**A study on the impact of developing technologies on internet of things security**

Swati Thakur Ashish Shukla Deepesh Tamrakar

Computer Sc. & engg. Computer Sc. & engg. Computer Sc. & engg.

SRGI SRGI SRGI

Jabalpur, India Jabalpur, India Jabalpur, India

[swati.rajput.cs@gmail.com](mailto:swati.rajput.cs@gmail.com) [ashishsoftskills09@gmail.com](mailto:ashishsoftskills09@gmail.com) [deepesh.tamrakar@gmail.com](mailto:deepesh.tamrakar@gmail.com)

**ABSTRACT**

The Internet of Things (IoT) has opened the door to unlimited application possibilities in many social sectors of the world, but it also comes with several difficulties. Security and privacy concerns are one of those difficulties. IoT devices are more vulnerable to security threats and attacks. Due to the limitations of IoT devices such as space, power, memory, etc., there is a lack of security solutions compatible with IoT devices and applications, making this world of securely connected things the "Internet of Insecure Things". In addition to traditional or standard methods, adding security solutions to IoT device hardware offers a viable solution to this problem. With the addition of new technologies such as machine learning, blockchain, fog/edge/cloud computing and quantum computing in IoT networks, the system now has more vulnerabilities. This article presents research on IoT security threats and solutions. This study also describes the integration of emerging technologies such as machine learning and blockchain into the Internet of Things, the difficulties that arise as a result of the integration, and possible solutions to these problems. The article describes information security issues and their solutions, using the 4-layer IoT architecture as a reference.

**Keywords—** IOT security, Machine learning, Blockchain, Threats, Security solution.

# INTRODUCTION

The booming IoT sector is witnessing the growing number of IoT devices in the market, but many of these devices face resource constraints. As a result, many IoT devices cannot be protected by traditional security solutions, so it is necessary to provide these devices with more flexible security options. The network, hardware and software constraints of IoT devices are security constraints. Compute, storage, power, and memory limitations are all hardware-induced. Software-based restrictions consist of built-in software restrictions. Mobility, scalability and slow, intermittent network connections are just some of the limitations associated with networks. These are due to the use of low-power radios, so they also operate at low data rates.

Several works have been published on IoT security; However, they focus on some specific IoT topics. More detailed explanations are needed as some topics are not covered, such as security challenges when incorporating new technologies into IoT and security hardware solutions to accommodate resource-constrained IoT devices. The following is a list of what this work contributed:

# • Analyze IoT integration difficulties and possible solutions and integrate new technology.

# • Present low-cost hardware security options as a viable option for resource-constrained IoT devices.

# • Explore numerous IoT security threats from a mobile hardware, software and data perspective.

# • Identify and describe popular IoT security primitives and other techniques used to protect IoT networks and devices from threats or attacks.

# IoT security threats

Three categories of security threats are possible. threats in the form of hardware attacks, including those involving IC applications. Threats that take the form of employing malicious software to take complete control of devices come in second. threats that intercept and alter data as it is being transmitted, lastly. Figure 1 depicts them. The three types of typical IoT security threats are mentioned below with a brief overview of each:

**Hardware threats:**

1. Hardware Trojan - Using a Trojan, an attacker monitors, modifies or shuts down the data contained in the chain or the communication in the chain. This is done during the design or manufacture of the device. The general concept of hardware Trojans is shown in Figure 2. There are several types of hardware Trojans:

2. Combination/sequence. Combination: the occurrence of a certain situation in certain internal nodes of the chain requires the activation of the Trojan.

3. Sequential: Activation of the Trojan requires a certain series of unusual logical values ​​in the internal nodes.

4. Attributes. Activity, physical and activation.

5. Trigger and carrier mechanism. There are two types of operating mechanisms: digital and analog.

When a hacker uses physical data stolen from the system while the application is running, it is called a side-channel attack. The adversary conducts non-intrusive hardware-based attacks using energy consumption, electromagnetic radiation, timing information, and audio measurements. The resulting data can be analyzed to obtain private information such as encryption keys. Techniques for performing a side-channel attack include differential error analysis, power monitoring, electromagnetic analysis, and key decryption using audio cryptanalysis. An attack design for using differential power analysis to extract secret information from a smart card is shown in Figure 3.

