Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 665-669, Kasım 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 665-669, November 2021

Research Article

An in-depth exam of IoT, IoT Core Components, IoT Layers, and Attack Types

Muhammed Yıldırım[1*], Uğur Demiroğlu[2], Bilal Şenol[3]

[1*] Firat University, College of Engineering, Computer Engineering Department/ Elazığ, Turkey, (ORCID: 0000-0003-1866-4721) muhyldrm23@gmail.com
[2]Firat University, Technical Vocational School, Computer Sciences Department, Elazığ,Turkey (ORCID: 0000-0002-0000-8411) ugurdemiroglu@firat.edu.tr
[3]Inonu University, College of Engineering, Computer Engineering Department,Elazığ, Turkey(ORCID: 0000-0002-3734-8807) bilal.senol@inonu.edu.tr

(1st International Conference on Applied Engineering and Natural Sciences ICAENS 2021, November 1-3, 2021)

(**DOI:** 10.31590/ejosat.1010023)

ATIF/REFERENCE: Yıldırım, M., Demiroğlu, U. & Şenol, B. (2021). An in-depth exam of IoT, IoT Core Components, IoT Layers, and Attack Types. *European Journal of Science and Technology*, (28), 665-669.

Abstract

The Internet of Things (IoT) is a global network of devices that can communicate with each other through different communication protocols and have the ability to detect and process data. Since the Internet of Things connects electronic devices to the Internet for efficient examination and execution of daily activities, it has a seriously positive effect on human life. These devices use some communication protocols to communicate with each other. The selection of these communication protocols is of great importance. The data obtained from these smart devices are stored with the help of cloud technology. These stored data reveal the concept of big data. The processing and analysis of these data are of great importance. Machine learning methods are of great importance in processing this large amount of data. In this study, IoT, the basic components of the IoT, layer structure, security attacks are examined.

Keywords: Attack Type, IoT, IoT Components, IoT Layers

IoT, IoT Çekirdek Bileşenleri, IoT Katmanları ve Saldırı Türlerinin Derinlemesine İncelenmesi

Öz

Nesnelerin İnterneti (IoT), farklı iletişim protokolleri aracılığıyla birbirleriyle iletişim kurabilen ve verileri algılama ve işleme yeteneğine sahip küresel bir cihaz ağıdır. Nesnelerin İnterneti, günlük aktivitelerin verimli bir şekilde incelenmesi ve yürütülmesi için elektronik cihazları internete bağladığından, insan hayatı üzerinde ciddi anlamda olumlu bir etkiye sahiptir. Bu cihazlar birbirleriyle iletişim kurmak için bazı iletişim protokollerini kullanır. Bu iletişim protokollerinin seçimi büyük önem taşımaktadır. Bu akıllı cihazlardan elde edilen veriler bulut teknolojisi yardımıyla saklanmaktadır. Depolanan bu veriler, büyük veri kavramını ortaya çıkarmaktadır. Bu verilerin işlenmesi ve analizi büyük önem taşımaktadır. Bu büyük miktardaki verinin işlenmesinde makine öğrenmesi yöntemleri büyük önem taşımaktadır. Bu çalışmada IoT, IoT'un temel bileşenleri, katman yapısı, güvenlik saldırıları incelenmiştir.

Anahtar Kelimeler: Saldırı Türü, IoT, IoT Bileşenleri, IoT Katmanları

[*] Corresponding Author: muhyldrm23@gmail.com

1. Internet of Thinks

Different communication systems connect end-users as the internet communication infrastructure develops (Lin et al., 2017). Many sensor devices can now be incorporated into the internet environment using various communication protocols thanks to recent technological advancements (Luis Bustamante, Patricio, & Molina, 2019). Continuous and real-time data flow from sensor devices, patient and elderly monitoring, traffic management systems, security, transportation, smart cities, industry, agriculture, and energy, among other applications. It's been applied successfully in a variety of fields, including (Ozkaya et al., 2018).

It is self-evident that the Internet has a huge impact on our daily lives through enhancing communication, information sharing, and interpersonal connection. IoT is a concept that describes the intelligent linking of smart devices through items that can perceive and interact with one another (Citoni et al, 2019). In order for smart devices to communicate with each other, each must have an ID. In addition, these devices must have sensing capabilities to communicate with each other. The communication of smart devices with each other also has a great impact on human life (Abdel et al, 2019). In a short period of time, the IoT has added a new dimension to human capacities such as working, living, and learning. It is also clear that this technology will develop very quickly.

