4th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November 20-21, 2019 - Iran University of Science & Technology

Classification of Attacks on IoT

Hamidreza Damghani [1], Leila Damghani [2], Heliasadat Hosseinian [3], Reza Sharifi [4]

[1] Faculty of Mechanics, Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

hamidreza.damghani@gmail.com

[2] Faculty of Computer Engineering- Artificial intelligence, Kharazmi University, Tehran, Iran.

Damghani.iau@gmail.com

[3] Faculty of Mechanics, Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran.

helia.hosseinian@aut.ac.ir

[4] West Tehran Branch, Islamic Azad University, Islamic Azad University, Tehran, Iran.

Sharifi@ee.iust.ac.ir

ABSTRACT

Security is the biggest concern in adopting Internet of things technology. In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. The current IoT space comes with numerous security vulnerabilities. These vulnerabilities include weak authentication (IoT devices are being used with default credentials), unencrypted messages sent between devices, SQL injections and lack of verification or encryption of software updates. This allows attackers to easily intercept data to collect PII (Personally Identifiable Information), user credentials can be stolen at login or malware can be injected into newly updated firmware. There are so many attacks on IoT have been invented before actual commercial implementation of it. The present study discusses various IoT attacks happening, classify them, its countermeasures and finding the most prominent attacks in IoT. In fact, ensuring the security of data exchange is among the great challenges of the Internet of things. The present study discusses various IoT attacks happening, classify them, its countermeasures and finding the most prominent attacks in IoT.

KEYWORDS: Internet of Things (IoT); Attacks; Physical Attacks; Network Attacks; Software Attacks; Encryption Attacks; Privacy; Security.

1 INTRODUCTION

The Internet of Things (IoT) has attracted strong interest from both academia and industry. The IoT integrates radiofrequency identification (RFID), sensors, smart devices, the Internet, smart grids, cloud computing, vehicle networks, and many other information carriers. However, interconnecting many "things" also means the possibility of interconnecting many different threats and attacks. For example, a malware virus can easily propagate through the IoT at an unprecedented rate. In the four design aspects of the IoT system, there may be various threats and attacks [1]: (1) Data perception and collection: In this aspect, typical attacks include data leakage, sovereignty, breach, and authentication. (2) Data storage: The following attacks may occur: denial-of-service attacks (attacks on availability), access control attacks, integrity attacks, impersonation, modification of sensitive data, and so on. (3) Data processing: In this aspect, there may exist computational attacks that aim to generate wrong data processing results. (4) Data transmission: Possible attacks include channel attacks, session hijacks, routing attacks, flooding, and so on [2]. Apart from attenuation, theft, loss, breach, and disaster, data can also be fabricated and modified by the compromised sensors. The IoT also views everything as the same, not even discriminating between humans and machines. Things include end users, data centers (DCs), processing units, smartphones, tablets, Bluetooth, ZigBee, the Infrared Data Association (IrDA), ultra-wideband (UWB), cellular networks, Wi-Fi networks, near field communication (NFC) DCs, RFID and their tags, sensors and chips, household equipment, wristwatches, vehicles, and house doors; in other words, IoT combines "factual and virtual" anywhere and anytime, attracting the attention of both "maker and hacker." Inevitably, leaving devices without human intervention for a long period could lead to theft. IoT incorporates many such things [3]. Protection was a major issue when just two devices were coupled. Protection for the IoT would be unimaginably complex.

2 PHASES OF IOT SYSTEM

The IoT requires five phases, from data collection to data delivery to the end users on or off demand, as shown in Figure 1.

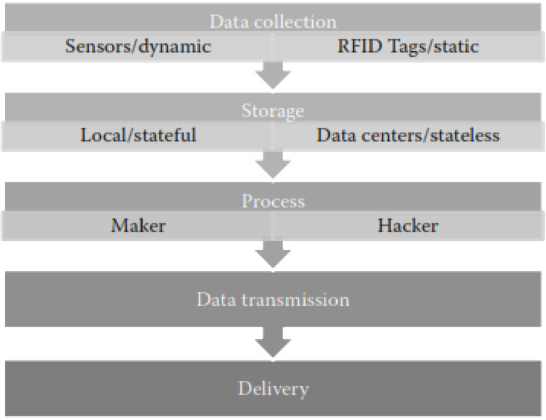

Figure. 1. Phases of IoT system.

