Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

A COMPARATIVE METHOD OF IOT ARCHITECTURES, CHALLENGES, PRIVACY AND SECURITY ISSUES

Ramisetti Uma Maheswari[1], V Mareeswari[2]
Department of Computer Science & Engineering, A C S College of Engineering, Bangalore
Visvesvaraya Technological University, Belagavi, Karnataka - India
ramisetti.uma22@gmail.com, mareesh.prasanna@gmail.com

ABSTRACT: It has been anticipated that all the different things of our surroundings to be under the internet. At current internet is a global network of computing or computer devices. The Idiom IoT is the scope of the internet is to be prolonged outside computer devices being interconnected to different things. Internet of Things is a categorization or classification where interconnects these non-living things like devices that can club together then try to communicate or to establish a protocol between them that they can effectively communicate among themselves and they can perform in a good manner without human intervention. As of now there is no efficient usage of IoT framework due to its now and then remodeling strategies, Due to heavy usage of IoT framework there is lot more to concern about security and privacy. This particular article deals with various IoT framework and their working and challenges of IoT framework.
Keywords: IoT framework, challenges, security issues, privacy concerns.

1. Introduction

One basic element in that made smart home and smart cities possible is IoT which has an enormous future the coming trend. The term IoT was introduced by Kevin Auston. The Internet is associated with nearly over 10 billion ‘things. The number of connected things is going to be projected across 20 billion and trillions in the future. The IoT is going to be a very complex network with a much wider scope than the internet with many more complexities.

At present IoT is a very advanced technology making them around things as “connected mode”? IoT is moving towards any time, any place, any device connected to anything [1]. Figure 1 describes that the IoT can have the potential to interconnect via the internet to anything. Anything connected to any device present in any place at any time by providing good services by using any network to anyone. The basics of the IoT diagram are given below Figure 1.

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

IoT can be offered as a community of close to effects that are regarding the Internet as a multiplicity of sensors, gadgets that can be captured, stored, managed. The quantity of IoT units is developing every day. The primary issue for developing the quantity of IoT gadgets is that they come up with the money for a higher effect compared to humans.

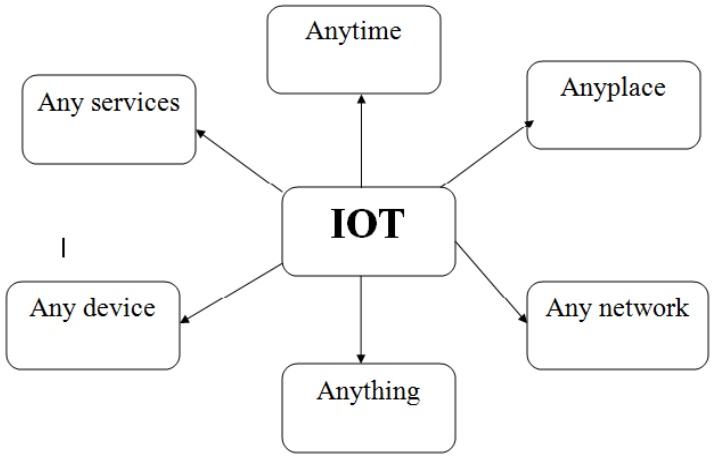

Figure 1. Iot Block Diagram

Section 2 presents related work. Section three suggests the proposed methodology with quite several IoT architectures and several challenges of IoT. Section four discusses performance evaluation. At last the article ends with a good overview and reported about future scope.

2. Related Work

In [2] the author states that there are many types of research are being carried out on IoT and security of IoT. The main research is being carried out on communication protocols of IoT as these protocols are quite different from regular its protocols, even though there are main research carried out there are still several questions remained unchanged due to un unified security framework of IoT. The author concluded many international organizations are still working hard to provide a solution for security for IoT based applications. In [3] the main aim of this author is to propose a six layered secure iot architecture to overcome the problems which we are facing in previous architecture where these architectures have a different number of layers numbering from 3 to 5 layers with divergent features and functionality.

The author is mainly focusing on privacy and security issues in IoT [4] .so in ordered to overcome this problem he has done many types of research and surveys on privacy and security issues and gave a four-dimensional solution where every solution has a different point of view. The first solution is to provide security to IoT devices components like battery power consumption for which he proposed a lightweight encryption scheme specifically developed for embedded systems. The second one deals

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

with various possibilities for IoT security attacks such as remote and physical attacks. The Third one is regarding authentication and authorization of IoT devices. The Fourth one deals with IoT layer security in IoT architecture [5][6].

