IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10704

Privacy and Security in Internet of Things (IoT): Threats, Challenges, and Solutions

Nedhal A. Ben-Eid

Computer Department, The Higher Institute for Telecomm. and Navigation, Public Authority for Applied Education and Training (PAAET), Shuwaikh, Kuwait

Abstract: The Internet of Things technology played a vital role in our daily lives. It allows billions of devices and people to communicate, share data, and personalize services to enhance the living style. This wireless communication devices are distributed everywhere at smart homes, smart cities, smart transportations, as well as in military, business, and healthcare fields. Due to the rapid increase of IoT devices all around the world, it became a target for many hackers to trespass the privacy of people by collecting sensitive information and use it in suspicious tasks. Moreover, many of intruders have harmful intentions to destroy systems and infrastructures of some organizations. The deployment of efficient security and privacy protocols in IoT networks is extremely needed to ensure confidentiality, authentication, access control, and integrity, among others [5]. In this paper, the Internet of Things topic is introduced, its architectures and characteristics are clarified, the security threats and challenges are highlighted, and some essential solutions are explained.

Keywords: Internet of Things (IoT), Security, Privacy, Authentication, Access Control, Cyberattack, Fog Computing, Cloud Computing, Blockchain.

I. INTRODUCTION

The Internet of Things (IoT) has a great attention during the last decade. It was first coined by Kevin Ashton in 1999, but this technology took several years later to be matured. Many definitions are generated by experts and researchers to describe this technology, but we can simply define “Internet of Things” as a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. The IoT devices have embedded systems and have the ability to be connected to the Internet, it can collect data from the surroundings using sensors and process this data to take discussions and actions.

Since IoT devices are user friendly, easy to be managed, and cost effective; many homes, offices, manufactures, and organizations had been adopted this technology. There are many types of IoT applications, like smart watches, smart mobiles, security cameras, medical sensors, smart factory equipment, air quality sensors, smart cars, and much more. Many companies and manufacturers are competing to produce smarter devices that can collect, process, manipulate, and store data with minimal latency, high level of QoS, and minimum operational cost, to help in making the life easier and better [13].

The IoT technology is taking advantage of the growing adoption of Cloud Computing, it fuelled the development of IoT since it support it with great storage and powerful infrastructure, the developing of on-site IoT infrastructure that can process and store big data can be very expensive, keeping the IoT data in the cloud will reduce the cost as well as increase the security level.

The number of connected devices is increasing rapidly in the global, according to CISCO Annual Internet Report (2018-2021), we can highlight a comparison between the growth of Internet Adoption, devices, and connection in 2018 and the estimated numbers by 2023. Table 1 summarizes this comparison.

TABLE I GLOBAL INTERNET ADOPTION AND DEVICES AND CONNECTION

Category	**Internet Users**	
	2018	**2023**
Internet Users	3.9 billion	5.3 billion
Percentage of Internet Users	51 % of global population	66 % of global population
Total Number of Connected Devices	18.4 billion	29.3 billion
Number of Connected Devices per Person	2.4/capita	3.6/capita
Machine-to Machine (M2M)	33 %	50 % (14.7 billion)
Global Mobile Subscriber	5.1 billion	5.7 billion
Percentage of Global Mobile Subscriber	66 % of global population	71 % of global population
5 G Devices and Connection	8.8 billion	13.1 billion

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10704

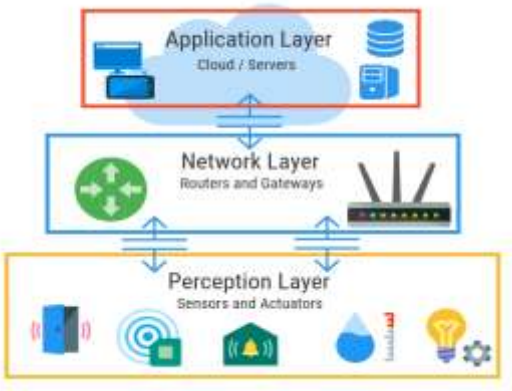
The recent rapid development of the Internet of Things (IoT) and its ability to offer different types of services have made it the fastest growing technology, with huge impact on social life and business environments [7].

II. THE ARCHITECTURE OF INTERNET OF THINGS (IOT)

There are many IoT architectures proposed by experts, but no single architecture is adopted by consensus. Some IoT architecture uses three layers, four, five, six, or even seven. We will introduce the most basic one which is the three-layer architecture, and the five-layer architecture since it is used mostly.

