Internet of Things 15 (2021) 100420

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws

Ashwin Karale*

Department of Computer Engineering, University of Mumbai, Maharashtra 400098, India

ARTICLE INFO

Article history:
Received 3 January 2021
Revised 18 May 2021
Accepted 8 June 2021
Available online 16 June 2021

Keywords:
Internet of Things
IoT Challenges
Ethical Issues
IoT Laws
Privacy Threats
Security Attacks

ABSTRACT

Internet of Things or IoT is a rapidly growing network of interconnected 'things' embedded with sensors to collect and exchange data over the internet without the need for human intervention. As the applications of IoT continue to skyrocket, it introduces major security, ethical, privacy, and legal challenges that have a substantial impact on our lives. There is a need for a comprehensive overview covering all of these challenges. Therefore, this paper provides a clear overview of the security, ethical, and privacy challenges faced by the common users and examines the current and emerging IoT laws and standards enacted by governments across different countries to combat the vulnerabilities of IoT. Trust and the potential challenges of smart contracts have also been discussed. In addition, the multitude of use cases described in this paper provides an insight into how the threats and vulnerabilities of IoT influence our lives. This study emphasizes a need for globalized IoT laws and that the common user be made aware of the security, ethical, and privacy threats imposed by modern IoT devices. Lastly, this paper identifies the gaps and proposes certain recommendations to direct future researchers.

1. Introduction

It was in 1967 when Lawrence G. Roberts was appointed as program manager for the ARPANET project, the development of internetworking protocols began piecing together a single network known as the Internet- a shorthand for internetworking [1]. The 21st century has seen a massive advancement in technology, bringing the world closer through high-speed internet available on our computers and mobile devices. Let it be texting, calling, shopping, or just surfing the web, everything is within our grasp. We have adapted to this technology which is now considered a 'smart' ecosystem. A terminology called the 'Internet of Things' or IoT, in short makes this possible. With IoT growing as a new business and consumer sector, it exhibits us with immense potential of capabilities.

The concept of IoT was first advised in 1999 by Kevin Ashton, the founder of MIT Auto Identification Centre, 1999. He attributed it to an interconnected network of things connected with RFID i.e., Radio-Frequency-Identification Technology. RFID uses Radio waves and their automation to identify or authenticate objects, collect data, and control the objects. RFID comprises transmitters (tags) and receivers (readers). The tag acts as an identifier that transmits or communicates with the reader through radio waves, thus making RFID imperative for the Internet of Things.

* **Corresponding Author:** Ashwin Karale, Department of Computer Engineering, University of Mumbai, Maharashtra 400098, India. Tel.: +91 98193 94616.
E-mail address: ashwinkarale24@gmail.com

https://doi.org/10.1016/j.iot.2021.100420
2542-6605/

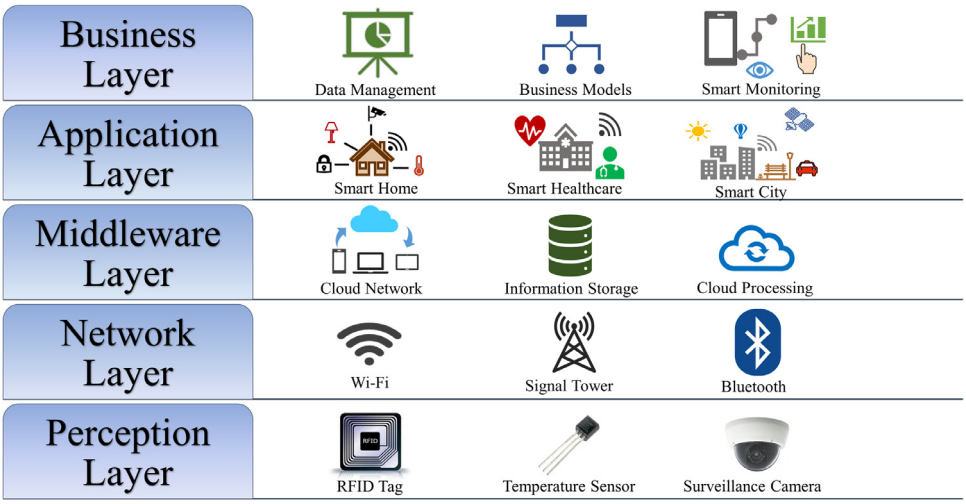

Figure 1. IoT Five-Layered Architecture

IoT comprises billions of intelligent interconnected 'things' in which humans and things can always be connected anywhere and anytime exquisitely by any path or network [2]. 'Things' refer to any object that is an embedded system that can transmit and receive information over a network and has a unique identifier. IoT uses sensors and devices to collect data from the environment. The changes from the surroundings are noticed by the sensor and are sent to a device. Sensors come in a variety of formats depending on the user's needs in passive sensors, active sensors, or thermal, mechanical, electrical, etc. These sensors forward their data to the devices. A device consumes the material and sends it to the cloud for processing. The consumer's device uses a gateway to transmit the data to the network within the cloud. This data is stored in the cloud which in turn makes services and functions accessible [3]. IoT started projecting its growth from half a billion inter-connected things in 2003 to around 25 Billion in 2015. By the end of 2020, IoT is projected to get 50Billion+ things connected to the internet [4].

