**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 ashishsoftskills09@gmail.com deepesh.tamrakar@gmail.com

**ABSTRACT**

The Internet of Things (IoT) has widened the door to a world of limitless potential for implementations in a variety of societal sectors, but it also comes with many difficulties. Security and privacy issues are one of those difficulties. IoT equipment is more vulnerable to security threats and assaults. Due to the limitations of IoT devices, such as those related to space, power, memory, etc., there is a dearth of security solutions that are compatible with IoT devices and apps, which is turning this world of securely linked things into the "internet of insecure things." Beyond the conventional or standard approaches, incorporating security solutions in the IoT device's hardware offers a viable solution to this issue. As new technologies like machine learning, blockchain, fog/edge/cloud computing, and quantum computing have been incorporated into IoT networks, there are now more weak points in the system. The study on IoT security threats and solutions is introduced in this article. This survey also describes the integration of developing technologies like machine learning and blockchain in IoT, the difficulties that have arisen as a result of this integration and possible solutions to these difficulties. The paper describes security problems and their solutions using the 4-layer IoT architecture as a reference.

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

# INTRODUCTION

A thriving IoT sector is indicated by the increasing number of IoT devices on the market, yet many of these devices experience resource limitations. Due to this, many IoT devices cannot be protected by traditional security solutions, so it is imperative to offer these devices more flexible security options. According to [17], IoT device networking, hardware, and software restrictions constitute security constraints. Computing, storage, power, and memory restrictions are all caused by hardware. Software-based restrictions consist of embedded software restrictions. Mobility, scalability, and slow intermittent network connections are only a few networking-related limitations. These are brought on by the use of low-power radios, which also causes them to operate at low data rates.

Several works have been published on IoT security; however, they focus on a small number of IoT-specific topics. There is a need for more thorough surveys because some topics have not been addressed, such as the security issues with incorporating new technologies into IoT and security hardware solutions that can match the resource-constrained IoT devices. Following is a list of what this work has contributed:

* Analysis of IoT integration difficulties and potential solutions, as well as new technology integration.
* Outline affordable hardware security options as a feasible choice for IoT devices with limited resources.
* Review the many IoT security threats from the viewpoints of hardware, software, and data in transit.
* Identify and describe popular IoT security primitives and other technologies used to defend IoT networks and devices from threats or assaults.

# 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, the attacker watches, modifies, or shuts down the data contained in the circuit or the communication of the circuit. This is carried out when the gadget is being designed or made. The overall concept of a hardware Trojan is shown in Figure 2. There are several types of hardware trojans:
2. Combinational/Sequential. Combinational: The occurrence of a specific circumstance at specific internal nodes of the circuit is required for the trojan to be activated.
3. Sequential: The occurrence of a particular sequence of uncommon logic values at internal nodes is required for the trojan to be activated.
4. Attributes. Action, physical, and activation.
5. Mechanism for the trigger and payload. There are two different kinds of trigger mechanisms: digital and analogue.

A side channel attack occurs when a hacker takes use of the physical information that is leaked from a system while an application is running. The adversary uses power utilisation, electromagnetic radiations, time data, and sound measurements to carry out non-intrusive hardware-based attacks. To extract private information like cryptographic keys, the obtained data can be analysed. Differential fault analysis, power monitoring, electromagnetic analysis, and acoustic cryptanalysis key extraction are techniques for carrying out a side channel attack. Figure 3 depicts the attack's architecture for obtaining secret data from the smart card via differential power analysis.

When an attacker modifies an IC's related data after it has been used in an application, this is known as tampering. The majority of IoT devices will be installed in environments without any physical protections against an attacker physically getting access to the device or wirelessly tampering with the firmware's software. To alter the behaviour of an IC or the device, the attacker can add malicious hardware or software.

When attackers tamper with an IC's internal workings to prevent users from using the service, it is known as a Denial of Service (DoS) or Distributed DoS (DDoS).

