# Security issues with the four-layer architecture of IoT model

– **Harivansh Sharma**
Bachelor of Computer Applications (BCA) 4th Semester, Amity University Noida, India
@harivansh20 https://orcid.org/0000-0001-6361-0955 harivansh.021@gmail.com

**Article History**
**Paper Nomenclature:**
Experiential Research Papers (ERP)
**Paper Code:** CYBNMV1N7DEC2019ERP1
**Submission Online:** 03-Dec-2019
**Manuscript Acknowledged:** 10-Dec-2019
**Originality Check:** 12-Dec-2019
**Originality Test Ratio:** 13%
**Peer Reviewers Comment:** 14-Dec-2019
**Blind Reviewers Remarks** 21-Dec-2019
**Author Revert:** 22-Dec-2019
**Camera-Ready-Copy:** 23-Dec-2019
**Editorial Board Citation:** 25-Dec-2019
**Published Online First:** 11-Feb-2020

Over recent years, the Internet has become the most significant thing for people to deal with it. Around 2 billion people around the world use the Web for e-mails, social media apps, extensive data sharing, sports, etc. The use of the Internet continues to grow; the Web is another major platform for connectivity and networking, defined as the Internet of things (IoT), for computers and intellectual artifacts. The Internet of things is a global platformIoT is indeed a system that allows us to link objects around us (for example, the console with the computer) and communicate through the internet.

**Keywords** : IoT | Security Protocol | Linking | Layers | Internet

## Introduction

IoT manages to find its use in almost all areas to provide enhanced communication among various systems and computers, as well as to allow human contact with the simulated world. Nevertheless, IoT is prone to different security vulnerabilities and has significant concerns about privacy for end-users, as with all that requires the Internet infrastructure to exchange information. In light of its advanced data sharing mechanisms, the concept of IoT remains flawed from such a security point of view, and the correct steps need to be taken at the first stage until the effective and widely recognized acceptance of IoT is further enhanced.

IoT refers (i) to the worldwide network, which interconnects digital objects with IoT technology (ii) a set of technology supporters such as RFIDs (radio frequency identification), sensors, and actuators, machine-to-machine communication devices, etc.

The IoT relies on three components, based on the ability of the smart device to (i) be identified (anything recognizes itself), (ii) connect (anything communicates) and (iii) engage (anything interacts).

The main challenges involved in creating IoT include:

1. Linking: The first problem with interconnection is how systems connect to the internet and the cloud-related platform. It is entirely determined by the ecosystem of the device application and the form of network infrastructure provided.
2. Information and Security: The first issue is that protection and IoT safety are fundamental and distinct from network security, which we know. IoT Protection has always been a contentious issue.
   i. Data Exchange Security
   ii. Cloud Storage Security
   iii. Physical Security
   iv. System Update
3. Connectivity and Adaptability: As the IoT environment is continuously evolving, the company must guarantee that future innovations are supported. Nevertheless, when developing a product, it needs to balance software and hardware.
4. Collection and analysis of data: In addition to safety and privacy, all data collected need to be processed correctly. To manage the cloud storage capacity and to meet the network demands, we must first determine the quantity of data stored and obtained.

## Research methodology

This document states that data confidentiality, anonymity, and trust conform with document states that data confidentiality, anonymity, and trust conform with IoT protection. The overview of the collected data provides new insights, as well as the potential risk hierarchy in the IoT context, to direct further study into the main safety layers of IoT architecture. The risk analysis for each stratum is limited in the absence of precise data to subjective evaluation. While several variables may affect the risk analysis, the risk classification per the application of the IoT model in different environments depends upon the development in the application of the IoT over the years 2013-2014. This article examines the issue as a fundamental safety component of all forms of the information and communication environment from a safety risk approach.

## The four-layer architecture of IoT

The concept of IoT design relies on open standards for enabling current network protocol. IoT design is a traditional, layered architecture consists of four main structures (application layer, network layer, middleware layer, and perception layer).A different layer of IoT architecture shown in fig.1.