A. The Three-Layer IoT Architecture:

This architecture summarizes the IoT system in three steps: Perception, Network, and Application. Figure 1 illustrates the three-layer architecture and the involved devices.



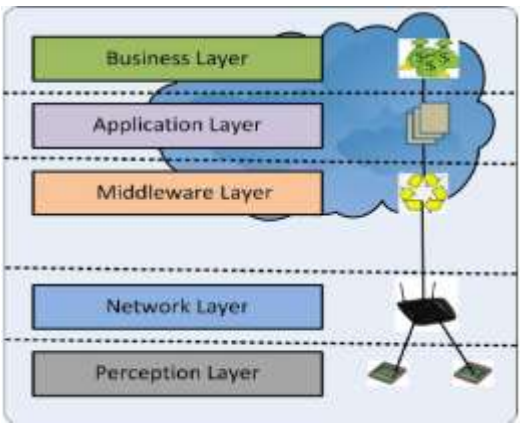
Source: waziup.io

Fig. 1 Basic Three-Layer IoT Architecture

- **Perception Layer**: Which involves the sensors and actuators. The sensors sniff the physical environment around the device and gather data, while the actuators perform specific actions on the sensed data. Sensors are different kinds, like camera sensors, weather sensors, pollution sensors, etc. There can be mechanical, electrical, electronic, or chemical sensors used to sense the physical environment. Various sensing layer technologies are used in different IoT applications like RFID, GPS, WSNs, RSNs, etc [6].
- **Network Layer**: It is responsible for transmitting the sensed and processed data from the perception layer to send it to the core network servers.
- **Application Layer**: It is responsible for delivering services to the users to interact. When application layer receives the processed data from network layer, it will manipulate and store the data in the cloud (data centers) and provide users with various services and applications.

B. The Five- Layer IOT Architecture:

The development of new and high-tech IoT devices imposes more specialized architecture to support the smart tasks. The five-layer IoT architectures are used by many experts and researchers. Some of them uses different Layer's names, but at least using the same concept and sequence. Figure 2 illustrates the five-layer architecture.



Source: researchgate.net

Fig. 2 Five-Layer IoT Architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10704

- **Sensing (Perception) Layer**: The IoT sensors and actuators gather data from the surroundings (like temperature, sound, video, etc) to take actions according to this useful information. The collected data are then transferred to the next layer.
- **Network (Communication) Layer**: This layer is responsible for the communication between the sensing layer and middleware layer, it gets the data and uses the networking technologies (like 3G,4G, 5G, etc), then some security and privacy routines are applied.
- **Middleware Layer**: In this layer, data is processed and stored. Moreover, some tasks are done on the sensed data based on some calculations.
- **Application Layer**: The process is managed by this layer, and the application (IoT device) is controlled by turning it On/Off, activate some tasks, and so on.
- **Business Layer**: This layer is responsible for analyzing the results to improve the performance and quality of service to reach the customer satisfactions.

III. THE CHARACTERISTICS OF INTERNET OF THIGS (IOT)

Some most popular characteristics of Internet of things are [7]:

A. Intelligence:

The IoT devices are equipped with high technology hardware and software that have the capability to act smartly and interactively with the surrounding environment using effective algorithm. It can collect data from the physical location, decide the appropriate actions, and then do specific tasks. The growing attention of IoT devices at home appliances comes from the fact that IoT devices are user friendly with graphical user interface that makes it easy for people with basic knowledge to interact with these devices.

B. Connectivity:

Connectivity is an important feature, the IoT devices should be connected to the network anytime and anywhere. Without connectivity, IoT devices will be standalone devices, and cannot interact or share resources.

C. Dynamic Nature

The IoT devices collect the data from the physical location. The dynamic changes that happen in the IoT environment and surroundings will change the state of the devices (like on/off, hot/cold, … etc).

D. Sensing

Sensing technology is collecting the raw input data from the physical world by specialized devices called “sensors” and then input this data into the IoT device that can translate it into a meaningful information. By using the sensors, a true understanding of the complex world is translated to the devices to analyze it and generate suitable actions.

E. Heterogeneity

IoT devices come from different hardware and service platform, they can interact effectively and cooperate in a harmonic manner. Manufacturer design and produce IoT devices to be scalable, extensible, and compatible with each other.

F. Security

Although the IoT has many benefits and changed our lifestyles to be easier and managed effectively, it is prone to multiple types of threats and challenges. It is essential to secure the edge points as well as the core network.

