**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.

When a hacker uses physical information that is stolen from a system while an application is operating, this is known as a side channel attack. The enemy conducts non-intrusive hardware-based attacks using power consumption, electromagnetic radiations, time data, and sound measures. The acquired data can be analysed to derive private information like cryptographic keys. Techniques for conducting a side channel attack include differential fault analysis, power monitoring, electromagnetic analysis, and key extraction via audio cryptanalysis. The attack's design for using differential power analysis to retrieve secret data from the smart card is shown in Figure 3.

Tampering occurs when an attacker changes an IC's associated data after it has been used in an application. The vast majority of Internet of Things (IoT) devices will be put in settings without any physical defences against an attacker physically gaining access to the device or wirelessly altering the firmware. The attacker can insert malicious hardware or software to change how an IC or device behaves.

A Denial of Service (DoS) or Distributed DoS (DDoS) occurs when attackers tamper with an IC's internal operations to prevent users from using the service.

**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:**
* • To eavesdrop or sniff, an attacker uses a programme or piece of software (such as Wireshark) to record data as it is being transferred. Hackers use technologies created to find and record conversations involving personal information. If a device's security protections are insufficient, an attacker just needs to read or listen to the data collected to obtain useful information. Security flaws that use eavesdropping include sound comber and artificially intelligent assistants like Alexa and Siri. Figure 6 depicts the design of the Sound Comber mobile application.
* • When a hacker steals data packets from an authenticated device, retains them, and then delays or retransmits them later while posing as an authenticated device, this is known as a replay attack.
* • Looking at recorded network traffic and extracting useful data from communication patterns is the process of traffic analysis. Link-load analysis attacks, which are used to gauge the volume of traffic on a network communication channel, and flow analysis attacks are the two types of traffic analysis attacks.assault on connectivity aimed at determining the flow connectivity between a sender and a receiver

• A man-in-the-middle assault occurs when the offender enters the dialogue as a relay or proXy between the sender and the recipient. An attacker in this position has the power to eavesdrop on and alter conversations between sender and receiver. Graph 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.

In charge of the keys. If a key management protocol demonstrates the security characteristics of availability, integrity, confidentiality, authentication, and non-repudiation, it is said to be secure. IoT key management protocols fall into three categories: distributed, decentralised, and central. The centralised key management protocol makes use of the Key Distribution Centre, which serves as a server and is consulted before group members communicate with one another. It also distributes the encryption keys to each group member. To avoid a single point of failure, the encryption group key can be distributed to all group members using a decentralised key management protocol. To build a shared session key for the dispersed protocols, the group members collaborate.

**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

**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.

# Emerging technologies: challenges and countermeasures

**Machine Learning (ML) security risks**

Despite the fact that machine learning systems exist in a variety of forms, they all share a pipeline that presents unique security vulnerabilities for any single machine learning system. Figure 17 displays the general machine learning system's pipeline. The first nine essential components of any machine learning system are represented in this diagram: global raw data, dataset assembly, datasets, learning algorithm, evaluation, evaluation, inputs, inputs, model, inference algorithm, and outputs. The nine components of the overall machine learning system are each associated with a list of risks in this section. Some of these dangers are cross-referenced among the various components. A number of safeguards are also suggested in order to reduce the security risks associated with employing each machine learning component.

Data in a machine learning system is just as important for security as the learning algorithm and any technical implementation, according to the raw data in the world. The phrase "raw data" in this context refers to all sorts of data, not simply the training data used by machine learning algorithms.

 

Fig. 15 a generic machine learning system with attacks

**IV. Blockchain technology security risk:**

Transactional privacy, decentralisation, immutability of data, non-repudiation, transparency, pseudonymity, and traceability, integrity, authorization, system transparency, and fault tolerance are the main security properties of blockchain, as described in Section V. Despite these beneficial security features, there are still security dangers or vulnerabilities when implementing blockchain technology in the IoT. developed a list of possible threats to the components of the blockchain and the accompanying safeguards to mitigate their consequences. Figure 18 shows nine (9) components that make up a blockchain: system management, consensus on the blockchain, network, membership services, events, ledger, smart contracts, system integration, and wallet.

