through which data can be gathered.

Middleware: This layer is responsible for processing the raw data, data storage, analysis and managing resources.

Presentation layer: It comprises efficient visualization tools that are compatible with various platforms for different applications and present the data to the end user in an understandable form.

In this work, a classification and analysis of Internet-of-Things architecture based on scalability, security and energy efficiency. Various contributions of researchers in different areas of IoT architecture are evaluated. Numerous challenges related to the IoT architecture have been identified, ranging from interoperability, QoS, reliability and lack of common standards. Implementation of various IoT protocols like Constrained Application Protocol, Distributed Location Service, Distributed Geographic Table are discussed and analyzed from architectural perspective. Cross layer IoT architecture is analyzed to over come the limitations of scalability, heterogeneity and security. Use of edge computing is explored for

detection of devices dynamically, their configuration and management of data. Use of Advanced Encryption Standard is explored for authenticating a Radio frequency identification tag to a reader device. Various approaches for providing better energy efficiency to the IoT nodes are compared and evaluated.

Rest of the paper is organized as follows. Section two gives the various IoT architectures proposed in few major earlier works. Classification of IoT architecture based on scalability, security and energy-efficiency is presented in section 3. A brief analysis is done in section 4. Finally, section 5 concludes the work.

2. Architecture of IoT

This paper provides classification of architectures of IoT based on scalability, security, and efficient-energy consumption. There is no global consensus on the architecture of IoT, so different IoT architectures have been suggested by many researchers [3]. The architecture of IoT is based on the "Three based architecture" model as mentioned in [5]. The basic Three Layer Architecture (Fig 1) comprises mainly the perception layer, network layer, and application layer.

The Perception Layer: Through this layer information about the environment is gathered with the help of sensors at the physical level.

The Network layer: This layer is responsible for transmitting and processing sensor data and connecting to other smart things, network devices, and servers.

The Application layer: Specific services are delivered to the user through this layer. It defines various applications in which the IoT can be implemented, for instance, home automation, smart cities, smart transportation, health care facilities and many more.

In addition to this three-layer architecture, two more layers transport layer and processing layer, business layer have been included in the architecture of IoT [6]-[7].

The transport layer and the processing layer: Transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC. The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer.

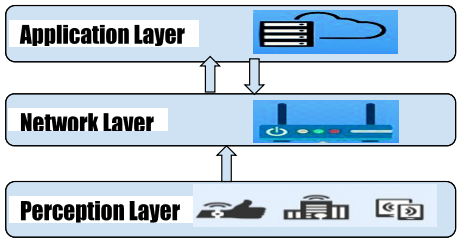

Fig 1: Three Layer Architecture

The business layer: Manages the whole IoT system, including applications, business and profit models, and users' privacy.

2. Classification of Architecture of IoT

Classification of IoT architecture has been done based on scalability, security and energy-efficiency and is shown in Table 1.

Scalability

With the growth of IoT, one of the major challenges is scalability. Scalability is the ability of a device to adapt to the changes in the environment and meet the changing needs in the future. It is an essential feature of any system which has the capability to handle the growing amount of work.

In [8] the authors have designed a peer-to-peer architecture of automatic service discovery for large-

scale IoT networks. The architecture implements the Constrained Application Protocol (CoAP) [20] -based service catalogs and extensively use the Distributed Location Service (DLS) and Distributed Geographic Table (DGT) for service registration and query. Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability. To access a resource the name resolution service is DLS based on the Distributed Hash Table (DHT). A distributed hash table (DHT) [21] is a decentralized storage system that provides lookup and storage schemes similar to a hash table, storing key-value pairs. Each node in a DHT is responsible for keys along with the mapped values. The DGT is used to retrieve a list of resources matching geographic conditions based on a distributed node location database.