It is of great importance to store data obtained from smart devices located in different locations. If the data is not stored and processed, it does not make sense. With the internet of things, data obtained from smart devices brings the concept of cloud computing. Cloud computing technology is a model that allows access to a common pool of configurable computing resources, whenever and wherever (Yildirim, Çinar, & Cengil). With the developing technology, the use of this model is increasing day by day. With cloud technology, the size of the data kept in databases is also increasing. It is important to evaluate this increasing amount of data with machine learning methods and produce results that can be used for technical and commercial purposes (Eroğlu et al, 2021).

In this study, the Internet of Things in the first part, IoT basic components in the second part, IoT architectures and security threats in the third part, and finally, the fourth part is given conclusions.

2. IoT Core Components

There are multiple definitions for IoT. IoT can be defined as a network structure in which devices or machines transmit data among themselves, gather information, and make decisions based on that information, all without the need for human interaction or manual data entry. One of the basic components that make up the IoT structure is smart devices. The important thing in IoT is that these devices communicate with each other using certain communication protocols and store the obtained data. IoT consists of a large ecosystem. As shown in Figure 1 in the ecosystem of objects, the main components are devices, communication protocols, and cloud structures where the obtained data is stored (Borycki, 2017). Processing, storing, and analyzing the data kept in the cloud infrastructure is of great importance. Machine learning methods are frequently used to process this large amount of data (Çınar et al, 2021).

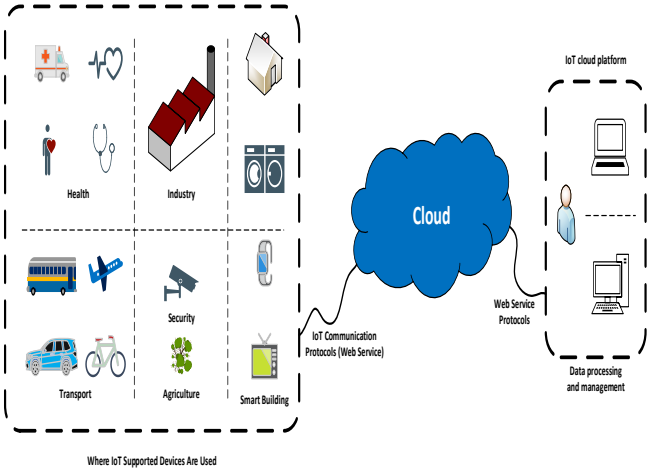

Figure 1. IoT Components

As seen in Figure 1, the first of the IoT components are the devices. The task of smart devices, the first of the basic components of IoT, is to collect data from the environment, interact with devices via wired or wireless network technologies, and enable communication over the internet. As can be seen in Figure 2, these devices are made up of three primary components.

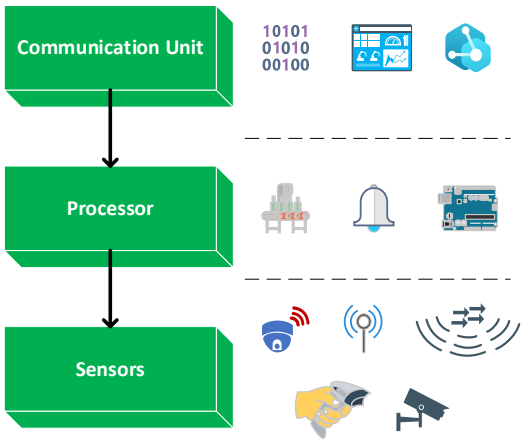

Figure 2. Main Components of Devices

In order for these devices to communicate and communicate over the internet, they must have their own private addresses. In addition, these devices must have a communication unit in order for these devices to collect data and communicate with each other. Another component that should be in these devices is the sensors. If these devices do not have sensors, it becomes impossible for the devices to communicate with each other. With the development of IoT, these smart devices have increased internet traffic the most (Das et al, 2018). At the same time, with the increase in internet traffic, the amount of data kept in databases has started to increase very rapidly. Since these data are connected from different places and in different ways, the concept of cloud technology is also developing rapidly. Another component that should be in IoT devices is the processor or embedded systems.

Another component of IoT is communication protocols. Communication protocols are of great importance in the IoT system (Moraes et al, 2019). Communication protocols are developed to enable communication of smart devices working over the network and are also defined as web services. In addition, how the devices will transfer the data to the cloud environment is

determined using these protocols. There are different communication layers developed on the subject. The most widely used communication protocols are CoAP, MQTT, AMQP, XMPP, DDS, and HTTP REST (Seleznev & Yakovlev, 2019). These communication layers are given in Figure 3.