**Software threats:**

Botnet: A group of online computers that have been infected with malicious software. IoT devices with limited resources are easy targets for cybercriminals because they lack robust security measures. These gadgets can be used to create fully controlled botnets by the cybercriminal. Cybercriminals utilise botnets to conduct Distributed Denial of Service (DDoS), spamming, phishing assaults, and malware distribution. Peer-to-peer architecture, centralised architecture, or a hybrid of the two can all be used in botnets . Figure 4 displays the fundamental botnet architecture.

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

A denial of service (DoS) occurs when an attacker uses a computer or computers to overwhelm or flood a target with a large volume of messages or data. User datagram protocol (UDP) flooding, ICMP flooding, or ping flooding are a few of the most popular DDoS assaults. DDoS assaults include those using SYN floods, ping of death, slowloris, NTP amplification, HTTP flood, and zero-day exploits. A DoS attack architecture is illustrated 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:**
* Eavesdropping/Sniffing is done by an attacker who utilizes a programme or piece of software (like Wireshark) to record data as it is being transmitted. Hackers utilize tools designed to find and record discussions involving private data. In the event that a device lacks sufficient security measures, the attacker only needs to read or listen to the collected data in order to gain useful information. Sound comber and artificially intelligent assistants like Alexa and Siri are security exploits that use eavesdropping. The architecture of the smart phone app Sound comber is shown in Figure 6.
* A replay attack occurs when a hacker steals data packets from an authenticated device, saves them, and then delays or retransmits them later under the guise of an authenticated device.
* Traffic analysis is the process of looking at recorded network traffic to determine meaningful information based on communication patterns. There are two forms of traffic analysis attacks: link-load analysis attacks, which are used to determine the rate of traffic on a network communication channel, and flow analysis attacks.-attack on connectivity with the objective of identifying the flow connectivity between a sender and a receiver
* A man-in-the-middle assault is one in which the perpetrator intervenes in the conversation as a relay or proXy between the sender and the recipient. Assailant in this position has the ability to intercept and change communications between sender and receiver. Picture 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

Utilizing the top encryption techniques to safeguard data in transit (data sent over a communication link) and data at rest (data stored on a device) is the standard procedure for addressing various threats and attacks on IoT devices and IoT networks. Once the identity of an entity requesting access to a network, device, or service has been established, appropriate authentication techniques are required. Then, from the standpoint of the layers of the IoT security architecture (discussed above), we need to consider how to implement various security protocols. Additionally, IoT networks and devices must be safeguarded with appropriate security measures against sophisticated threats and possible application-specific attacks.

* 1. **Cryptographic solutions for data protection**

To protect our sensitive data, a variety of cryptographic methods are available. Unfortunately, not all of them are appropriate for situations with limited resources, such as IoT devices.

IoT devices used in both commercial and industrial settings are susceptible to IoT-specific assaults. Security will become a much bigger problem in the near future if we stick with the current IoT device design cycle, where it is treated as an afterthought. In order to develop a robust cryptographic solution for restricted IoT devices, lightweight cryptographic techniques are being studied.

Lightweight t cryptography. To securely protect the data created and transferred by the layers—the perceptual, network, and application—each requires encryption. A lightweight cryptographic system is required since the perceptual layer, out of these three, has all the limited components. To assess how lightweight a cryptographic method is, there are two criteria to consider. The first criterion is the cipher's software weight, which is defined by its time and memory complexity. Memory complexity and time complexity both refer to how long it takes the cypher to convert plaintext to ciphertext. Time complexity refers to how much memory is required to complete the ciphering process. The second criterion is the hardware weight of the cypher, which is based on its size and power requirements. The cipher's area is indicated by the quantity of gate equivalencies (GE) utilised to implement it, while the cipher's power consumption is the amount of energy used during execution. The area of a two-input NAND gate is divided by its area (measured in micrometre squared; m2) to get the general efficiency (GE). The algorithm must adhere to lightweight requirements while performing similarly to conventional algorithms in terms of security standards and defence against security assaults. Asymmetric key cryptography and symmetric key cryptography are the two categories into which the current cryptographic primitives fall.