Capture occurs when an attacker modifies data associated with an IC after it has been used in an application. Most Internet of Things (IoT) devices are configured without physical security to allow an attacker to physically access the device or modify the firmware wirelessly. An attacker can add malicious hardware or software to change the operation of an IC or device. Denial of Service (DoS) or Distributed DoS (DDoS) occurs when attackers manipulate the internal functions of an IC to prevent users from using a service.

**Software threats:**

Botnet: A group of networked computers infected with malware. Resource-constrained IoT devices are easy targets for cybercriminals because they lack strong security measures. These devices can be used to create botnets that are completely controlled by the cybercriminal. Cybercriminals use botnets to distribute Distributed Denial of Service (DDoS), spam, phishing attacks and malware. Botnets can use a peer architecture, a centralized architecture, or a combination of the two. Figure 4 shows the basic architecture of a botnet.

Phishing is the act of an attacker pretending to be a legitimate IoT device or authenticated user to gain access to a network. The legitimate user's Media Access Control address or Internet Protocol address is used for this.

A Denial of Service (DoS) occurs when an attacker uses a computer or computers to overwhelm a target with a large volume of messages or data. User Datagram Protocol (UDP) flood, ICMP flood or ping flood are some of the most popular DDoS attacks. DDoS attacks include SYN flood, ping of death, slowloris, NTP verification, HTTP flood and zero-day attacks. The DoS attack architecture is shown in Figure 5.

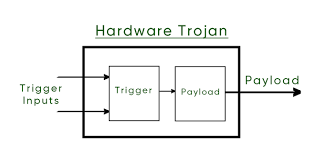


Fig. 1 General Structure of Hardware Trojan

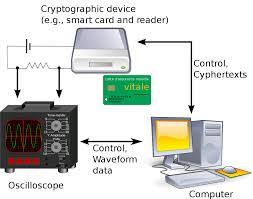


Fig. 2 differential power analysis attack

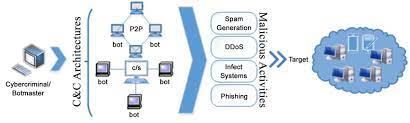


Fig. 3 Basic Botnet Architecture

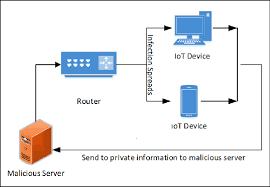


Fig. 4 An example of Spoofing



Fig. 5 DoS Attack Architecture

* 1. **Data in transit:**
* To eavesdrop or sniff, an attacker uses a program or software such as Wireshark to record the transmitted data. Hackers use techniques designed to search for and record conversations that contain personal information. If the security of the device is insufficient, an attacker must read or listen to the collected information to obtain useful information. Security flaws that use eavesdropping include voice combing and artificially intelligent assistants like Alexa and Siri. Figure 6 shows the design of the Sound Comber mobile application.
* When a hacker steals data packets from an authenticated device, stores them, and then delays or resends them while impersonating the authenticated device, this is called a replay attack. • Viewing recorded network traffic and extracting useful information from traffic patterns is the process of traffic analysis. Link load analysis attacks, which are used to measure the volume of traffic on a network communication channel, and flow analysis attacks are two types of traffic analysis attacks. A connection attack that aims to determine the connection of a stream between a sender and a receiver.
* A man-in-the-middle attack occurs when a criminal acts as an intermediary or proxy between the sender and receiver of the dialogue. An attacker in this position can eavesdrop and modify conversations between sender and receiver. Scheme 7.
  1. Table 1: displays information about reported security assaults based on IoT threat classes, along with a description of each attack.

# IoT security solutions

Using best-in-class encryption techniques to protect data in transit (data sent over a side link) and data at rest (data stored on devices) is a standard procedure for combating threats and attacks against IoT devices and IoT networks. Once the identity of the entity requesting access to the network, device or service is established, appropriate authentication techniques are required. We then need to consider how the various security protocols are implemented from the perspective of the security architecture layers of IoT (discussed above). In addition, IoT networks and devices must be protected with appropriate security measures against advanced threats and potential application-specific attacks.