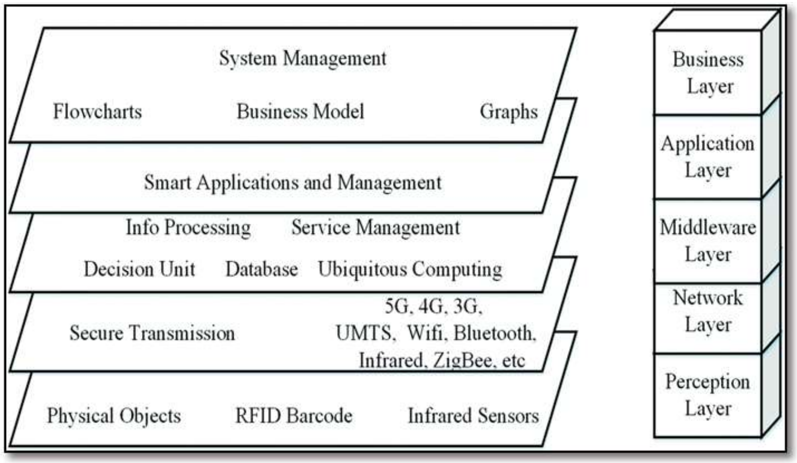


Fig. 1. Four-layer architecture

The perception layer constitutes of two primary functions, collection of data and communication among the same layer components. A network layer comprises of two sublayers, connectivity sublayer which is the central part of the IoT infrastructure, the primary function of which is data transfer to the next point, middleware, which carries on tasks including Smart Route, and Subnet mask Transcription, and the collection of data from the perception layer, transferring information to the sublayer of the Network. The middleware layer for data recovery, replication, synchronization, and cognitive analysis is the most commonly deployed cloud computing system. After collection, the information transferred to the application layer, which utilizes the data to provide and deliver various services to an end-user.

## IoT architecture layers security factors

### Perception layer security issue

Security issues in the perception layer: it is the lowest level of IoT design. The Perception Layer offers access to resources throughout the IoT. The physical protection of sensing devices and confidentiality in the perception layer address security concerns. IoT does not have the security protection system available and is fragile due to limited storage flexibility and light, insufficient node defense that influences the case of terminals such as WSN, RFID, and M2 M.RFID covers security issues such as leakage of information, replay attacks, monitoring of data, hacking, cloning attacks, and man-in - the-medium attacks.

## 4.1 Security issues with wireless sensor networks (WSNs)

WSN are collections of separate nodes with limited frequency and bandwidth wireless communication. The communication nodes of a standard network of wireless sensors compose of the following components:

1. Storage
2. Remote Transceiver
3. Processor
4. Power supply

Despite the limited transmitting path for each WSN sensor node, there is a multi-hop information exchange between the transmitter and the ground station. Wireless sensors retrieve the required information by coordinating the various nodes that have been sentto the node of the sink for driven routing to the ground station. The complex communication network generated by the use of wireless radio transmitters facilitates data transmission among nodes. The transfer of multi-hop data takes multiple nodes to take different congestion loads.

WSN contains sensor nodes, actuator nodes, and others. WSN is a collection node,so security issues are at stake. A wireless sensor activity can be categorized into three sections:

a. Silent threats on network integrity
b. Attacking network efficiency
c. Attacking service integrity

## RFID technology security issue

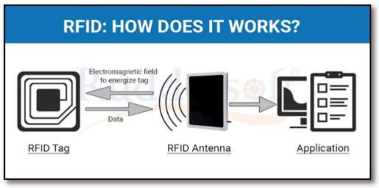


Fig.2. RFID

The lack of sufficient security protocols in a variety of RFID tags enables unauthorized access to their information. Even though the text of the tag might not be challenging to read, it is quite feasible to unauthorize alter or erase the files. A DoS hack could be used to damage the effectiveness of RFID tags. The DoS attempt makes the transmission of the data stored in the tags to failure. Threats against data privacy include threats, including tag interception using an illegal reader to capture confidential information such as zip codes, telephone numbers, and distinguishing tags.Attacks on data integrity refer to unauthorized cloning of tags with the use of unauthorized readers that enable cloning to bypass the authentication methods used.