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 were successful in taking advantage of a weakness in the Jeep's firmware update system. |
|  | Tempering | Voice-Controllable System | To connect to equipment like a thermostat, commands based on laser-based audio injection are employed. |
| Software | Botnet DDoS | Malware Attack | IoT devices were once rendered permanently inoperable by BrickerBot. |
|  | Botnet | Silex malware  | Brickerbot deleted the firmware on 2000 Internet of Things devices. |
|  | Botnet DDoS | Mirai botnet  | The Dyn-controlled infrastructure for the domain name system on the internet was brought down by this attack. |
|  | Botnet | Malware attack  | The 500K network routers and network-attached storage devices that the VPNFilter botnet has infected. |
| Data in Transit | Traffic Analysis Eavesdropping/ Sniffing | Sybil attack on Tor Network | Discovered the IDs of website owners using Tor hidden services by taking advantage of a flaw in the Tor protocol. |
|  | MITM Attack Eavesdropping/ Sniffing | Tesla Model S key fob attack | By wirelessly receiving signals from its transmission, a hacker can gain the cryptographic key for the key fob and create a copy of it. |
|  | Eavesdropping/ Sniffing | Target’s data br-each involving IoTHVAC system | The credit card information of nearly 41 million people was exposed in this breach. |

**Asymetric Key Cryptography**

Asymmetric cryptographic algorithms have received some attention from a small number of academics studying lightweight cryptography, but sadly the progress has not yet been as continuous and productive as that of symmetric cryptographic algorithms. Lightweight asymmetric cryptographic methods are frequently neither space or power efficient since they are difficult to operate. These algorithms are getting more exposed as attack models develop. Trapdoor functions like prime and semiprime factorization and the Euler's totient function are commonly used in asymmetric algorithms. The two types of asymmetric algorithms are key distribution algorithms and encryption algorithms. Rivest-Shamir-Adleman (RSA) is one of the best asymmetric encryption algorithms. Elliptical Curve Cryptography (ECC) and Diffie-Hellman provide as good illustrations of asym- metric key distribution techniques. In the context of public key cryptosystems, ECC and the Digital Signature Algorithm (DSA) collaborate to produce a digital signature. Fig. 8.

Algorithm for digital signatures (DSA). DSA outperforms other asymmetric algorithms in terms of efficiency and speed. The method of Additionally, it is challenging to share signatures, and digital signatures only last a short time.

 

Fig. 8 Asymmetric Key Cryptography

**Symmetric Key Encryption:**

Encryption using symmetric keys. Because most operations in symmetric cryptography are based on bitwise functions like XOR and permutations, they are quicker and don't consume a lot of resources. These algorithms are better suited for IoT applications as a result [56]. Between stream cyphers, hash functions, and block cyphers is a crucial distinction in symmetric algorithms. The usual symmetric key cryptography architecture is depicted in Fig. 9.

the stream cypher. the stream cypher. Trivium, Chacha, WG-8, and Espresso are a few examples of popular, light-weight stream cyphers with large throughput gains. Although Grain 128 has a lower throughput, it is more suited as a lightweight cypher for constrained devices . Figure 10 illustrates how a stream cipher's encryption and decryption process works.

The hash functions. Fast computation and reducing output value duplication are two fundamental characteristics of a good hash function. Recent study has looked at several compact hashing operations that might be useful for the Internet of Things. enumerate the applications of the PRESENT block cypher in hashing modes of operation. Spongent, PHOTON, and GLUON are more illustrations of compact hash functions used in research. Figure 11 depicts a has function's typical construction.

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.

Managing the keys. A key management protocol is regarded as secure if it possesses security traits including availability, integrity, confidentiality, authentication, and non-repudiation. There are three categories of IoT key management protocols: distributed, decentralised, and centralised. The Key Distribution Centre, which functions as a server and is consulted prior to communication among group members, is used in the centralised key management protocol. Each group member's encryption keys are distributed by it as well. A decentralised key management protocol can be used to distribute the encryption group key to every group member, preventing a single point of failure. Group members work together to create a shared session key for the dispersed protocols.