But, as for all great things comes its downside, which is its limitations and negative adoption. As much as the applications of IoT continually grow in the coming ages to make our lives more comfortable and smoother, the user's security and data privacy persist to be one of the biggest issues for IoT to date. Hackers can hack into data systems and steal user's data or breach a company's database for malicious operations. Hence, the user would want assurance of security for their data to not fall into the wrong hands. For this purpose, the governments ensure the accountability for data flow in the IoT framework by playing a principal role in IoT handling and enacting regulations and laws upon the IoT companies to meet the demands of the users as mentioned above [5].

In contrary to the wide-known benefits of IoT, its downsides are usually not touched upon. Although research has been carried out on the vulnerabilities of IoT like security and privacy, none has focused specifically on providing a comprehensive overview of all the challenges of IoT together with reviewing the concerning laws in place. The contribution of this paper is to provide a clear overview of the security, ethical, and privacy concerns faced by the users and to examine the current and upcoming IoT-related laws and standards enacted by governments across different countries around the globe. Due to limited research highlighting the downsides of smart contracts, the challenges of smart contracts have also been discussed. This paper will identify the gaps and highlight the areas that should be focused upon by laying the ground for future studies and research. The rest of this paper is organized in the following manner: Section 2 explores IoT architecture, applications, and use cases; Section 3 discusses smart contracts and its respective challenges; Section 4 reviews the security challenges of IoT; the ethical & privacy challenges posed by IoT are examined in Section 5; Section 6 discusses trust; Section 7 analyzes the laws implemented by the governments and authorities around the globe concerning IoT; Section 8 presents the discussion and lastly, the paper is concluded in Section 9.

2. IoT architecture, applications & use cases

2.1. IoT architecture

IoT is a complex system, and for all the elements to be laid out ideally, the elements must peace together perfectly in a systematic structure. A robust framework is necessary, and this is where the IoT Architecture comes into effect. Worldwide, researchers have projected a variety of IoT architecture models.

The Five-Layered is a basic model and conveys the main concept of the Internet of Things. Although these scientists do not agree on a single model, the most widely used is the Five-Layered Architecture as shown in Figure 1, this framework

Table 1
IoT Five-Layered Architecture Summary

Layer Number	Layer Name	Description	References	Examples
1	Perception Layer	The Perception Layer is the tangible layer that uses devices and sensors for the collection of data from the environment	[7]	RFID Tags, Sensors, Smart Gateways
2	Network Layer	The Network Layer connects the devices to other smart devices by the transmission of the data to the cloud servers for processing	[7]	Internet, Signal, Bluetooth
3	Middleware Layer	The Middleware Layer links the database and matches services with equivalent requesters as a software layer	[8]	Cloud Network, Information Storage
4	Application Layer	The Application Layer delivers the operation essential services to the user that depicts large scale IoT applications	[7]	Smart Homes, Smart Cities
5	Business Layer	The Business Layer can manage the overall system and this layer builds assorted business models	[8]	Business Models, Monitoring

Table 2
IoT Cloud Systems Architecture Summary

Layer Name	Description	References	Examples
IoT Things Layer	The IoT Things layer for the most part manages information sensing and capturing. Things implanted with sensors and actuators form a part of this layer	[9]	Sensors, Smart Devices
Edge Layer	In the Edge layer, the processing is carried out along the network's edge. This is an intermediate layer between the end-user and the cloud and provides storage and processing functionalities to an enormous number of IoT devices	[9]	Smartphones, Routers
Fog Layer	In the Fog layer, computing is shifted below to the Local Area Network for information to be processed at IoT gateways or micro-data centers likewise	[9]	Fog Nodes, Satellites
Cloud Layer	The cloud layer focuses on big data analytics, industrial level databases, and processing along with data warehousing. All these calculations are carried out centrally in far-away cloud centers	[9]	Cloud Storage, Cloud Servers