In [9], the authors have proposed a Distributed Internet-like Architecture for Things (DIAT), which overcomes most of the obstacles in the process of large-scale expansion of IoT. DIAT is a cross layer architecture that provides solutions to limitations of scalability, heterogeneity and security. The authors group the IoT infrastructure into three layers namely; (i) Virtual Object Layer (VOL), (ii) Composite Virtual Object Layer (CVOL), and (iii) Service Layer (SL), these three layers and their functionalities are put together as a stack called the IoT Daemon. The VOL hosts the virtual representation of physical objects and is responsible for communication between the digital and physical world. The CVOL is responsible for communication and coordination between multiple VOs in order to achieve a particular task. The creation and management of services is handled by the SL. After receiving the service request, SL analyzes and divides it into subtasks according to the requirement.

Table 1. Classification of Architecture of IoT

Issue Addressed	Related Work	Approach
Scalability	A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things [8]	Self-configuring peer-to-peer (P2P)-based architecture
	DIAT: A Scalable Distributed Architecture for IoT [9]	Distributed Internet-like Architecture for Things
	A scalable and manageable architecture based on transparent computing [10]	Five-layer Architecture
	Scalable IoT Platform for Heterogeneous Devices in Smart Environments [11]	Edge computing for smart environments
Security	A Novel Secure Architecture for the Internet of Things [12]	Security verification system
	Strong Authentication for RFID Systems Using the AES Algorithm [13]	A low-power implementation of the AES
	Low-Cost Cryptography for Privacy in RFID Systems [14]	Probabilistic (symmetric or asymmetric) encryption Function
	Secure communication and firewall architecture for IoT applications [15]	Firewall architecture
Energy Efficiency	An Energy-Efficient Sleep Scheduling With QoS Consideration in 3GPP LTE-Advanced Networks for Internet of Things [16]	Prolonged Sleep Scheduling
	An Energy-Efficient Architecture for the Internet of Things (IoT) [17]	Three layer architecture
	Self-Organized Things (SoT) An energy efficient next generation network management [18]	Self Organized Thing framework,
	An energy efficient hierarchical clustering index tree for facilitating time-correlated region queries in the Internet of Things [19]	Hierarchical clustering index tree

In [10], a manageable, scalable, and transparent IoT architecture is proposed by the authors as a response to these challenges. The proposed architecture consists of five layers, i.e., end-user layer, edge network layer, core network layer, service & storage layer, and management layer. The architecture is evaluated as an efficient solution in terms of energy consumption for resource management and on-demand service provisioning of IoT objects.

In [11], the authors have proposed an open and scalable IoT architecture using edge computing, which allows discovery of devices dynamically, their configuration

and management of data. The proposed approach is based on the given characteristics: i) handle large number of users ii) provide standard communication protocol which remains same in all smart environments iii) to retrieve a list of IoT devices available in the network, device discovery mechanism is implemented iv) to optimize data publication, data consumption and network consistent hashing load balancing is done at the edge of the network.

Security

Security becomes vital in IoT applications as they are expected to interact with the physical world, especially in safety critical applications like health, defense, automobiles etc. The traditional security model for Internet applications is not suitable for IoT, as it is mostly non-realtime and non-safety critical. The information exchange needs to be secured so that any unauthorized user should not access the information.

In [12] the authors proposed a novel security architecture for the IoT to solve the relationship between heterogeneous devices and different security issues. Most of the architectures based on security require a random number generator to be implemented in the devices. In [13], the authors proposed a secure IoT architecture that implements device authentication without the requirement of any random numbers. They introduce an authentication protocol which serves as a proof of concept for authenticating a Radio frequency identification (RFID) tag to a reader device using the Advanced Encryption Standard (AES). Advanced Encryption Standard (AES) is a symmetric block cypher and adopted as the standard of encryption. The main part of this work is an implementation of AES hardware which encrypts a 128-bit block of data within 1000 clock cycles.

In [14], authors have proposed a scheme based on probabilistic encryption function and a coupon-based signature function. By choosing low-cost cryptographic algorithms, highly secure solutions can be achieved in the RFID environment without affecting the current communication protocols. Novel secure communication and firewall architecture is proposed in [15], which is based on off-loading computational load by introducing a server in the network to decrease computational load to prevent attacks to IoT. Edge devices provide distributed operation among the IoT network using dynamic host configuration protocol and domain name systems.