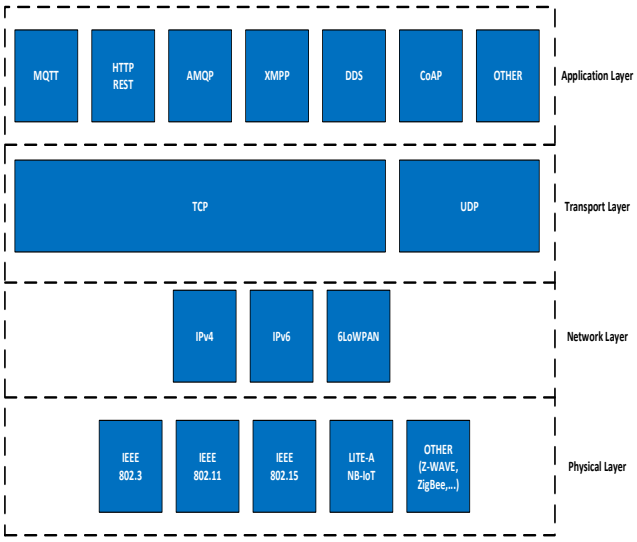

Figure 3. Communication Layers

The fact that the communication protocol to be selected is related to the subject and device is of great importance in data transport and communication of devices (Andy, Rahardjo, & Hanindhito, 2017). In addition, there are different criteria to be considered in the selection of these communication layers.

When Figure 1 is examined, cloud computing emerges as one of the basic components of IoT. Cloud computing technology is one of the basic components of IoT in this component. It provides the opportunity to access a common pool of configurable computing resources whenever and wherever. Therefore, it is important to process, store and analyze the data in the cloud structure.

3. IoT Layers and Attack Types

There is no single and generally accepted structure for IoT architecture (Rao & Haq, 2018). Some researchers argue that this structure should consist of 3 layers, some researchers 4, and some researchers argue that it should consist of 5 layers. IoT layer architecture is given in figure 4.

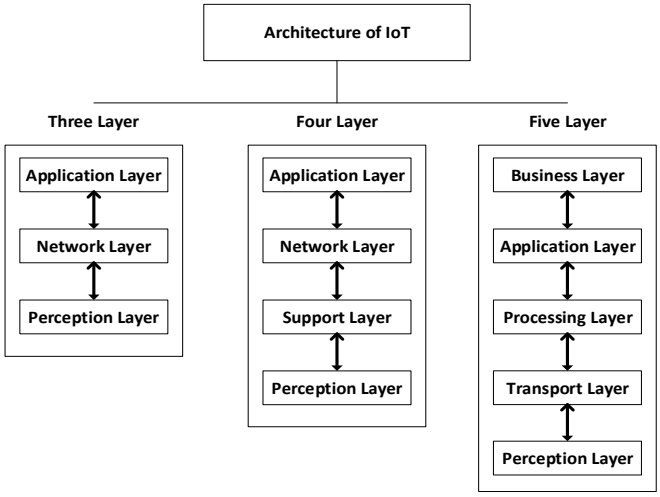

Figure 4. IoT Layer Architecture

Three-layer architecture emerged with the concept of IoT and is one of the first proposed architectures. This proposed 3-layer architecture consists of Perception, Network, and Application layers (Zhang et al., 2017). With the development of IoT technology, 4-layer architecture has been developed. There is an extra layer in this 4-layer architecture. This layer is the support layer. A 5-layer architecture is proposed to solve the security and storage problems of the 4-layer architecture. The layers used in these architectures are explained in order, and the attacks in each layer are examined in detail.

3.1. Perception Layer

The sensor layer, also known as the perception layer, functions similarly to people's eyes, hearing, and nose. The sensor layer's principal job is to recognize things and collect data from them. There are many different types of sensors that can be mounted to items to collect data. The application needs to choose the sensors. These sensors can capture temperature, humidity, heat, movement, vibration, and other data (Khattak, Shah, Khan, Ali, & Imran, 2019). However, attackers who wish to utilize the sensor for replacing it with their own are primarily interested in these. As a result, the sensors are the source of the majority of the threats. The common security threats of the perception layer can be grouped into five categories.