In addition to these risks, systems utilizing RFID technologies are also sensitive to eavesdropping, MitM threats, spoofing, and many others.

### 4.2. Network layer security factor

It is the foundation of any information and communication system and is not a particular framework for the IoT world. Thus, in other contexts, bugs and risks are exist in this framework, which often reappears in examined mechanisms of security. The IoT definition network layer consisting of the sublayer of connectivity and the sublayer of the Internet The collection of data from the perception layer and for transmission of information to the central network, which forwarded data to the middleware layer, the access sublayer is often used.The primary security vulnerability throughout the network layer constitutes of routing threats such as malicious actions against the path and transmitting data, DoS threats, and so on due to the strict closure of both the backbone network. Route attacks differ from those in the perceptive layer are performed by wired or wireless network transmission.

### 4.3. Middleware security factor

With several different technologies in operation inside the IoT benchmark, various forms of middleware layers are also involved in the integration and protection of systems and data within the same information network. Data needed for specific security restrictions in middleware as well. However, the different communication media for broad IoT implementations can be considered into account in middleware design and development. Although many intelligent devices natively support the continued introduction of IPv6 communications, the IP protocol may not be recognized in the area.Then, ad hoc gates and middleware is used.

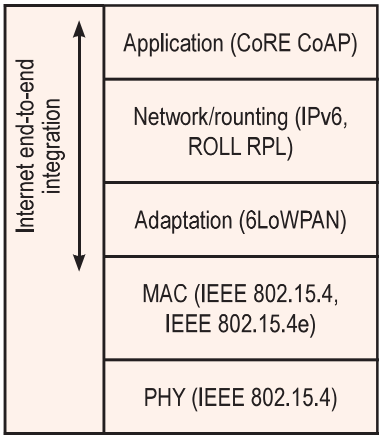

Internet end-to-end integration
Application (CoRE CoAP)
Network/rounting (IPv6, ROLL RPL)
Adaptation (6LoWPAN)
MAC (IEEE 802.15.4, IEEE 802.15.4e)
PHY (IEEE 802.15.4)

Fig. 2.1 Communication protocols in the IoT

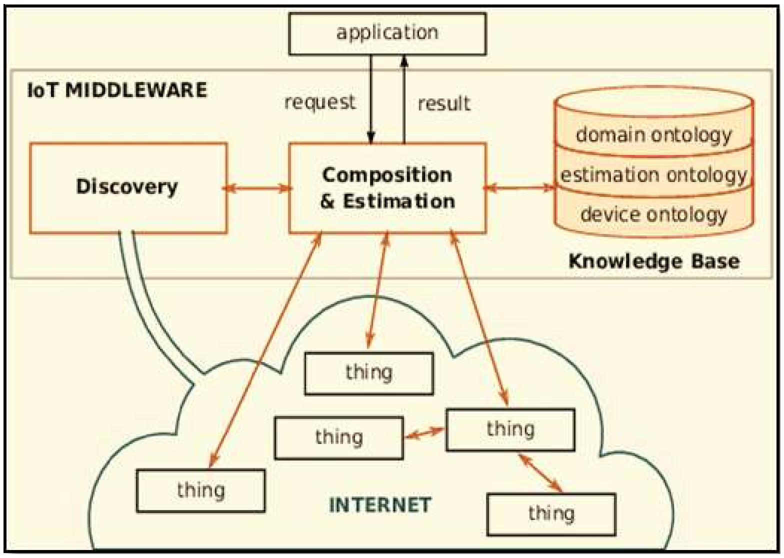


Fig.3. middleware architecture

Because of their advantages, such as delivering storage resources to end-users, efficiency, scalability, and others, the middleware layer is focused on cloud computing. It allows a large number of collected data on the perception layer to be analyzed and processed data to be delivered to end-users using a variety of applications.Thanks to its continued growth and high rate of acceptance, the architecture produces a large number of challenges and flaws in the middleware layer of the IoT cloud computing platform.