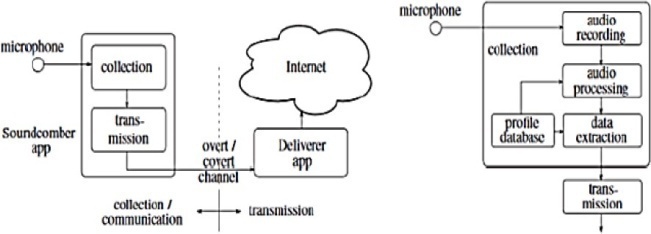
* 1. Cryptographic solutions for data protection

Several encryption methods are available to protect our sensitive data. Unfortunately, not all are suitable for situations where resources are limited, such as IoT devices. IoT devices used in commercial and industrial settings are vulnerable to IoT-specific attacks. Security will become a much bigger issue in the near future if we stay in the current IoT device design cycle where it is an afterthought. Lightweight encryption techniques are explored to develop a robust encryption solution for constrained IoT devices.

Lightweight t-encryption. Encryption is necessary to securely protect the data created and transmitted by the layers - the observation layer, the network and the application. A lightweight cryptosystem is necessary because the perception layer has all the limited components of these three. To judge how lightweight an encryption method is, two criteria must be considered. The first criterion is the weight of the encryption software, which is determined by its time and memory complexity. Memory complexity and time complexity both refer to how long it takes a cipher to convert plaintext to ciphertext. Time complexity refers to how much memory is required to perform the encryption process. Another criterion is the hardware weight of the encryption, based on its size and power requirements. The encryption area is expressed by the number of gate equivalents (GE) is used to execute it, while the energy consumption of encryption is the amount of energy used during execution. The area of ​​a two-input NAND gate is divided by its surface area (measured in micrometers squared; m2) to obtain the overall gain (GE). The algorithm must meet lightweight requirements and work just like regular algorithms according to security standards and safeguards. Asymmetric key encryption technology and symmetric key encryption

there are two classes to which current cryptographic primitives belong.

Fig. 6 Architecture of a Soundcomber



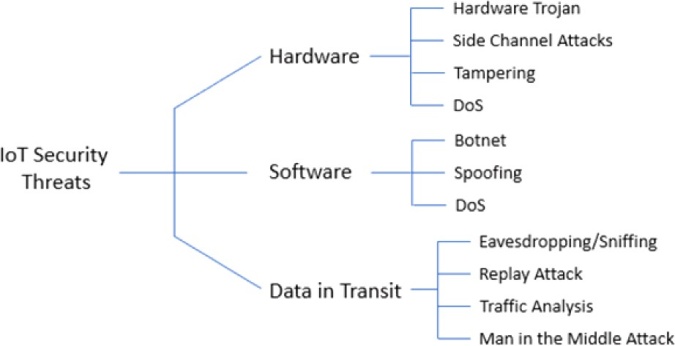


Fig. 7 IoT Security Threats

Table 1: Security Threats and Attacks on the Internet of Things Based on Recent Reports of Attacks

|  |  |  |  |
| --- | --- | --- | --- |
| Security Threats/Attacks | | Reported Attacks | Description |
| Hardware | Tempering | Jeep hack | Hackers managed to exploit a weakness in Jeep's firmware update system. |
|  | Tempering | Voice-Controllable System | Commands based on laser-based sound injection are used to connect devices such as a thermostat. |
| Software | Botnet DDoS | Malware Attack | BrickerBot once rendered IoT devices permanently unusable. |
|  | Botnet | Silex malware | Brickerbot removed firmware from 2,000 IoT devices. |
|  | Botnet DDoS | Mirai botnet | The infrastructure of the domain name on the Internet, run by Dyn, crashed as a result of this attack. |
|  | Botnet | Malware attack | 500,000 network routers and network storage devices infected by VPNFilter botnet. |
| Data in Transit | Traffic Analysis Eavesdropping/ Sniffing | Sybil attack on Tor Network | Discovered the IDs of website owners using Tor-wide services by exploiting a flaw in the Tor protocol. |
|  | MITM Attack Eavesdropping/ Sniffing | Tesla Model S key fob attack | If a hacker can receive signals from its transmission wirelessly, they can obtain the encryption key from the key and create a copy of it. |
|  | Eavesdropping/ Sniffing | Target’s data br-each involving IoT  HVAC system | This breach exposed the credit card information of nearly 41 million people. |