- Eavesdropping: Eavesdropping is a real-time attack in which an attacker intercepts private communications such as calls, texts, faxes, and video conferences. The main purpose here is to steal information sent over the network (Hoang et al, 2019).
- Fake Node and Malicious: This type of attack is an attack where the attacker enters fake data through a node added to the system. Here it is aimed to stop the transmission of real information. In addition, the node inserted by the attacker consumes and potentially controls the energy of the actual nodes to destroy the network (Ahmad et al, 2020).
- Node Capture: In this attack, the attacker controls a switch node, such as a gateway node. As a result, communication between the sender and recipient and any information stored in memory may be compromised.
- Timing Attack: This attack is usually carried out on smart devices with low computing capacity.
- Replay Attack: In this type of attack, the attacker receives information from the network between the

sender and the receiver. By demonstrating his authenticity and proving his identity, the attacker sends the same verified information that was previously received in his communication to the victim. Since the message sent by the attacker is encrypted, the receiver can evaluate it correctly (Rughoobur & Nagowah, 2017).

3.2. Network Layer

The perception layer and the application layer communicate through this layer. Network layer is to transmit the data gathered from physical objects using different communication technologies, wired or wireless. This layer is also vulnerable to attacks because it connects devices and other network components (Ceron et al, 2019). It is possible to examine the threats emerging in the network layers under 4 headings.

- Denial of Service (DoS) Attack: The purpose of this attack is to prohibit users from accessing devices or other network resources. Attackers send unnecessary requests to devices and network resources, making users harder to access.
- Main-in-The-Middle (MiTM) Attack: The attacker interrupts and modifies the communication between the sender and recipient in this form of attack. In this type of attack, the attacker can control the communication.
- Storage Attack: This type of attack is made to the place where the data is kept. Where the data is kept, the data can be modified by the attacker.
- Exploit Attack: In this type of attack, the attacker tries to infiltrate the system using security vulnerabilities. In this type of attack, the aim is to steal data (Andreica et al, 2020).

3.3.Application Layer

It is the layer that is responsible for the operation of all applications. This layer has to provide services to applications (Sun & Ansari, 2017). It is possible to collect common security threats emerging in this layer under 3 headings.

- Cross Site Scripting: It enables an attacker to script a trusted website that other users visit. Here, the attacker can modify the information and damage the system.
- Malicious Code Attack: It is a system-damaging code located anywhere in the software. This code can run itself and damage the system.
- The ability of dealing with Mass Data: It's a form of attack that causes data loss and network disruption.

3.4.Support Layer

The fourth layer is primarily required for security reasons. Because information is transferred directly to the network layer in a three-tier architecture, the network will be exposed to additional risks. The support layer is a layer that runs between the Network and Perception layers. This layer checks if the information comes from real users. This layer is also responsible for transmitting information to the network layer (Ashouri et al, 2018). Transmission at this layer can be wired or wireless. In this layer, it is possible to give the most common threats under 2 headings.

- DoS Attack: The DoS attack in this layer is basically a Network layer attack. The attacker sends a large volume of data to lock down the network traffic. IoT users are unable to access the system as a result of this.
- Malicious Insider Attack: An authorized user from an IoT environment launches a sophisticated assault to gain access to users' personal information.

Business Layer, Processing Layer, and Transport Layer layers are used in the 5-layer architecture, unlike the 3- and 4-layer architecture.

3.5.Processing Layer

In a five-layer architecture, this layer is used to eliminate useless information from the Transport layer. This reduces the burden of working with big data for IoT objects (Nasiri et al, 2019). Unfortunately, there are a variety of attacks that can damage this layer and the performance of IoT devices.

- Exhaustion: These attacks aim to consume IoT objects' battery, energy, and memory over time.

Malware: The purpose of this attack type is to access user information. Here, viruses, adware, spyware are some of the tools used in these attacks.

3.6.Transport Layer

The Transport layer is a layer between the Processing and Perception layers. This layer carries out the communication task between the Processing and Perception layers.

3.7.Business Layer

The Business Layer is a layer that acts as the administrator of the entire system, especially the users' privacy. Most of the security problems that occur in this layer are caused by the previous layer (Navan et al, 2017). We can classify the two most common attacks in the Business layer as Business Logic Attack and Zero-Day Attack.

- Business Logic Attack: This attack, which takes advantage of the deficiencies in the software, controls the information exchange. The most common programming errors are password recovery and login verification.

Zero-Day Attack: This type of attack is caused by security vulnerabilities in an application that the user is not used to. The attacker's goal is to gain control.

4. Conclusion

IoT is a rapidly advancing field with developing technology. It is obvious that this area will positively affect human life. IoT is a global network that refers to the communication of devices with each other using different communication protocols. In this study, we examined the IoT core components and explained where and how these components are used. We also examined the IoT layers and the types of attacks on these layers. We also discussed various challenges associated with IoT technology. As a result, we aimed to present a general perspective on this field with our study.