Evidence has demonstrated that cloud computing has significant security considerations. The avoidance of data loss and the isolation and protection of data contribute to these aspects. The fact is that all the data obtained from this perception layer raises severe questions regarding data security.

### 4.4 Security issues for the application layer

The Internet of Things has some threats to face in the network, such as unauthorized entry, anonymity, data eavesdropping, privacy, DoS threats, disruption, virus attacks, man-in-middle attacks, and others. IoT detects an extensive range of devices, hence a variety of data forms. IoT implementation is indeed a product of integration with communications technology, digital technology, and industry professionals in numerous fields. Health challenges involve spying and exploitation in the code layer.This layer is vicariously liable for the regulation of traffic. It provides resources for different applications to convert data to a comprehensible type or improve in data gathering by submitting inquiries. Throughout the application layer, constant DoS attacks were introduced by triggering the sensor nodes to generate significant traffic on the road to an access point.

This layer has the functionality of detecting and correctly handling harmful data, spam data, and legitimate data. Social engineering, device glitches, ransomware, spoofing, and sniffing actions are among the issues with protection in this network.

## Business Layer

This layer controls the total resources and operations of the IoT network. Business Layer generates a business model based on data received from the Applications Layer, images, flowchart, and others. The Business Layer is also responsible for implementing, designing, monitoring, analyzing, and developing the IoT elements. This layer facilitates systems of decision making focused on the analysis of big data. Four-layer is also tracked and managedin the business layer.The output for each layer is also linked to planned performance to boost services. It creates different business models for successful market strategies.

## CONCLUSION

IoT is the next move to use Anywhere or Anytime via the Internet. IoT helps us, anywhere, Anyplace, Anything and Anyone to link individuals and computers. This paper gives a description of the IoT and security requirements of IoT.Reported that 50 billion devices will be linked by 2020 through this concept, which places high demands and difficulties in maintaining the necessary level of security in such an environment.In evaluating security vulnerabilities, the most significant safety concern was the interpretation of the design of IoT due to different application limits and the communication infrastructure that was implemented on that platform, accompanied by the cloud-based middleware layer and the inherited vulnerabilities.

## References

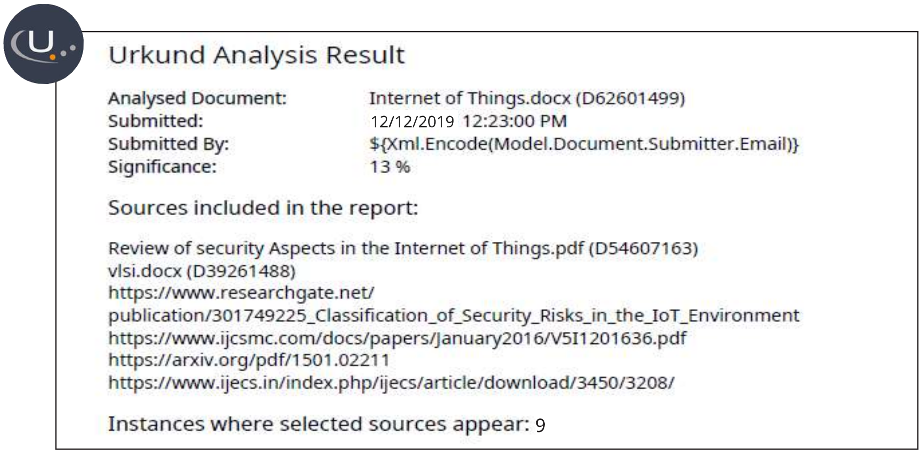
- Ivan, C[vitic]; Vujic, M[iroslav] & Husnjak, S[inisa] (2016), “Classification of Security Risks in the IoT Environment”.
- Suchitra.C et al., “International Journal of Computer Science and Mobile Computing”.
- Balte et al, “International Journal of Advanced Research in Computer Science and Software Engineering.”
- Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu., “Security of the Internet of Things: perspectives and challenges Wireless Networks.”
- S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini,“Security Privacy and Trust in the Internet of Things.”
- T. Borgohain, U. Kumar, and S. Sanyal, “Survey of Security and Privacy Issues of Internet of Things”“International Jurnal of Advanced Network Applications”.
- J. Granjal, E. Monteiro, J. Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues.”
- TuhinBorgohain, Uday Kumar and SugataSanyal “Survey of Security and Privacy Issues of Internet of Things”
- Krushang Sonar, HardikUpadhyay  “A Survey: DDOS Attack on Internet of Things“International Journal of Engineering Research and Development