**Asymetric Key Cryptography**

Asymmetric encryption algorithms have attracted the attention of a small number of researchers studying lightweight cryptography, but unfortunately the development has not yet been as continuous and productive as the development of symmetric encryption algorithms. Lightweight asymmetric encryption methods are often not space- or energy-efficient because they are difficult to use. These algorithms will become visible as attack models evolve. Reading gate functions such as prime and semi-prime factors and Euler sum function are commonly used in asymmetric algorithms. Two types of asymmetric algorithms are key distribution algorithms and encryption algorithms. Rivest-Shamir-Adleman (RSA) is one of the best asymmetric encryption algorithms. ECC (Elliptical Curve Cryptography) and Diffie-Hellman provide good examples of asymmetric key distribution techniques. In the context of public key cryptosystems, ECC and Digital Signature Algorithm (DSA) work together to create a digital signature. Figure 8. Digital Signature Algorithm (DSA). DSA outperforms other asymmetric algorithms in terms of efficiency and speed. In addition, sharing signatures is difficult and digital signatures only last a short time.

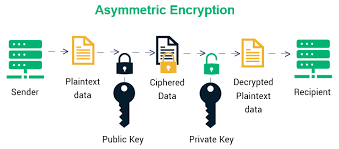


Fig. 8 Asymmetric Key Cryptography

**Symmetric Key Encryption:**

Encryption with symmetric keys. Since most operations in symmetric cryptography are based on bidirectional functions such as XOR and permutations, they are faster and do not consume many resources. Therefore, these algorithms are more suitable for IoT applications. The main difference between symmetric algorithms is between stream ciphers, hash functions and block ciphers. A standard symmetric key encryption architecture is shown in Fig. 9.

The stream encryption. stream encryption. Trivium, WG-8 and Espresso are some examples of popular high-performance lightweight streamers. Although Grain 128 has lower throughput, it is better suited for lightweight encryption on limited devices. Figure 10 illustrates how the stream encryption and decryption process works.

Routing functions Fast computation and reduction of output value overlap are two key features of a good hash function. A recent study looked at several compact hash functions that may be useful in the Internet of Things. list CURRENT block cipher applications in decentralized modes. Spongent, FOTON, and GLUON are more examples of compact hash functions used in research. Figure 11 shows a typical structure of the has function.the block cypher. For IoT applications, this method is particularly beneficial. The encryption and decryption techniques used in this operation are nearly symmetrical or identical. Because block cyphers have a low latency, they are the IoT security solutions that have been most extensively studied and improved. Block cyphers come in many forms, with a few examples include Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3DES, Blowfish, and Twofish. Different strategies have been developed by researchers to make block cyphers suitable for IoT and lightweight. A few simple block cyphers under investigation include Curupira, PRESENT, KATAN, TEA, Hummingbird, RECTANGLE, and SIMON. Figure 12 depicts a standard block cypher model.

Responsible for the keys. If the security properties of a key management protocol are availability, integrity, confidentiality, authentication and non-repudiation, it is considered secure. IoT key management protocols fall into three categories: decentralized, distributed, and centralized. A centralized key management protocol uses a key distribution center that acts as a server and is consulted before group members communicate with each other. It also distributes encryption keys to each group member. To avoid a single point of failure, a cryptographic group key can be distributed to all members of the group using a distributed key management protocol. Group members work together to create a shared session key for decentralized protocols.

**Authentication solutions**

Device or person identification. This procedure checks for online objects. From an IoT perspective, each object must be able to identify and authenticate all other objects in the system or system components with which it interacts. Hardware-based, token-based, non-token-based, and procedural are the four authentication techniques offered.