2.1 *Phase I: Data collection, acquisition, perception*

Be it a telemedicine application or vehicle tracking system, the foremost step is to collect or acquire data from the devices or things [4]. Based on the characteristics of the thing, different types of data collectors are used [5]. The thing may be a static body (body sensors or RFID tags) or a dynamic vehicle (sensors and chips).

2.2 *Phase II: Storage*

The data collected in phase I should be stored. If the thing has its own local memory, data can be stored. Generally, IoT components are installed with low memory and low processing capabilities. The cloud takes over the responsibility for storing the data in the case of stateless devices.

2.3 Phase III: Intelligent processing

The IoT analyzes the data stored in the cloud DCs and provides intelligent services for work and life in hard real time. As well as analyzing and responding to queries, the IoT also controls things. There is no discrimination between a boot and a bot; the IoT offers intelligent processing and control services to all things equally [6].

2.4 Phase IV: Data transmission

Data transmission occurs in all phases:

- From sensors, RFID tags, or chips to DCs
- From DCs to processing units
- From processors to controllers, devices, or end users

2.5 Phase V: Delivery

Delivery of processed data to things on time without errors or alteration is a sensitive task that must always be carried out [7].

3 Internet of Things as Interconnections of Threats

Privacy and security will be the major factors of concern at that time. The IoT can be viewed in different dimensions by the different sections of academia and industry; whatever the viewpoint, the IoT has not yet reached maturity and is vulnerable to all sorts of threats and attacks. The prevention or recovery systems used in the traditional network and the Internet cannot be used in the IoT due to its connectivity [8].

2.5.1 Phase attacks

Data leakage, sovereignty, breach, and authentication are the major concerns in the data perception phase.

1-1) Data leakage or breach

Data leakage can be internal or external, intentional or unintentional, authorized or malicious, involving hardware or software. Export of unauthorized data or information to an unintended destination is data leakage. Generally, this is done by a dishonest or dissatisfied employee of an organization. Data leakage is a serious threat to reliability.

1-2) Data sovereignty

Data sovereignty means that information stored in digital form is subject to the laws of the country. The IoT encompasses all things across the globe and is hence liable to sovereignty.

1-3) Data loss

Data loss differs from data leakage in that the latter is a sort of revenge-taking activity on the employer or administrator. Data loss is losing the work accidentally due to hardware or software failure and natural disasters [9].

1-4) Data authentication

Data can be perceived from any device at any time. They can be forged by intruders. It must be ensured that perceived data are received from intended or legitimate users only. Also, it is mandatory to verify that the data have not been altered during transit. Data authentication could provide integrity and originality [10, 11].

1-5) Attack on availability

Availability is one of the primary securities for the intended clients. Distributed denial of service (DDoS) is an overload condition that is caused by a huge number of distributed attackers. But this, not the only overload condition that makes the DCs unavailable to their intended clients. The varieties of overload threat occurrence that cause DCs to freeze at malicious traffic are analyzed here [12]:

- Flooding by attackers
- Flooding by legitimates (flash crowd)
- Flooding by spoofing
- Flooding by aggressive legitimates

1-5-1) Flooding by attackers

DDoS is flooding of malicious or incompatible packets by attackers toward the DCs. This kind of overload threat can be easily detected by Matchboard Profiler. If the attacker characteristic is found, the user can be filtered at the firewall [13].

1-5-2) Flooding by legitimates (flash crowd)

Flash crowd is an overload condition caused by huge numbers of legitimate users requesting the DC resources simultaneously. This can be solved by buffering an excess number of requests so that this overload condition remains life only for a certain period of time [14].

1-5-3) Flooding by spoofing attackers

This is caused by impersonation which can be detected by acknowledging each request and by maintaining the sequence number of the requests and requesters' Internet protocol (IP) address [15].