IoT has extended its research in transportation also which deals with some unique features like finding the current location of the vehicle, the total load on the vehicle, current speed at a particular point of time can also be calculated. Author [7] has extended his research on transportation by opting for some solutions like sending alerts to nearby police stations if a vehicle cross speed limit. This is done by using some speed calculating sensors like accelerometers, gyroscopes and speedometers which are installed in vehicles [8]. He gave a distinctive solution to automatically reduce the speed by taking control of the vehicle gear and brake system.

In [9] the author defined a problem of query optimization in the internet of things as we know the iot devices sense the huge amount of data every data so it is an enormous task to optimize the data and provide an efficient solution for it [10]. So, the author comes up with a query optimization technique which breaks large query into smaller modules and finds the solution individually. In this technique the predefined data division request is made through which the query will be divide and distributed equally among the entire processors.

3. Proposed Methodology

3.1 IoT Architecture

IoT architecture is like OSI and TCP/IP models. In IoT there are many layers to be interconnected for each layer there should be a protocol the same in OSI and TCP/IP model [11]. This article presents the different IoT frameworks starting in the year 2008 to current there are numerous and unique frameworks that came into play.

In the 2008 [12] IoT framework, the first layer is the perception layer it is identified as a network access layer that is used to represent the information from the atmosphere and stored in it. The second layer is the internet network layer which is also identified as the network layer which is responsible for advertising and data packets, manipulation, and mainly used for routing. The third layer is the transport layer which is also identified as the middleware main task of this layer is to have a communication of end to end. It can provide connections to devices for sending and receiving. The fourth layer is the application layer. This is the higher layer in the OSI model it acts as an administrator and reports end-user services of the fifth layer is the business layer. It is used for managing the overall architecture and functioning of layers. IoT architecture is shown in figure 2.

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/
P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

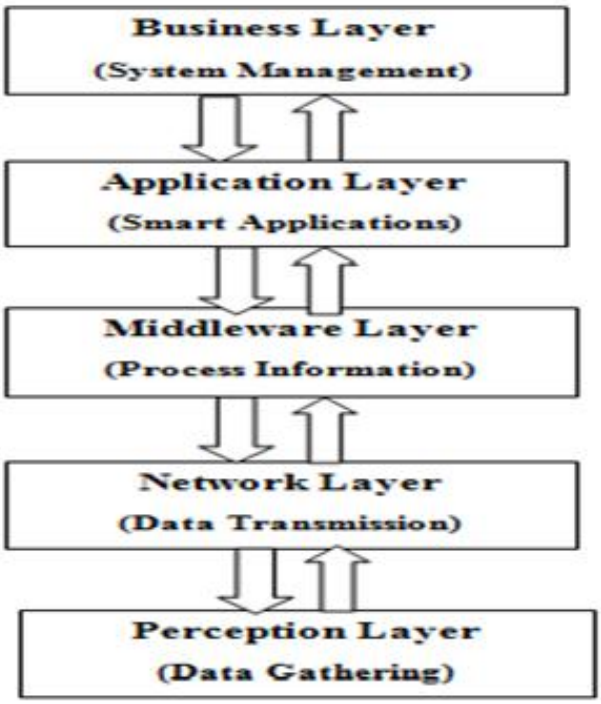

Figure 2. IoT Architecture

3.2 IoT Challenges

Any application definitely would face the challenges many challenges are there in the IoT are:

3.2.1. Security and Privacy:

Whenever the records are stored in a cloud that raised a question that data is safe or not. Data is our asset. The data is exposed outside of the firewall. The data is to be attacked and vulnerable. The hacker can hack the data. This is a very major challenge in business. Privacy and security are the foremost problems that will face in the cloud.

3.2.2. Bandwidth and Related Constraints:

In Bandwidth, there is not necessary to invest in the network, not necessary for the maintenance of the network to the cloud. All these are advantages in bandwidth. But certainly, there are disadvantages. By transferring the data at a low rate. For a large amount of data, we need a high bandwidth rate. In IoT the sensors capture the data and send in very fast so we need a high bandwidth rate.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

3.2.3. Portability/ Migration:

The records are to be stored in a cloud. The data is to be migrated from one place to another is not easy because it is a huge amount of data known as big data. The amount of data is all about sensors, data on IoT. It is crucial to migrating the data.