**Harivansh Sharma** is finishing the second year at Amity university at Noida, where he is interested in programming and business. Although he has yet to declare a major, he is considering artificial intelligence or machine learning. His interest in programming began during high school in 2017 when he was introduced to programming in C++.

@harivansh20 harivansh.021@gmail.com

## Annexure I

| Submission Date | Submission Id | Word Count | Character Count |
|---|---|---|---|
| 12-Dec-2019 | D62601499 (Urkund) | 2505 | 16579 |



Urkund Analysis Result

| | |
|---|---|
| Analysed Document: | Internet of Things.docx (D62601499) |
| Submitted: | 12/12/2019 12:23:00 PM |
| Submitted By: | ${Xml.Encode(Model.Document.Submitter.Email)} |
| Significance: | 13 % |

Sources included in the report:

Review of security Aspects in the Internet of Things.pdf (D54607163)
vlsi.docx (D39261488)
https://www.researchgate.net/publication/301749225_Classification_of_Security_Risks_in_the_IoT_Environment
https://www.ijcsmc.com/docs/papers/January2016/V5I201636.pdf
https://arxiv.org/pdf/1501.02211
https://www.ijecs.in/index.php/ijecs/article/download/3450/3208/

Instances where selected sources appear: 9

*Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.*

## Reviewers Comment

**Review 1:** This Article contains an unusual quantity of items IoT, Security protocol, and some important facts, points, which is important in current era.

**Review 2:** In my opinion, IoT makes once “dumb” devices “smarter” by giving them the capability to send data over the internet, letting the device to interconnect with people and other IoT-enabled things.

**Review 3:** In current scenario the IoT, this collective allows devices to attach and talk to each other and also to us, transfer reams of data and in-depth analysis that will expectantly increase the creation about us.

## Editorial Excerpt

The article has 13% of plagiarism which is an accepted percentage for publication. After plagiarism check, this article is gone through the review. The finding related to “Security issues with the four-layer architecture of IoT model” are noteworthy. The IoT is increasing fast, and is set to move into more and more areas in the years to come, resulting in a smarter world that previously was only imaginable in science fiction. The internet of things is also a natural extension of SCADA (supervisory control and data acquisition), a category of software application program for process control, the gathering of data in real time from remote locations to control equipment and conditions. Hence it is decided to earmarked under “**Experiential Research Papers** (ERP)’ category.

## Acknowledgement

I am highly indebted & thankful to our mentor and teacher Ms. Rajbala Simon for encouraging me to write an article entitled “Security issues with the four-layer architecture of IoT model” for the magazine Cybernomics.

## Disclaimer

All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section..

## Citation

Harivansh Sharma
“Security issues with the four-layer architecture of IoT model”
Volume-1, Issue-7, Dec 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
**Conflict of Interest**: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in