1-5-4) Flooding by aggressive legitimates

Aggressive legitimates are users who are restless and repeatedly initiate similar requests within a short time span. This leads to an overload condition, where the legitimate users flood the server with requests that slow down the DC performance.

1-6) Modification of sensitive data

During transit from sensors, the data can be captured, modified, and forwarded to the intended node. Complete data need not be modified; part of the message is sufficient to fulfill the intention.

4 ATTACKS AS PER ARCHITECTURE

The IoT has not yet been confined to a particular architecture. Different vendors and applications adopt their own layers [16].

4.1.1 External attack

In order to make full use of the benefits of the IoT, security issues need to be addressed first. Trustworthiness of the cloud service provider is the key concern. Organizations deliberately offload both sensitive and insensitive data to obtain the services. But they are unaware of the location where their data will be processed or stored [17].

4.1.2 Wormhole attack

Wormhole attack is very popular in ad hoc networks. IoT connects both stationary and dynamic objects, ranging from wristwatches and refrigerators to vehicles.

4.1.3 Selective forwarding attack

Malicious nodes choose the packets and drop them out; that is, they selectively filter certain packets and allow the rest. Dropped packets may carry necessary sensitive data for further processing.

4.1.4 Sinkhole attack

Sensors, which are left unattended in the network for long periods, are mainly susceptible to sinkhole attack. The compromised node attracts information from all the surrounding nodes. Thereby, the intruder posts other attacks, such as selective forward, fabrication, and modification [18].

4.1.5 Sewage pool attack

In a sewage pool attack, the malicious user's objective is to attract all the messages of a selected region toward it and then interchange the base station node in order to make selective attacks less effective.

4.1.6 Witch attack

The malicious node takes advantage of the failure of a legitimate node. When the legitimate node fails, the factual link takes a diversion through the malicious node for all its future communication, resulting in data loss [19].

4.1.7 HELLO flood attacks

In HELLO flood news attacks, every object will introduce itself with HELLO messages to all the neighbors that are reachable at its frequency level. A malicious node will cover a wide frequency area, and hence it becomes a neighbor to all the nodes in the network.

4.1.8 Addressing all things in IoT

Spoofing the IP address of virtual machines (VMs) is another serious security challenge. Malicious users obtain the IP address of the VMs and implant malicious machines to attack the users of these VMs. This enables hacking, and the attackers can access users' confidential data and use it for malicious purposes.

4.1.9 Distributed denial of service (DDoS)

DDoS, an attack initiated and continued by some hundreds or even thousands of attackers, starts by populating unwanted traffic packets with enormous size in order to capture and completely deplete memory resources. At the same time, the traffic disallows legitimate requests from reaching the DC and also depletes the bandwidth of the DC [20, 21].

4.1.10 Flash crowd

A flash crowd is basically a sudden increase in the overall traffic to any specific web page or website on the Internet and the sudden occurrence of any event that triggers that particular massive traffic of people accessing that web page or website [22, 23 ,24].

4.1.11 IP spoof attack

Spoofing is a type of attack in which the attacker pretends to be someone else in order to gain access to restricted resources or steal information. This type of attack can take a variety of different forms; for instance, an attacker can impersonate the IP address of a legitimate user to get into their accounts.

4.1.12 Types of spoof attacks

Among the several types of spoofing attacks, the following attacks are addressed, as they are launched on behalf of clients and destroy DC's resources [20, 25].

Type I, Hiding attack: Attackers simultaneously send a large number of spoofed packets with a random IP address. This creates chaos at the DC regarding which specific packets should be processed as legitimate packets, shown in Figure 1.5.

Type II, Reflection attack: Attackers send spoof packets with the source IP address of the victim to an unknown user. This causes unwanted responses to reach the victim from unknown users and increases the flood rate.

Type III, Impersonation attack: Attackers send spoof packets with the source IP address of any unknown legitimate user and acting as a legitimate user. This is equivalent to a man-in-the-middle attack. The spoof attacker receives requests from clients, spoofs IP, and forwards the requests to the DC, acting as a legitimate user. The responses of the DC are again processed intermediately and sent to the clients. This leads to confidentiality issues and data theft or loss at DC.