IV. IOT SECURITY THREATS

Although the Internet of Things (IoT) technology has changed our living style positively, we must be attention that it is prone to various types of security threats due to many reasons:

- Lack of standardization and regulation around IoT security [18].
- Lack of hardware capacity needed to support robust cybersecurity application (unlike smartphones) [18].
- The IoT device is dealing with sensitive and private information which makes it a target for many intruders.
- Since IoT devices are considered high-value targets for attackers; professional and sophisticated cybercrimes are used that leads to costly and harmful consequences.

Some threats lead to shortage of resources, service, or even trespass the privacy of people or organizations, and some threats do malicious and suspicious tasks. We can categorize the security threats (attacks) according to the level of severity:

- Low- Severity Attack: When the intruder tries to trespass the IoT system, but his attempt is not succeeded.
- Medium-Severity Attack: When the intruder breaks into the medium as an eavesdropper to monitor or listen only without altering data integrity.
- High-Severity Attack: When the attacker breaks into the network to alter the data integrity and change it.
- Very High-Severity Attack: When the attacker breaks into the network as an unauthorized user to modify the system in order to interrupt or destroy the system or part of it, causing jamming, unavailable connection, or malfunction.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10704

As discussed in Three-Layer Architecture, any IoT infrastructure can be divided into three layers: Perception, Network, and Application. Each layer could suffer from multiple security threats. Various possible threats are discussed for each layer of the IoT system:

A. Security Threats in the Perception Layer [6]:

- Adding/ Replacing Malicious Nodes: The attacker may add or replace IoT device by a malicious node. It will appear as part of the system to perform harmful or suspicious tasks.
- Harmful Code Attack: The attacker forces a node to perform malicious tasks by using a code that is injected in the memory of the IoT device. The attacker will have the ability to access the IoT system. The code could be erroneous data that will cause malfunctioning.
- Boot Process Attack: During the boot process in the IoT device, the attacker can take the advantage of the lack of security, since the security routines are not yet performed. Securing the boot process is essential.
- Draining the battery: The attacker may use malicious code that runs infinite loops to increase the power consumption of the IoT device and lead to drain in the battery.

B. Security Threats in the Network Layer:

- Phishing: The network layer is highly vulnerable to phishing. The attacker may send malicious e-mail to the user, or even while the user visiting a suspicious website, a cyberattack could happen.
- Unauthorized Access: An unauthorized person can access the IoT network to gather sensitive and valuable information.
- DDoS/DoS Attack: The attacker here floods the server with unwanted requests to disturb its function.
- Routing Attack: A malicious node is added in the IoT system to redirect the routing traffic during the data movements.
- Person-in- the- Middle: A cyberattack where the attacker alters the communication between two nodes without being detected. He inserts himself in the middle, interrupts information, and sends malicious links.
- SQL Injection Attack: In such attacks, attacker can embed malicious SQL statements in a program. Then, the attackers can obtain private data of any user and can even alter records in the database [6].
- Signature Wrapping Attack: In a signature wrapping attack, the attacker breaks the signature algorithm and can execute operations or modify eavesdropped message by exploiting vulnerabilities in SOAP (Simple Object Access Protocol) [6].
- Cloud Malware Injection: In this type of attack, the attacker inserts a malicious code into the cloud to create a remotely controlled machine that can access the services requested by the legitimate users. By this way, the attacker can monitor and get all the private and sensitive user's information.
- Flooding the Cloud: This attack works the same as DoS attack, many requested services are sent by the attacker to over flood the cloud which will interrupt the server.

C. Security Threats in the Application Layer:

- Data Thefts: Data in IoT network always moving due to the nature of user's applications, this movements will make the data vulnerable to cyberattack by data stealing. This kind of attack could happen in any pace of the network layer as well.
- Access Control Attack: If the system is not defending itself by a powerful authorization mechanism, then it will be vulnerable to an unauthorized person that can access the system and do malicious or harmful attacks.
- Denial of Service (DoS) Attack: This kind of attack works by flooding the machine with traffic to make it inaccessible by legitimate users.
- Code Injection Attack: This attack is done by injecting a malicious script into the application to interrupt it or change the way it is functioning.
- Sniffing Attack: The attacker can use any sniffing application to monitor the network traffic going out or in the IoT node.
- Reprogramming Attack: This kind of attack is done by reprogramming the IoT node remotely, causing a hijacked IoT system.