3.2.4. Availability:

Availability is one of the finest challenges that are facing. IoT is all about monitoring the devices, monitoring the environment, gathering the data continuously and it has to be spontaneous when to store data. If availability is lack then the data has to store in the device and send and receive. It is a critical problem. The service needs of a cloud of 24/7 to store data.

3.2.5. Reliability:

When the fewer amounts of data are sending to the cloud is reliable but a huge record is speedily transferring to the cloud it is robustness.

3.2.6. Data Ownership:

The data has to be stored safely in the cloud. We agree that data is safe. But the data is stored in a cloud service provider that means the data owns by the service provider. This is a huge challenge in IoT. We don't know the data is safe or not it depends on the cloud service provider.

3.2.7. Complexity:

IoT block diagram consists of several layers like network layer, software layer, etc, for every layer contains an enormous number of devices that are associated and these devices require communication. To merge all the devices connected in every layer with a network is very difficult.

4. Performance Analysis

This section analyses the existing work with the proposed methodologies. As shown in Table 1, several models regarded isolation renovation in IoT. Every architecture represents layers where every layer has a special task to perform. IoT frameworks starting in the year 2008 to current there are numerous and unique frameworks that are mainly concentrated on privacy and security issues.

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/
P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

Table 1. Comparison of IoT Architectures

Architecture	Year	Architecture Stack	Security	Privacy
Five-layered IoT Architectures	2008	1. Business 2. End User 3.Processing 4. Internet 5. Network Access	No	No
IoT Three-layer Architectures	2010	1. End User 2.Transport 3. Network Access	No	No
IoT Architecture based on Trusted Security System.	2011	1. User . Trusted method 2. Internet . Trusted method 3. Network. Trusted method 4. Middleware . Trusted method 5. Agent. Trusted Method	Yes	No
Five-layered IoT Architectures	2012	1. Business 2. Processing 3. Transport 4. Internet 5. Network Access	No	No
IoT based Service-oriented Architecture	2014	1. Network Access 2. Transport 3. Internet 4. Process	No	No
IoT	2015	1. Application	Yes	No

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

architecture on Decentralized Data and Centralized Control		2. Process 3. Transport 4. Internet		
Four-layered IoT architecture on security	2017	1. Business 2. Process 3. Transport 4. Internet	Yes	No
An IoT architecture on Block chain for management in scalable access	2018	1. Wireless Sensor Network. 2. Administrators 3. Users Node 4. Block chain Network 5. Administration Hubs	Yes	No
5G-IoT architecture	2018	1. Access Layer 2. Data Communication 3. Edge Computing 4. Middleware 5. Data Analysis Service 6. Application 7. Collaboration and Processes 8. Protection	Yes	No
IoT Architecture Based on Micro services	2018	1. Customer devices and application 2. Cloud based micro services 3. Edge server micro services	Yes	No

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

This graph in Figure 3 represents the IoT privacy and security concerns. By every year our IoT architecture concentrated on privacy and security issues from 2008 to 2018 still users are facing privacy issues because billons of devices are connected to IoT.