4.1.13 Goodput

Goodput is the application-level throughput, that is, the number of useful information bits, delivered by the network to a certain destination, per unit of time.

4.1.14 Data centers (DCs)

A DC is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

4.1.15 Botnet

A botnet is a collection of Internet-connected computers whose security defenses have been breached and control ceded to a malicious party. Each such compromised device, known as a “bot,” is created when a computer is penetrated by software from a malware distribution, otherwise known as malicious software [16]. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as Internet Relay Chat (IRC) and hypertext transfer protocol (HTTP) [17, 26, 27].

4.1.16 Confidentiality

All the clients' data are to be transacted in a network channel with greater visibility regarding assurance for the intended clients that data are tamperproof.

4.1.17 Physical security

The hardware involved in serving clients must be continuously audited with a safety checkpoint for the sake of hysteresis identification of threats.

4.1.18 Software security

Corruption or modification of application software by threats could affect several clients who depend on that particular application programming interface (API) and related software interfaces.

4.1.19 Network security

Bandwidth attacks such as DoS and DDoS can cause severe congestion in the network and also affect normal operations, resulting in communication failure.

4.1.20 Legal service-level agreement (SLA) issues

SLAs between customer and service provider must satisfy a legal requirement, as the cyber laws vary for different countries. Incompatibilities may lead to compliance issues.

4.1.21 Eavesdropping

Eavesdropping is an interception of network traffic to gain unauthorized access. It can result in failure of confidentiality. The man in the middle attack is also a category of eavesdropping. The attack sets up a connection with both victims involved in a conversation, making them believe that they are talking directly but infecting the conversation between them [28, 29].

4.1.22 Replay attack

The attacker intercepts and saves old messages and then sends them later as one of the participants to gain access to unauthorized resources.

4.1.23 Back door

The attacker gains access to the network through bypassing the control mechanisms using a “back door,” such as a modem and asynchronous external connection.

4.1.24 Sybil attack

Impersonation is a threat in which a malicious node modifies the data flow route and lures the nodes to wrong positions. In a Sybil attack, a malicious user pretends to be a distinct user after acquiring multiple identities and tries to create a relationship with an honest user. If the malicious user is successful in compromising one of the honest users, the attacker gains unauthorized privileges that help in the attacking process.

4.1.25 Byzantine failure

Byzantine failure is a malicious activity that compromises a server or a set of servers to degrade the performance of the cloud.

4.1.26 Data protection

Data Protection It is difficult for the cloud customer to efficiently check the behavior of the cloud supplier, and as a result, the customer is confident that data is handled in a legal way. But practically, various data transformations intensify the job of data protection.

4.1.27 incomplete data deletion

Incomplete Data Deletion Accurate data deletion is not possible, because copies of data are stored in the nearest replica but are not available.

5 ATTACKS BASED ON COMPONENTS

The IoT connects “everything” through the Internet. These things are heterogeneous in nature, communicating sensitive data over a distance. Apart from attenuation, theft, loss, breach, and disaster, data can also be fabricated and modified by compromised sensors. Figure 1.8 shows the possible types of attacks at the component level. Verification of the end user at the entry level is mandatory; distinguishing between humans and machines is extremely important. Different types of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) help in this fundamental discrimination [18, 19, 20].

6 CONNECTIVITY PROTOCOLS-BASED ATTACKS

IoT objects are armed with different connectivity protocols divided broadly into two main categories, wired and wireless protocols. The wired connection requires a physical medium between IoT objects, while a wireless connection runs through radio waves. Both connectivity technologies have several key properties such as range, data rate, power consumption, spectrum, TCP/IP support, and topology.

6.1.1 *RFID-based attacks:* RFID technology facilitates automatic information exchange between tags and readers using radio waves. RFID uses Automatic Identification and Data Capture (AIDC) technology. RFID tags, recently, have been utilized in many applications such as credit cards, assets tracking, and military [21, 23].

6.1.2 *Replay:* In this type of attacks, an attacker could use tags’ responses to fake readers’ challenges. In replay attacks, the transmitted signal between the reader and the tag is captured, documented, and repeated at a later time to the receiving object, resulting in counterfeiting the accessibility of the tag.