References

Abdel-Basset, M., Manogaran, G., Mohamed, M., & Rushdy, E. (2019). Internet of things in smart education environment: Supportive framework in the decision-making process. *Concurrency and Computation: Practice and Experience, 31*(10), e4515.

Ahmad, A., Hababeh, M., Abu-Hantash, A., AbuHour, Y., & Musleh, H. (2020). Reduce Effect of Dependent Malicious Sensor Nodes in WSNs using Pairs Counting and Fake Packets. *International Journal of Computers, Communications and Control, 15*(5).

Andreica, G. R., Bozga, L., Zinca, D., & Dobrota, V. (2020). *Denial of service and man-in-the-middle attacks against IoT devices in a GPS-based monitoring software for intelligent transportation systems.* Paper presented at the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet).

Andy, S., Rahardjo, B., & Hanindhito, B. (2017). *Attack scenarios and security analysis of MQTT communication protocol in IoT system.* Paper presented at the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI).

Ashouri, M., Davidsson, P., & Spalazzese, R. (2018). *Cloud, edge, or both? Towards decision support for designing IoT applications.* Paper presented at the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security.

Borycki, D. (2017). *Programming for the Internet of Things: Using Windows 10 IoT Core and Azure IoT Suite*: Microsoft Press.

Ceron, J. M., Steding-Jessen, K., Hoepers, C., Granville, L. Z., & Margi, C. B. (2019). Improving iot botnet investigation using an adaptive network layer. *Sensors, 19*(3), 727.

Citoni, B., Fioranelli, F., Imran, M. A., & Abbasi, Q. H. (2019). Internet of Things and LoRaWAN-enabled future smart farming. *IEEE Internet of Things Magazine, 2*(4), 14-19.

Çınar, A., Yıldırım, M., & Eroğlu, Y. (2021). Classification of pneumonia cell images using improved ResNet50 model. *Traitement du Signal, 38*(1), 165-173.

Das, A., Dash, P., & Mishra, B. K. (2018). An innovation model for smart traffic management system using internet of things (IoT) *Cognitive Computing for Big Data Systems Over IoT* (pp. 355-370): Springer.

Eroğlu, Y., Yildirim, M., & Çinar, A. (2021). Convolutional Neural Networks based classification of breast ultrasonography images by hybrid method with respect to benign, malignant, and normal using mRMR. *Computers in biology and medicine, 133*, 104407. doi: https://doi.org/10.1016/j.compbiomed.2021.104407

Hoang, T. M., Nguyen, N. M., & Duong, T. Q. (2019). Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering. *IEEE Wireless Communications Letters, 9*(2), 139-142.

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems, 100*, 144-164.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE internet of things journal, 4*(5), 1125-1142.

Luis Bustamante, A., Patricio, M. A., & Molina, J. M. (2019). Thinger. io: An open source platform for deploying data fusion applications in IoT environments. *Sensors, 19*(5), 1044.

Moraes, T., Nogueira, B., Lira, V., & Tavares, E. (2019). *Performance Comparison of IoT Communication Protocols.* Paper presented at the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC).

Nasiri, H., Nasehi, S., & Goudarzi, M. (2019). Evaluation of distributed stream processing frameworks for IoT applications in Smart Cities. *Journal of Big Data, 6*(1), 1-24.

Navani, D., Jain, S., & Nehra, M. S. (2017). *The internet of things (IoT): A study of architectural elements.* Paper presented at the 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS).

Ozkaya, U., Öztürk, Ş., Tuna, K., Seyfi, L., & Akdemir, B. (2018, April). Faults Detection With Image Processing Methods In Textile Sector. In 1st International Symposium on Innovative Approaches in Scientific Studies.

Rao, T. A., & Haq, E. (2018). Security challenges facing IoT layers and its protective measures. *International Journal of Computer Applications, 179*(27), 31-35.

Rughoobur, P., & Nagowah, L. (2017). *A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare.* Paper presented at the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS).

Seleznev, S., & Yakovlev, V. (2019). Industrial Application Architecture IoT and protocols AMQP, MQTT, JMS, REST, CoAP, XMPP, DDS. *International Journal of Open Information Technologies, 7*(5), 17-28.

Sun, X., & Ansari, N. (2017). Dynamic resource caching in the IoT application layer for smart cities. *IEEE internet of things journal, 5*(2), 606-613.

Yıldırım, M., Çınar, A., & Cengil, E. Investigation of Cloud Computing Based Big Data on Machine Learning Algorithms. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi, 10*(2), 670-682.

Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., & Sun, J. (2017). A new digital watermarking method for data integrity protection in the perception layer of IoT. *Security and Communication Networks, 2017*.