V. SECURITY AND PRIVACY IN (IOT)

security is the biggest challenge in IoT, securing the data, devices, and network with an efficient security mechanism is very necessary to overcome any threats and attacks. The security mechanisms must be embedded at every layer of IoT architecture. Many devices like computers, smartphones, and tablets have built-in security features to face any security or privacy threats, but this is not available in the IoT devices in the market today. Designing and deploying smart devices that are capable to handle security threats is highly priority in the future of IoT to ensure authentication, confidentiality, integrity, and access control.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

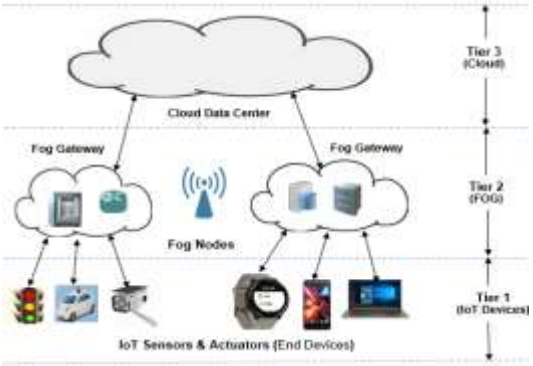
DOI 10.17148/IJARCCE.2021.10704

At the user end, many simple actions may be helpful to secure the IoT system, like:

- Changing the device default password.
- Setting a strong password and changing it regularly.
- Applying multi-factor authentication.
- Updating firmware and keep software up-to-date.
- Disabling any unused device feature.
- Reading security and privacy policies carefully and never neglect any suspicious messages or unusual activity.

IoT Security Using Fog Computing:

Due to the rapid increase in IoT devices nowadays, the cloud was facing many challenges and troubles due to the heavy load processing and storage. A new novel technology was introduced to extend and support cloud computing to reach the optimal performance in the network. This technology is called "Fog Computing", it is acting by pushing the computing and services to the ground near the IoT devices, allowing IoT data to be processed locally rather than in the cloud to decrease latency and network congestion. The main function of fog computing is to handle the data generated by IoT devices to be processed, manipulated, and filtered; only the necessary data is transferred to the cloud. Fog computing architecture consists of three tiers: IoT devices, the Fog, and the Cloud. The basic Three Tier Fog Architecture is shown in Figure 3.



Source: researchgate.net

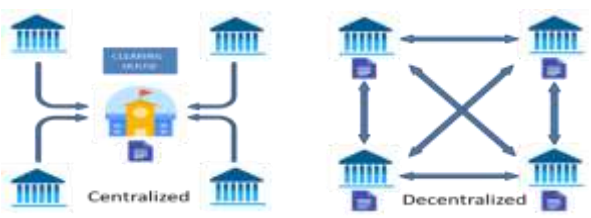
Fig. 3 Fog Computing Architecture

Fog computing infrastructure acts as an intermediate layer between IoT devices and the cloud servers; it can identify any threats or suspicious data generated by IoT devices. Fog layer is considered as security layer; multiple security and authentication mechanisms are applied to provide safe environment for the data processing and storage. Since the transit of data is reduced, the chance to be attacked is also reduced. The IoT nodes are resource constrained which make them easy target for attackers/intruders to enter the network and use their malicious and suspicious task, the fog will act as a proxy to secure and monitor nearby nodes.

IoT Security Using Blockchain:

Blockchain is one of the most effective technology to increase the security level in IoT network. Many companies adopted this novel technology to create a secure environment for their network. Blockchain is a shared immutable ledger that facilitates the process of recording transactions and tracking assets in a business network [21]. It is used to store the IoT data and release it for limited period of time to make transactions. Lightweight blockchain solutions have been introduced by many researchers for permitting the privacy in the IoT data [11].

This distributed ledger is used by the nodes in the network, if a transaction is requested, then a block is created and broadcasted to all nodes in the network. The nodes will legitimize the block that will be added to the chain. After that the transaction will be confirmed and executed. The blockchain technology will improve scalability, security, and privacy by using data decentralization and end-to-end encryption techniques. Figure 4 explains centralized versus decentralized ledger system.



Source: researchworld.com

Fig. 4 Centralized versus Decentralized Ledger Systems

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10704

VI. CONCLUSION

The Internet of Things (IoT) has been an extremely active topic in research and manufacturing fields, designing and implementing intelligent devices that enhance people's lives to have more comfort is a big challenge. Due to the tremendous growth in deploying IoT devices and the lack of security in these devices, IoT network became soft target for intruders and hackers. It is very essential to install a powerful security mechanism in the IoT network and apply it to the system, the application, as well as the communication network. Every single element in the IoT infrastructure must be secured properly.

The major aim of this paper was to understand the nature and characteristics of IoT network, highlighting the main security threats and challenges, and presenting Fog computing and Blockchain as two of the main solutions used to enhance the security of IoT network.