Energy Efficiency

The ubiquitous nature of IoT is responsible for draining out energy from its resources. Therefore, the energy efficiency of IoT resources has emerged as a major research issue.

In [16], authors have proposed a scheme where the device switches to sleep mode during non-active periods and wakes up on demand, thus saving energy of the device. To optimize the energy consumption of the device, the sleep periods can be prolonged. 3GPP LTE-A has defined the discontinuous reception/ transmission (DRX/DTX) mechanism which allows the devices to turn off their radio interfaces, to manage power consumption. This paper optimizes the DRX/DTX to maximize the sleep periods of devices without compromising on QoS.

In [17], authors proposed a three layer of hierarchical architecture namely Sensing and Control layer (SCL), Information Processing layer (IPL) and Application layer (AL). Energy related information is shared

between the SCL and the IPL, which controls the sleeping time interval of the sensors. These sensors work in two modes; periodic mode for periodic events and trigger mode for critical events. Energy efficiency and hardware resource utilization is increased by SCL and IPL. In [18], authors have proposed Self-organized Things (SoT), to reduce energy consumption, maintain connectivity and coverage area of the network and maximize network lifetime by undergoing automatic configuration of the sensors. These self-adapting devices interact with nearby devices to monitor the environment and change the process efficiently. In this self-management process of the SoT, specific spatial distributions of devices and intersections of their coverage areas are also analytically derived. In [19], authors have divided the sensor nodes into grid cells, and organize them by an energy-efficiency hierarchical clustering index tree. Energy consumption of the system is reduced at a primary level by reporting their values to the base station once in the beginning and then only when they change significantly.

3. Analysis

Many requirements have to be accomplished to achieve a functional implementation of IoT architecture. Several researchers have proposed different architectures ranging from three layers and five layers in order to mitigate the issues of scalability, security and energy-efficiency. Cross layered architecture has been generally proposed to handle large scale IoT networks. Most of the work relies on self-configuration of IoT devices. The DIAT [9] architecture not only handles scalability but also security and privacy aspects. Few researchers have addressed the issue of security at each layer individually. It is essential to secure and protect all these interactions with preservation of the highest system performance and limiting total incidents which are affecting the entire IoT system. The network life time is extremely crucial for the working of IoT, thus, energy consumption should be reducing redundancy of energy usage.

4. Conclusion

This paper provides an overview of various IoT architectures based on different parameters. The paper reviews and analysis these parameters and conclude that numerous challenges have been identified, ranging from interoperability, QoS, reliability and lack of common standards. A classification and analysis of Internet-of-Things architecture based on scalability, security and energy efficiency is presented. Various contributions of researchers in different areas of IoT architecture are evaluated. Numerous challenges related to the IoT architecture have been identified, ranging from interoperability, QoS, reliability and lack of common standards. Implementation of various IoT protocols like Constrained Application Protocol, Distributed Location Service, Distributed Geographic Table are discussed and analyzed from architectural perspective. Cross layer IoT architecture is analyzed to over come the limitations of scalability, heterogeneity and security. Use of edge computing is explored for detection of devices dynamically, their configuration and management of data. Use of Advanced Encryption Standard is explored for authenticating a Radio frequency identification tag to a reader device. Various approaches for providing better energy efficiency to the IoT nodes are compared and evaluated.Moreover, work can be done in designing architectures that meet the requirements of real-life applications of IoT and can

mitigate the problems faced in rural areas. The architecture should enable a seamless flow of information to and from a device, infrastructure, cloud and applications. The IoT architecture should also support the business requirements and outcomes.