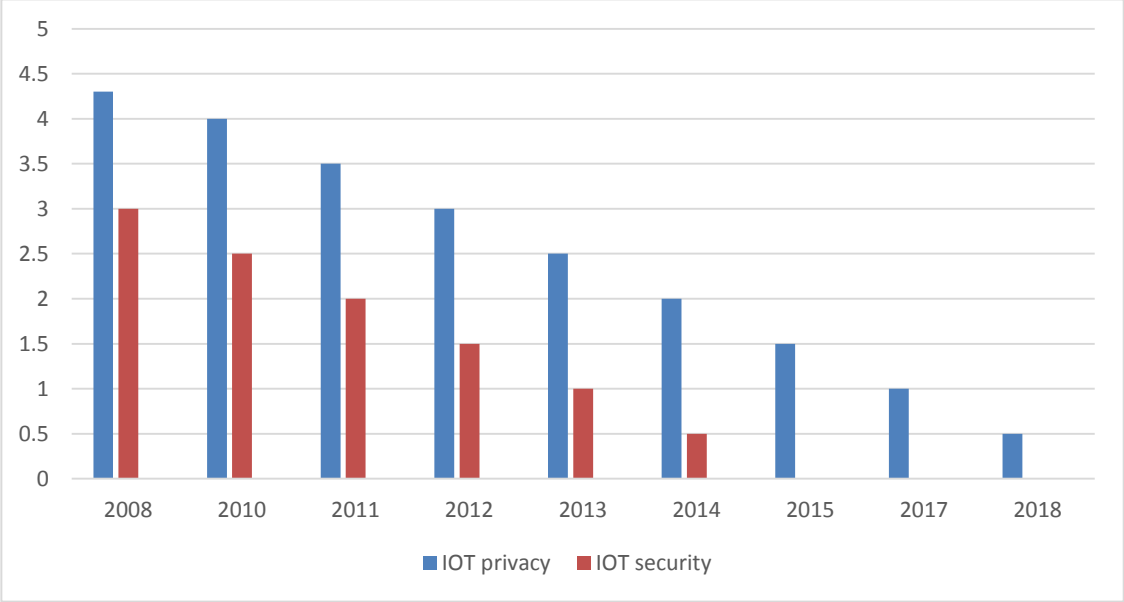

Figure 3. IoT privacy and security concerns

5. Conclusion and Future Work

The amount of IoT units is mounting in everyday life. The main issue for growing the range of IoT gadgets is that they grant a higher effect on devices compared to human beings. There are restrictions in every architecture. The consequence shows the enhancement of IoT architecture. In initial IoT, architecture didn't afford a comprehensive view of security and privacy. Late architectures are measured by IoT security and privacy concerns. This article describes the IoT models and the comparison of IoT models of security and privacy concerns. By using IoT many challenges are faced by many people in the world. By using IoT in 4G for data bandwidth rate, downloading the information, and transferring the data which are captured from sensors is vulnerable and not having the capability. The investigation is prolonged with regarding to privacy and security in current IoT frameworks and designing new methods to resolve issues in IoT architectures via the usage of 5G the upcoming technology of IoT is efficient and can limit safety and privacy concerns.

References

[1].Mritunjay Kumar, Km Annoo, Raman Kumar Mandal,“ The Internet of Things Applications for Challenges and Related Future Technologies & Development”, International Research Journal of Engineering and Technology Vol.5, Issue 1, 2018.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust In Internet Of Things: The Road Ahead”, Computer Networks, vol.76, pp. 146–164, 2015.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.230

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet Of Things Security: A Survey" , Journal of Network and Computer Applications, 2017.
[4] Andrew Whitmore & Anurag Agarwal & Li Da Xu, " The Internet Of Things—A Survey Of Topics And Trends", 2014.
[5] Yang Y , Wu L , Yin G , Li L , Zhao H , "A survey on security and privacy issues in internet-of-things" , IEEE Internet Things 2017 .
[6] Kumar JS, Patel DR, " A survey on internet of things: security and privacy issues", International Journal of Computer Applications, 2014 .
[7] B. Dhanalaxmi, Dr.G.Apparao Naidu, "A Survey on Design and Analysis of Robust IoT Architecture", International Conference on Innovative Mechanisms for Industry Applications, 2017.
[8] Koustav Routh, Tannistha Pal, "A survey on technological, business and societal aspects of Internet of Things by Q3, 2017" ,IEEE 2018.
[9] R. Kotamsetty and M. Govindarasu, "Adaptive Latency-Aware Query Processing On Encrypted Data For The Internet Of Things",25th International Conference On Computer Communication and Networks, pp. 1–7, 2016.
[10] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li_, and Hongbin Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things" ,IEEE 2016.
[11] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, " Research on the architecture of Internet of Things", 3rd International Conference on Advanced Computer Theory and Engineering, vol. 5, pp. 484-487, 2010.
[12] F Alshoumi, Mohammed S, Abdulla Ajhamadani, Dawood all-abri, " Systematic Review Of Existing IoT Architectures Security And Privacy Issues And Concerns", International Journal Of Advanced Computer Science And Applications, vol.10, issue 7, 2019.

Author's Profile

Ramisetti Uma Maheswari, received her B.Tech, M.Tech degree specialized in Computer Science and Engineering. Currently, she is working as an Assistant Professor in the Department of Computer Science and Engineering, MJR College of Engineering and Technology, Andhra Pradesh, and having 2 years of experience in teaching. Her research interests include the Internet of Things and Big Data.

Dr.V.Mareeswari received her B.E, M.E and Ph.D. degree specialized in Computer Science and Engineering. She is a member of various professional associations and has 16 years of experience in teaching. Currently, she is working as an Associate Professor and Head in the Department of Computer Science and Engineering, ACS College of Engineering, Karnataka, India. Her research interests include Information Retrieval, Data mining.