The Internet of Things (IoT) has been an extremely active area of research and development for more than two decades. Although a wealth of exciting activities including standardization, commercial developments and research have been conducted, many challenges still remain open due to the large scale and diversity of IoT devices, the openness of the IoT environment, and the security and privacy concerns [24].

The expected future of IoT is to be more socialized, smart devices will not only communicate with the users and take actions, but it will communicate with other devices directly according to smart decisions. The interaction between things and the Internet is known as Social Internet of Things SIoT, which is a hot topic in this field.

REFERENCES

[1] Yang Yang, Jianwei Huang, Tao Zhang, Joe Weinman, Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics, 1 st ed, John Wiley& Sons, 2020, USA
[2] K.G. Srinivasa, Pankaj Lathar, G. M. Siddesh, The Rise of Fog Computing in the Digital Era, IGI Global, 2019, USA
[3] C. S. R. Prabhu, Fog Computing and Internet-of-Things, BSP BS Pvt. Ltd., 2018
[4] William Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud, Indianapolis, Pearson Education:2016, Indiana, USA
[5] Mirza Abdul Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, 2017
[6] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures", in *IEEE Access*, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[7] Mohit Kumar Saini, Rakesh Kumar Saini, "Internet of Things (IoT) Applications and Security Challenges: A Review", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181 Published by, www.ijert.org NCRIETS – 2019 Conference Proceedings, Special Issue – 2019
[8] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, Muhannad Quwaider, "IoT Privacy and Security: Challenges and Solutions", Applied Sciences, 2020, 10, 4102. https://doi.org/10.3390/app10124102
[9] S. Balamurugan, A. Ayyasamy, K. Suresh Joseph, "A Review on Privacy and Security Challenges in the Internet of Things (IoT) to protect the Device and Communication Networks", International Journal of Computer Science and Information Security (IJCSIS), vol. 16, No. 6, June 2018
[10] A. Mallikarjuna Reddy, K. Srinivas Reddy, M. Prasad, A. Obulesh, "Internet of Things (IOT) Security Threats and Countermeasures", International Journal of Advanced Research in Engineering and Technology (IJARET), vol 11, Issue 8, August 2020, pp. 139-150
[11] Vikash Kumar Aggarwal, Nikhil Sharma, Ila Kaushik, Bharat Bhushan, Himanshu, "Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction", et al 2021 IOP Conf. Ser.: Mater. Sci. Eng. 1022 012103
[12] The CISCO Web Site [Online]: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
[13] Fog Computing and the Internet of Things: A Review - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Layered-architecture-of-fog-computing_fig2_324280213
[14] The Waziup Website [online]: https://www.waziup.io/courses/iotfundamentals/
[15] Smart gateway based communication for cloud of things - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Internet-of-Things-layers_fig1_269303095
[16] Podder, Prajoy & Mondal, M. Rubaiyat & Bharati, Subrato & Paul, Pinto. (2020). Review on the Security Threats of Internet of Things. International Journal of Computer Applications. 176. 37-45. 10.5120/ijca2020920548.
[17] Bhawna Ahlawat, Anil Sangwan, Vikas Sindhu, "IOT System Model, Challenges and Threats", International Journal of Science & Technology Research (IJSTR), vol. 9, Issue 03, p. 6771-6776, Mar. 2020
[18] The Security Boulevard Website [online]: https://securityboulevard.com/
[19] Nedhal A. Ben-Eid, "The Fog Computing: Characteristics and Future Directions", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)", vol. 10, Issue 6, Jun 2021, pp. 58-62
[20] An Analysis of Fog Computing Data Placement Algorithms - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Fog-Cloud-computing-architecture_fig1_337706300
[21] The IBM Website [online]: http://www.ibm.com
[22] Umer Iqbal Wani, Ranbir Singh Batth, Mamoon Rashid, "Fog Computing Challenges and Future Directions: A Mirror Review", International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dec. 11-12, 2019, Amity University, Dubai, UAE
[23] M. Mukherjee et al., "Security and Privacy in Fog Computing: Challenges," in IEEE Access, vol. 5, pp. 19293-19304, 2017, doi: 10.1109/ACCESS.2017.2749422
[24] Zhang, Wei Emma & Sheng, Quan & Mahmood, Adnan & Tran, Dai & Zaib, Munazza & Hamad, Salma & Aljubairy, Abdulwahab & Alhazmi, Ahoud & Sagar, Subhash & Ma, Congbo, (2020), "The 10 Research Topics in the Internet of Things", 34-43. 10.1109/CIC50333.2020.00015