Procedural authentication. Such authentication can be one-way, two-way or three-way. With one-way authentication, the primary or trusted device verifies the identity of the untrusted entity. An overview of the Physical Unclonable Functions (PUF) protocol, a one-way authentication method, is shown in Figure 13. Both the trusted and untrusted entities authenticate each other using two-way (also known as mutual) authentication. When a third entity is involved in the two-entity authentication process, it is called three-way authentication and is considered reliable.

Brand specific. This technique authenticates the object based on information generated by the server. If a user enters a legitimate login and password, they often receive a token. An entity can access authentication resources using this permission. OAuth2 and Open ID are two protocols used for identity. Figure 14 shows the use of token-based authentication in an IoT application.

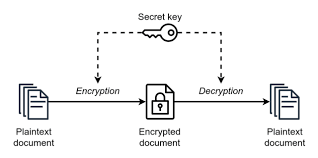


Fig. 9 Symmetric Key Cryptography

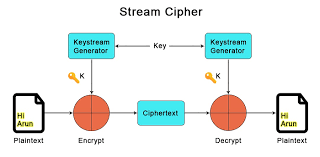


Fig. 10 Stream Cipher

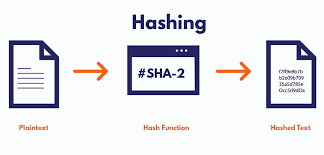


Fig. 11 Hash Function

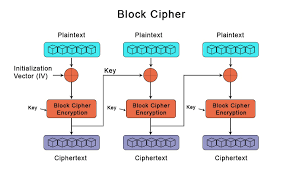


Fig. 12 Block Cipher

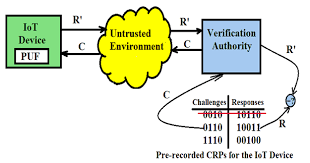


Fig. 13 PUF-based One-way Authentication

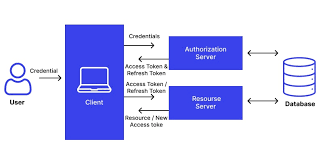


Fig. 14 Token-based Authentication

**Security solutions for IoT platforms**

Software that facilitates the sharing of data and services between IoT devices on a network is known as an IoT software platform. Connections and network management, device management, processing and visualization analysis, application deployment, information security, event processing, monitoring, integration and data storage and collection are some of the features of the platform. The data security solutions of the platform can be classified into four categories: secure data storage, identification of devices requesting connection and transmitting data, identification of devices sending data during data transmission and authorization of individuals or organizations. IoT platforms can be divided into two groups: cloud-based platforms and open source platforms. closed source IoT platform. Closed-source IoT platforms combine the full functionality of the platform with IoT devices and cloud computing as a service.

# Emerging technologies: challenges and countermeasures

**Machine Learning (ML) security risks**

Despite the fact that machine learning systems come in different forms, they all share a common pipeline that provides unique vulnerabilities for any machine learning system. Figure 17 shows the pipeline of a general machine learning system. This diagram shows the first nine essential components of any machine learning system: global raw data, dataset composition, datasets, learning algorithm, evaluation, evaluation, inputs, inputs, model, inference algorithm, and outputs. The nine components of the entire machine learning system are mapped to the risk list in this section. Some of these hazards are referenced between different components. A number of safeguards are also proposed to reduce the security risks associated with the use of each machine learning component.

According to the world's raw data, the data of a machine learning system is as important in terms of security as the learning algorithm and any technical implementation. The term "raw data" in this context refers to any type of data, not just the training data used by machine learning algorithms.