**Authentication solutions**

Identification of a device or an individual. This procedure verifies the existence of networked items. From an IoT standpoint, every object must be able to recognise and authenticate every other object in the system or a component of the system with which it communicates. Hardware-based, token-based, non-token-based, and procedural are the four proposed authentication techniques.

Procedure-based authentication. This kind of authentication can be one-way, two-way, or three-way. In one-way authentication, a principal or trusted device verifies the identity of an untrusted entity. An overview of the Physical Unclonable Functions (PUFs) protocol, a one-way authentication method, is shown in Figure 13. Both the trustworthy and the untrusted entity authenticate one another using two-way (also known as mutual) authentication. When a third entity participates in the authentication process of two entities, it is known as three-way authentication and is regarded as trustworthy.

Token-based. Based on a piece of data produced by a server, this technique authenticates an object. When the user enters a legitimate login and password, a token is frequently obtained. An entity can use the resources of the authenticator with the help of this token. OAuth2 and open ID are two protocols that are used to issue tokens. Figure 14 outlines 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

* 1. **Security solutions for IoT platforms**

A software programme that makes it easier for IoT devices on a network to share data and services is known as an IoT software platform. Connectivity and network management, device administration, processing analysis and visualisation, application enablement, security, event processing, monitoring, integration and storage, and data collecting are some of a platform's functions. Four categories can be used to categorise a platform's security solutions: safe data storage, identifying devices that request connections and transfer data, identifying devices sending data while in transit, and authorization of individuals or organisations. Platforms for the Internet of Things can be split into two groups: cloud-based platforms and open-source platforms.

a closed-source IoT platform. IoT closed-source platforms merge end-to-end platform functionality with IoT device and cloud computing as service functionality.

# III. Emerging technologies: challenges and countermeasures

**Machine Learning (ML) security risks**

Even though machine learning systems come in a wide range of designs, they all share a common pipeline that poses certain security risks for each individual machine learning system. The general machine learning system's pipeline is shown in Figure 17. This diagram shows the first nine fundamental elements of any machine learning system: raw data from the entire globe, dataset assembly, datasets, learning algorithm, evaluation, evaluation, inputs, inputs, model, inference algorithm, and outputs. This section lists the dangers connected to each of the nine parts of the general machine learning system. Between the various components, some of these risks are cross-referenced. Additionally, a number of controls are recommended to lessen the security risks brought on by using every machine learning component.

Raw Data in the World: When it comes to security, data in a machine learning system is just as crucial as the learning algorithm and any technical implementation. Here, the term "raw data" refers to all types of data, not just training data that are used in machine learning systems.

 

Fig. 15 a generic machine learning system with attacks

**IV. Blockchain technology security risk:**

The primary security features of blockchain, as outlined in Section V, are transactional privacy, decentralisation, immutability of data, non-repudiation, transparency, pseudonymity, and traceability, integrity, authorization, system transparency, and fault tolerance. Implementing blockchain technology in the IoT poses some security risks or threats, despite these advantageous security characteristics. examined a list of potential dangers to the blockchain's parts, along with the corresponding controls to lessen their effects. Nine (9) elements of blockchain are depicted in Figure 18: system administration, blockchain consensus, blockchain network, membership services, events, ledger, smart contracts, system integration, and wallet.

Transactional privacy, decentralisation, and immutability of data are the three fundamental security features of blockchain. The dangers that each blockchain component faces are covered in this section, along with suggested controls to reduce those risks. Our goal is to create a blockchain that an IoT network can easily integrate without having to worry about security.

Control of a system. The blockchain components can now be created, modified, and monitored thanks to this. There are some security risks associated with this component because of its crucial purpose.