6.1.3 *Spoofing:* This type of attack happens when a malicious tag pretends to be a valid tag and obtains unauthorized access. The spoofing attack used to eavesdrop the data coming from the valid tag and copies the captured data to another one [21].

6.1.4 *Tracking:* Tracking attack can be considered as a direct attack against an individual or a victim. Within the next few years, companies may place RFID tags on many household items. Tracking products using RFID tags could be used to treat the privacy of human by tracking their movements and generate an exact profile of their procurement [21]. Unauthorized access: Due to the lack of authentication in an RFID system, the tag could be vulnerable to an unauthorized attack. The main goal of such an attack is to manipulate its sensitive data [22].

6.1.5 *Virus:* RFID system is not a suitable environment for viruses as the tag has a small storage capacity of 128 bits. However, this situation has changed, as stated that RFID tags could be used as a medium to spread a computer virus. This paper also described how the RFID virus ran in supply chain products [22, 23]. Eavesdropping: An an RFID system, tags and readers are wirelessly connected and communicated without human intervention. So, there is a possibility that their communication medium can eavesdrop. In general, eavesdropping launches when an adversary captures data transmitted between tag and reader since most RFID systems lack any encryption technique during transmission process due to the memory capacity. As a result, it is very easy for an attacker to obtain sensitive data from RFID tags [21, 22, 24].

6.1.6 *Man in the middle (MITM):* MITM attack might happen on RFID system during the transmission of data between reader and tags. In this case, an attacker may intercept and modify the communication channel between the components of the RFID system. This type of attack is considered as a real-time attack, displaying and modifying the information before the legitimate object receiving it [25].

6.1.7 *Killing Tag:* Killing tag attack on RFID system could be launched to stop tags communication with their reader. Killing tags makes them impossible to be read, and therefore, it is absolutely essential to make sure that RFID tags are not killed by an illegal party. Kill command should be secured by a strong password as well [26].

7 CONCLUSION

The appearance of the IoT paradigm in the last few years has unleashed so many threats and feasible attacks against security and privacy of IoT objects and individuals. These threats lead to hampering the realization of this paradigm if they have been left without proper countermeasures. Despite an unprecedented number of security attacks generated on the IoT domain, there is a lack of a standard method to identify and address such attacks. This paper, therefore, makes a best effort to provide a comprehensive classification of IoT attacks based on a novel building-blocked reference model, along with proposed countermeasures to mitigate them. However, implementation of all these security measures and techniques together consumes computation as well as battery power of devices which is not acceptable for IoT technology and its devices. There is a need for a security mechanism which handles maximum security problems but it should be lightweight and robust for fit for IoT technology. Many of the attacks on IoT have been discussed and classified above. Some of these attacks can be avoided by just keeping some security precaution while the development of an application like checking node identity while communication or using devices which are difficult to tamper.

REFERENCES

[1] G. Chuankun, Wu. A preliminary investigation on the security architecture of the Internet of Things. *Strategy and Policy Decision Research*, 2010, 25(4): 411–419.

[2] Goldman Sachs. *IoT Primer, The Internet of Things: Making Sense of the Next Mega-Trend*. September 3, 2014.

[3] H. Damghani, H. Hosseinian, L. Damghani, and F. Faghihi, “Standardization for the Internet of Things,” in *4th International Conference on Combinatorics, Cryptography, Computer Science and Computation,* November 2019.

[4] International Telecommunication Union. ITU Internet reports 2005: The Internet of Things. 2005.

[5] Ibrahim Mashal, Osama Alsaryrah, Tein-Yaw Chung, Cheng-Zen Yang, Wen-Hsing Kuo, Dharma P. Agrawal. Choices for interaction with things on internet and underlying issues. *Ad Hoc Networks*, 2015, 28: 68–90.

[6] Jeyanthi, N., N.Ch.S.N. Iyengar. Escape-on-sight: An efficient and scalable mechanism for escaping DDoS attacks in cloud computing environment. *Cybernetics and Information Technologies*, 2013, 13(1): 46–60.