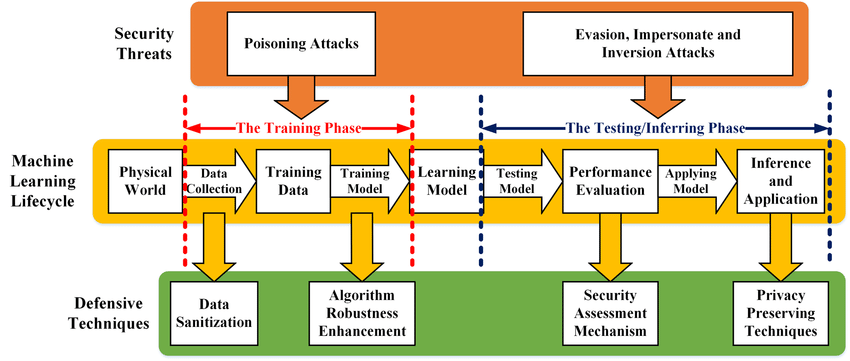


Fig. 15 a generic machine learning system with attacks

**IV. Blockchain technology security risk:**

Transaction privacy, decentralization, data immutability, non-repudiation, transparency, pseudonymity and traceability, integrity, authorization, system transparency and fault tolerance are the main security elements of blockchain described in Section V. Despite these useful security features, there are still some security risks or vulnerabilities when implementing Blockchain technology in the Internet of Things. compiled a list of potential threats to blockchain components and related safeguards to mitigate their consequences. Figure 18 shows the nine (9) components that make up a blockchain: System Management, Blockchain Consensus, Network, Member Services, Transactions, Ledger, Smart Contracts, System Integration and Wallet.

The three main security features of Blockchain are transaction privacy, decentralization and data immutability. This section covers the threats to which each component of the blockchain is exposed and recommended safeguards to mitigate those risks. Our goal is to develop a blockchain that the IoT network can integrate quickly and easily without worrying about security.

system administration. Thus, it is now possible to create, modify and track blockchain components. Since the function of this component is important, it comes with some security risks. Potential security risks:

Transaction Integrity: Transaction integrity can be compromised if the peer node processing it has a non-unique account address. To preserve the integrity of this transaction, the private keys should not be used in subsequent transactions. Often private key and ECC technology are used to generate the public key. An attacker who knows the recycled private key can decrypt the public key and view the raw data of the transaction. Each partner node must match the hash value of the new transaction block with the hash value contained in the blockchain when validating a new transaction block. An experiment by Leurend and Peyrin (2020) revealed a weakness in popular hashing algorithms such as SHA-1 and MD5.

Even if a partner or component fails, the blockchain is secure. However, a problem can arise if the failed partner is a network node that acts as a connection point to the gateway. If this node suffered a DoS attack, the blockchain would become unusable. A DoS attack on multiple blockchains affects network reliability or availability. If multiple nodes fail or are maliciously targeted at the same time, how many nodes are needed for a blockchain to be considered trustworthy?

Keeping a single blockchain node: Count accepted, processed and block-related transactions to join the blockchain, keeping only one partner. This monitoring does not provide information about the partner node's resource usage.



Fig. 16 Blockchain Components

The results of this monitoring do not include information about the status of other peers or information about peer network bandwidth, throughput and latency. controls provided It is important that the data in each block of the blockchain is consistent. Once uploaded to the blockchain, a transaction block cannot be deleted. SHA-256 is the most popular hash function on public and private blockchains. The redundancy required at the entry point of the blockchain network is achieved through many gateways. The health of the blockchain network depends on how well the processes work. Monitor the many features of the blockchain using tools. It was proposed to develop a reputation model that evaluates the behavior of each consensus node during the consensus process, Agreement on cryptocurrencies. Block data collection and processing partners maintain a duplicate ledger on an ongoing basis. Nodes on blockchains use consensus to decide which new blocks to add to the chain.

# V. Conclusion

There are countless opportunities for IoT applications in various sectors of society, but there are also many challenges. One of these challenges is security and privacy issues. Due to their shortcomings, IoT devices are more vulnerable to security threats and attacks. The lack of information security solutions suitable for IoT applications is pushing the world of securely connected things apart from the secure Internet of Things. In this review article, we discussed the current state of IoT security and the solutions that need to be put in place to convince readers that IoT's reputation is not only about providing cheap devices, but also about providing the best security solutions to deal with security threats and privacy concerns.

For the IoT to be secure, consumers, security managers and future IoT developers must be aware of its security aspects. It is the developer's responsibility to ensure that information security is considered when designing the system or program. In this work, we evaluated and investigated IoT security threats from several perspectives (including hardware, software and transmitted data) and emphasized the need for different security threats to avoid strategies. Security options are also being explored. To explore the limits of IoT devices, we compare available device security solutions with a focus on securing these devices.