Potential Security Risks:

Transaction Integrity: If the peer node processing the transaction has an account address that is not unique, the transaction's integrity may be compromised. Private keys shouldn't be utilised in another transaction in order to maintain the integrity of that transaction. The public key is often generated using the private key and an ECC method. An attacker with knowledge of the reused private key will be able to ascertain the public key and view the transaction data in its unprocessed state. When a new transaction block is being verified, each peer node must compare the blockchain's stored hash with the hash of the new transaction block. The vulnerability of hash methods like SHA-1 and MD5 was demonstrated by Leurent and Peyrin in 2020.

Blockchain is fault-tolerant, even in the event that a peer node or component fails. But if the peer node that fails is the network node that serves as the gateway's connection point, then there may be a problem. The blockchain would become unusable in the event of a DoS attack on this node. The network's dependability or availability will be impacted by a DoS assault on many blockchains. How many nodes are needed for the blockchain to be deemed reliable in the event that many nodes fail or are intentionally targeted simultaneously?

Monitoring a Single Blockchain Node: Just keeping track of a single peer node to find out how many transactions were accepted, processed, and added to a block to join the blockchain. Information on resource utilisation at the peer node is not provided by this monitoring.

 

Fig. 16 Blockchain Components

The health of other peer nodes or data on the bandwidth, throughput, and latency of the peer network are also not disclosed by this monitoring.

Proposed Controls: The consistency of the data saved in each blockchain block is crucial. A transaction block cannot be deleted once it has been added to the blockchain. In both public and private blockchain, SHA-256 is the predominant hashing function. Having numerous gateways will provide the redundancy that the blockchain network's entry point needs. The effectiveness of the systems is crucial to the blockchain network's health. Use tools to keep an eye on the blockchain's various characteristics. It was suggested that a reputation model be created to score the behaviour of all the consensus nodes in the consensus process, and that faulty nodes would receive a lower reputation if any malicious behaviour was found.

Cryptocurrency Consensus. The replicated ledger is continuously maintained by a group of data and processing peers present on the blockchain. Blockchains use consensus between nodes to choose which new blocks to add to the chain.

# V. Lessons learned

As was already established, there are three main categories of security threats to IoT devices: threats to the hardware, threats to the software, and threats to data in transit. An IoT device that is secure can manage any of these security risks and is sturdy. The security professionals should examine data at rest as another part of security concerns. Due to the development and incorporation of many technologies into IoT systems, this aspect has become apparent. From a security perspective, data that is inactive poses a serious problem. These information could be saved settings for a device with artificial intelligence (AI) or information kept in a database for cloud-based applications. Additionally, the IoT device itself should be shielded from the data that is kept there. any prospective danger. A secure IoT device must protect this type of data.

# VI. Conclusion

The Internet of Things has unlocked a world of limitless opportunities for applications in many facets of society, but it also faces numerous difficulties. Security and privacy issues are one of those difficulties. IoT devices are more vulnerable to security risks and assaults because of their limitations. For IoT applications, there is a shortage of appropriate security solutions, which is causing the internet of secure things to supplant the world of securely linked things. In this review article, we discussed the current state of IoT security and the solutions that must be implemented to convince readers that IoT's reputation is not just about offering inexpensive devices, but also about offering the best security solutions that address security threats and privacy concerns.

Consumers, security administrators, and future IoT developers all need to be aware of the security features of IoT in order to keep it secure. The developer's responsibility is to make sure that security is the top priority while creating a device or programme. In this paper, we evaluated and discussed IoT security threats from a variety of angles (including hardware, software, and data in transit), while also emphasising the need for various security threat prevention measures. Additionally demonstrated is a review of the available security measures. We compare the current hardware security solutions with a focus on delivering security to the IoT-constrained devices in order to analyse the limitations IoT devices face.

The IoT environment is made more vulnerable by the introduction of developing technologies, which affects the security of the entire network. We illustrated the effects of Machine Learning and Blockchain, two of the most significant developing technologies, on security when used in an IoT platform and suggested solutions to reduce these risks. This might provide scholars fresh ideas about how to further 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%2822%2900059-2/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].