[7] L. Damghani, H. Damghani, H. Hosseinian, H. Mohammadnezhad Shourkaei, “Analytics in Internet of Things and BigData,” in *4th International Conference on Combinatorics, Cryptography, Computer Science and Computation,* November 2019.

[8] H. Damghani and L. Damghani, “Security improvement of Common Scrambling Algorithm (CSA) using the encryption extension technique,” in *16th Iran Media Technology Exhibition & Conference (IMTEC2019),* IEEE, November 2019.

[9] H. Damghani, H. Hosseinian, and L. Damghani, “Bitcoin through Amateur Radio,” in *4th Conference on Technology In Electrical and Computer Engineering (ETECH2019),* 2019

[10] H. Damghani, H. Hosseinian, and L. Damghani, “Cryptography review in IoT,” in *4th Conference on Technology In Electrical and Computer Engineering (ETECH2019),* 2019.

[11] H. Hosseinian, H. Damghani, L. Damghani, G. Nezam and H. Hosseinian, “Home appliances energy management based on the IoT system,” *The International Journal of Nonlinear Analysis and Applications,* 2019.

[12] H. Hosseinian, H. Damghani, L. Damghani, E. Kouhi and M. Kouhi, “Asia’s Cities: The way to Going Smart,” *The International Journal of Nonlinear Analysis and Applications,* 2019.

[13] Kang Kai, Pang Zhi-bo, Wang Cong. Security and privacy mechanism for health Internet of Things. *The Journal of China Universities of Posts and Telecommunications*, 2013, 20(Suppl. 2): 64–68.

[14] H. Hosseinian and H. Damghani, “Smart home energy management, using IoT system,” in *5th Conference on Knowledge Based Engineering and Innovation (KBEI), IEEE,* 2019.

[15] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 2015, 32: 17–31.

[16] Lan Li. Study on security architecture in the Internet of Things. *Measurement,International Conference on Information and Control (MIC),* 2012, pp. 374–377.

[17] Peng, Xi, Zheng Wu, Debao Xiao, Yang Yu. Study on security management architecture for sensor network based on intrusion detection. *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, IEEE, New York.

[18] Prabadevi, B., N. Jeyanthi. Distributed denial of service attacks and its effects on cloud environment: A survey. *The 2014 International Symposium on Networks, Computer and Communications,* June 17–19, 2014, Hammamet, Tunisia, IEEE.

[19] Qazi Mamoon Ashraf, Mohamed Hadi Habaebi. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, 2015, 49: 112–127.

[20] H. Damghani, H. Hosseinian, and L. Damghani, “Overview of security aspects for LTE and LTE-A networks,” in *14th Media Technology Conference,* Islamic Republic of Iran Broadcasting, Tehran, Iran, December 2017.

[21] Qinglin, Cao. Review of research on the Internet of Things. *Software Guide,* 2010, 9(5): 6–7.

[22] Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenge of security and privacy in distributed Internet of Things. *Computer Networks*, 2013, 57: 2266–2279.

[23] Rolf H. Weber. Internet of Things—New security and privacy challenges. *Computer Law and Security Review*, 2010, 26: 23–30.

[24] H. Damghani, "RFID Technology: Benefits and Applications," *Monthly Journal of Transportation and Development*, vol. 36, pp. 70–73, August 2010.

[25] H. Damghani, H. Hosseinian, and L. Damghani, "Investigating attacks to improve security and privacy in RFID systems using the security bit method," in *5th Conference on Knowledge Based Engineering and Innovation (KBEI), IEEE*, 2019.

[26] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 2015, 76: 146–164.

[27] Wang, Y.F., Lin, W.M., Zhang, T., Ma, Y.Y. Research on application and security protection of Internet of Things in smart grid, *Information IET International Conference on Science and Control Engineering 2012 (ICISCE 2012)*, 2012, pp. 1–5, Shenzhen, China.

[28] Xingmei, Xu, Zhou Jing, Wang He. Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of Things. *3rd International Conference on Computer Science and Network Technology (ICCSNT)*, 2013, pp. 825–828.

[29] K. Naito, "A Survey on the Internet-of-Things: Standards, Challenges, and Future Prospects," Journal of Information Processing, vol. 25, pp. 23–31, Jan 2017.