Blockchain's three core security characteristics are transactional privacy, decentralisation, and data immutability. This section covers the hazards that each blockchain component is exposed to as well as recommended safeguards to lower those risks. Our objective is to develop a blockchain that an IoT network can quickly and simply integrate without having to worry about security.

system management. Thus, the creation, modification, and monitoring of the blockchain components are now possible. Given the importance of this component's function, there are some security risks attached.

Security risks that could exist:

Transaction Integrity: The integrity of a transaction may be jeopardised if the peer node processing it has a non-unique account address. To keep that transaction's integrity, private keys shouldn't be used in any subsequent transactions. Frequently, the private key plus an ECC technique are used to generate the public key. An attacker who knows the reused private key will be able to figure out the public key and see the raw transaction data. Each peer node must contrast the hash of the new transaction block with the hash contained in the blockchain while a new transaction block is being validated. Leurent and Peyrin's 2020 experiment exposed the weakness of popular hashing algorithms like SHA-1 and MD5.

Even in the case that a peer node or component fails, blockchain is fault-tolerant. However, there can be an issue if the peer node that fails is the network node that acts as the gateway's connection point. In the event that this node was subjected to a DoS attack, the blockchain would become inoperable. A DoS attack on several blockchains will have an impact on the network's reliability or availability. In the case that several nodes fail or are simultaneously targeted with malicious intent, how many nodes are required for the blockchain to be considered reliable?

Keeping an Eye on One Blockchain Node: Counting the number of transactions that were approved, handled, and appended to a block to join the blockchain by just monitoring one peer node. This monitoring does not offer data on resource usage at the peer node.

 

Fig. 16 Blockchain Components

The results of this monitoring do not include information on the condition of other peer nodes or information regarding the bandwidth, throughput, and latency of the peer network.

suggested controls It is essential that each blockchain block's data be consistent. Once it has been uploaded to the blockchain, a transaction block cannot be removed. SHA-256 is the most popular hashing function in both public and private blockchain. The redundancy required for the entrance point of the blockchain network will be provided by having many gateways. The health of the blockchain network depends on how well the processes perform. Monitor the many features of the blockchain using tools. It was proposed to develop a reputation model to rate each consensus node's behaviour during the consensus process,

The consensus surrounding crypto currencies. A collection of data and processing peers on the blockchain are continuously maintaining the duplicated ledger. To decide which new blocks to add to the chain, nodes in blockchains use consensus.

# V. Conclusion

There are countless prospects for applications of the Internet of Things in various sectors of society, but there are also many challenges. One of those challenges is security and privacy concerns. Due to their shortcomings, IoT devices are more susceptible to security threats and attacks. The lack of suitable security solutions for IoT applications is pushing the world of securely connected things aside in favour of the internet of secure things. In this review article, we discussed the current state of IoT security and the solutions that must be implemented to persuade readers that IoT's reputation is not just about offering cheap devices, but also about providing the best security solutions that address security threats and privacy concerns..

To make IoT secure, consumers, security administrators, and upcoming IoT developers must all be aware of its security aspects. It is the duty of the developer to make sure that security is given top consideration while designing a system or programme. In this work, we assessed and explored IoT security threats from many perspectives (including hardware, software, and data in transit), highlighting the necessity of various security threat avoidance strategies. A examination of the security options is also provided. In order to examine the constraints IoT devices encounter, we compare the available hardware security solutions with an emphasis on providing security to those devices.

The introduction of emerging technologies increases the vulnerability of the IoT environment, which has an impact on network security overall. We presented the security implications of using Blockchain and Machine Learning, two of the most significant emerging technologies, in an IoT platform and offered mitigation strategies. Scholars may get new insights from this about how to advance 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].