##### The introduction of new technologies increases the vulnerability of the IoT environment, which affects the security of the entire network. We presented the security implications of using two of the most important emerging technologies, blockchain and machine learning, on an IoT platform and proposed mitigation strategies. Researchers gain new insights into the progress of their field.

##### VII. REFERENCES

1. K. Ashton, “That ‘Internet of Things’ Thing,” June 22, 2009. [Online]. Available: <https://www.rfidjournal.com/that-internet-of-things-thing>. [Accessed on Jul. 4, 2020].
2. European Union Agency for Network and Information Security (ENSIA), “Baseline security recommendations for IoT,” November 20, 2017. [Online]. Available: <https://www.ensia.europa.eu/publications/baseline-security-recommendations-for-iot>. [Accessed: Jul. 4, 2020].
3. [S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (5) (2015) 164](http://refhub.elsevier.com/S2542-6605(22)00059-2/sbref0003).
4. M. Hasan, “IoT in healthcare: 20 examples That’ll make you feel better,” April 2, 2020. [Online]. Available: [https://www.ubuntupit.com/iot-in-healthcare-20-](https://www.ubuntupit.com/iot-in-healthcare-20-examples-thatll-make-you-feel-better) [examples-thatll-make-you-feel-better](https://www.ubuntupit.com/iot-in-healthcare-20-examples-thatll-make-you-feel-better). [Accessed: Nov. 5, 2020].
5. Lanner. “Examples of IoT devices in your next smart home,” September 10, 2018. [Online]. Available: [https://www.lanner-america.com/blog/5-examples-iot-](https://www.lanner-america.com/blog/5-examples-iot-devices-next-smart-home) [devices-next-smart-home](https://www.lanner-america.com/blog/5-examples-iot-devices-next-smart-home). [Accessed: October 10, 2020].
6. A. Grizhnevich, “IoT for smart cities: use cases and implementation strategies,” May 3, 2018. [Online]. Available: [https://www.scnsoft.com./blog/iot-for-](https://www.scnsoft.com./blog/iot-for-smart-city-use-cases-approaches-outcomes) [smart-city-use-cases-approaches-outcomes](https://www.scnsoft.com./blog/iot-for-smart-city-use-cases-approaches-outcomes). [Accessed: Oct. 10, 2020].
7. S. Chaudhary; R. Johari, R. Bhatia, K. Gupta and A. Bhatnagar, Craiot: concept, review, and application(s) of IoT. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019.
8. Alibaba, “Siemens and Alibaba cloud partner to power industrial Internet of Things in China,” [Online]. Available: [https://www.alibabagroup.com/en/news/](https://www.alibabagroup.com/en/news/press_pdf/p180709.pdf)

[press\_pdf/p180709.pdf](https://www.alibabagroup.com/en/news/press_pdf/p180709.pdf). [Accessed: Oct. 11, 2020].

1. DHL, “Internet of Things,” [Online]. Available: [https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/internet-of-](https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/internet-of-things-in-logistics.html) [things-in-logistics.html](https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/internet-of-things-in-logistics.html). [Accessed: Oct. 12,2020].
2. Konux, “Transform railway operations for a sustainable future,” [Online]. Available: [https://www.konux.com](https://www.konux.com/). [Accessed: Oct. 12, 2020].
3. Nexiot. [Online]. Available: [https://nexxiot.com](https://nexxiot.com/). [Accessed: Oct. 12, 2020].
4. Scandit. [Online]. Available: [https://www.scandit.com](https://www.scandit.com/). [Accessed: Oct. 14, 2020].
5. Apple. [Online]. Available: [https://www.apple.com](https://www.apple.com/). [Accessed: Oct. 14, 2020].
6. Cognigy. [Online]. Available: [https://www.cognigy.com](https://www.cognigy.com/). [Accessed: Oct. 14, 2020].
7. Huawei. [Online]. Available: <https://www.huawei.com/us>. [Accessed: Oct. 17, 2020].