References:

- O. Vermesan, P. Friess, P. Guillemin et al., "Internet of things strategic research road map," in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.
- I. Pena-Lopez, ´ Itu Internet Report 2005: The Internet of Things, 2005
- Sethi P. Sarangi S. R. (2017). "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, 2017, pp. 1–25. Advance online publication. 10.1155/2017/9324035
- Abdmeziem M.R., Tandjaoui D., Romdhani I. (2016) "Architecting the Internet of Things: State of the Art". In: Koubaa A., Shakshuki E. (eds) Robots and Sensor Clouds. Studies in Systems, Decision and Control, Springer, Cham. pp. 55-75 vol 36.
- A. Yousefpour, G. Ishigaki, R. Gour and J. Jue, "On Reducing IoT Service Delay via Fog Offloading," IEEE Internet of Things Journal , vol. 5, no. 1, 2018.
- O. Said and M. Masud, "Towards internet of things: survey and future vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.
- Wafa'a Kassab and Khalid A. Darabkh, "A-Z Survey of Internet of Things: Architectures, Protocols, Applications, Recent Advances, Future Directions and Recommendations," Journal of Network and Computer Applications, Elsevier, vol. 163, 102663, August 2020.
- S. Cirani et al., "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 508-521, Oct. 2014,
- C. Sarkar, A. U. Nambi S. N., R. V. Prasad, A. Rahim, R. Neisse and G. Baldini, "DIAT: A Scalable Distributed Architecture for IoT," IEEE Internet of Things Journal, vol. 2, no. 3, pp. 230-239, June 2015,
- Hui Guo, Ju Ren, Deyu Zhang, Yaoxue Zhang, Junying Hu, "A scalable and manageable IoT architecture based on transparent computing", Journal of Parallel and Distributed Computing, Volume 118, Part 1, pp. 5-13, 2018.
- A. Javed, A. Malhi, T. Kinnunen and K. Främling, "Scalable IoT Platform for Heterogeneous Devices in Smart Environments," IEEE Access, vol. 8, pp. 211973-211985, 2020.
- J. Qian, H. Xu and P. Li, "A Novel Secure Architecture for the Internet of Things," in 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2016, pp. 398-401.
- Feldhofer M., Dominikus S., Wolkerstorfer J. (2004) "Strong Authentication for RFID Systems Using the AES Algorithm" In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg.
- B. Calmels, S. Canard, M. Girault, and H. Sibert, "Low-Cost Cryptography for Privacy in RFID Systems," in Smart Card Research and Advanced Applications, vol. 3928, J. Domingo-Ferrer, J. Posegga, and D. Schreckling, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 237–251
- N. Maheshwari and H. Dagale, "Secure

communication and firewall architecture for IoT applications," in Proc. 10th Inter. Conf. on Communication Systems & Networks (COMSNETS), pp. 328-335, 2018, doi: 10.1109/COMSNETS.2018.8328215.

- J. Liang, J. Chen, H. Cheng and Y. Tseng, "An Energy-Efficient Sleep Scheduling with QoS Consideration in 3GPP LTE-Advanced Networks for Internet of Things," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 13-22, March 2013, doi: 10.1109/JETCAS.2013.2243631.
- N. Kaur and S. K. Sood, "An Energy-Efficient Architecture for the Internet of Things (IoT)," IEEE Syst. J., vol. 11, no. 2, pp. 796–805, Jun. 2017.
- U. Akgul, B. Canberk, "Self-Organized Things (SoT): An Energy Efficient Next Generation Network Management," Computer Communications (Elsevier), vol. 74, pp. 52-62, January 2016.
- Tang, Jine, ZhangBing Zhou, Jianwei Niu, and Qun Wang. "An energy efficient hierarchical clustering index tree for facilitating time-correlated region queries in the Internet of Things," Journal of Network and Computer Applications, vol. 40, pp. 1-11, 2014.
- Z. Shelby, K. Hartke, and C. Bormann. (Jun. 2013). Constrained Application Protocol (CoAP). RFC 7252 (Proposed Standard), Internet Engineering Task Force [Online]. Accessed: July 2, 2021.
- K. Wehrle, S. G otz, and S. Rieche, "Distributed hash tables," Peer-to-Peer Systems and Applications, vol. 3485. Springer, 2005, pp. 79–93