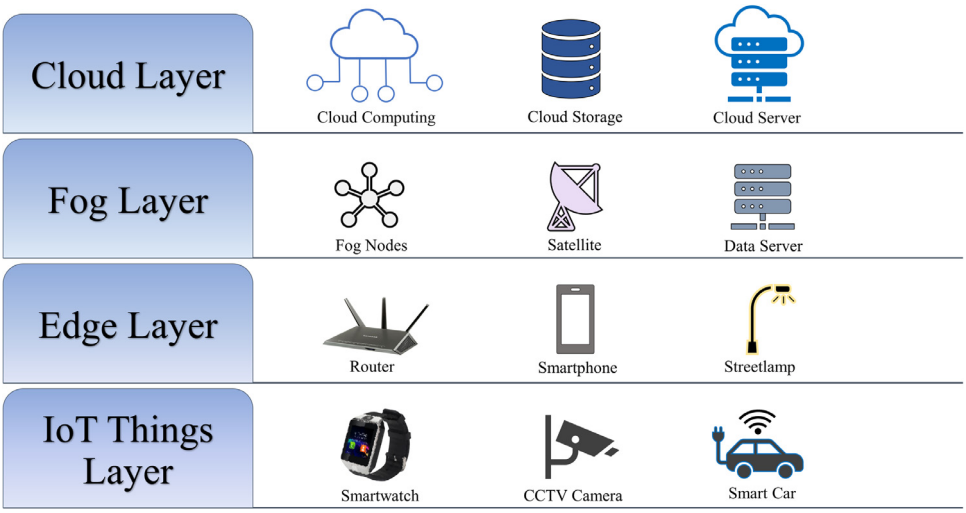

Fig. 2. IoT Fog-Edge-Cloud Architecture

formed the basis of IoT Architecture during the initial stages of IoT development [6]. All the five layers are discussed briefly in Table 1 below.

Researchers have suggested the need to incorporate fog-edge computing with IoT. IoT applications can run with real-time control along with the response time of milliseconds. FEC empowers planning and building a versatile and scalable IoT platform that underpins frameworks requiring solid detecting, analysis, incitation, examination, and control. The Fog-Edge-Cloud architecture of IoT Cloud Systems is discussed in Table 2 below. A pictorial representation of the layers is shown in Figure 2, this FEC architecture inherits the basic engineering of IoT [9].

2.2. IoT applications

IoT has its appositeness in this emerging technological industry. IoT is used in enabling Smart Homes, which makes use of NEST Thermostats, Smart Lighting, Real-Time Automation, Smart TVs, Home pods, etc. remotely, thereby eliminating the need for being physically close to the device. Smart Cities are now a reality, thanks to IoT. IoT optimizes and manages public transport services, street lightings, surveillance of public places, garbage assembly, and much more. Wearables have made life more flexible by incorporating things such as smartwatches, heart-rate trackers, Fitbit, smart wristbands, and so on [10]. It is practiced in the Healthcare sector, to better workflows in clinics and hospitals. The sensors and components of IoT are used for monitoring and improving the estimations of the patient's temperature, pulse, blood pressure and glucose level, cholesterol levels as so forth. IoT is practiced in Smart Agriculture in improving and monitoring soil quality and humidity, control small-scale climates for better crop yields and monitoring water and fertilizer levels, and much more [11]. Likewise, IoT is applicable in Industries. Sensors, software, analytics, and digitalized machinery make the job so much easier. Subsequently, the applications of IoT continue to escalate exponentially and influence our day-to-day life.

2.3. IoT use cases

The majority of the challenges in IoT arise from the domains of Smart Homes, Healthcare, Smart Wearables, Biometrics, Connected Cars, Retail, Smart Cities, and Smart Energy. To spark the discussion of the challenges of IoT, this section will explore the use cases from these domains to illustrate and cover all of the security, ethical, privacy, trust, and legal issues of IoT.

1. Smart Homes

Use Case: AI Assistants

Challenges: Consider the dome of smart homes wherein IoT services like Google Home, Apple Home, and Amazon Echo devices make up the smart ecosystem; whenever we say a phrase like 'Alexa' or 'Ok Google', the device turns on. It turns out that for these devices to pick up on this prompt, they must be listening every time [12]. The device will sure turn on and aid us with the task provided, but it also listens to our private conversations in turn violating our privacy. Also, this raises an array of ethical issues as the user does not have control as to how this data will be recorded or handled.

Use Case: Home Entertainment

Challenges: Nowadays, almost all of the commercially available television sets (TVs) are internet-enabled. Some of these Smart TV companies collect their users' information for evaluating their viewing patterns [13]. The manufacturers use the data for analytic purposes which results in the user's data being sent to and fro from the device to the company without proper encryption. These data collection schemes stem up ethical dilemmas and challenge the user's data privacy. Users view this as a privacy threat.

Use Case: Smart Locks

Challenges: IoT-enabled door locks are not as secure as they seem to appear. Consider, for instance, the user does not update their firmware or their device gets locked. Apart from limited manufacturers that have additional backup plans, the majority of the time the user will simply be locked out and will have to reach out to the device manufacturer creating further hassle. Or for instance, the user's connected app gets hacked. The attacker can now easily access the user's home as per his need. This simple example portrays that IoT can be a major threat to an individual's privacy and security.

2. Healthcare

Use Case: Disease Tracking

Challenges: Disease Tracking has become popular in recent times as a way to limit the damage caused by an epidemic or pandemic by observation and prediction. Take, for instance, contact tracing apps for tracing and limiting the spread of the coronavirus (COVID-19) pandemic. We are all familiar with how these apps work. These apps either use a centralized or decentralized approach. The apps using a centralized approach have greater privacy issues like data breaching, movement & location tracing, and so on. These applications have been found to track and monitor the users without their consent. There are certainly no laws on handling issues as such which is worrying given the fact that these apps are developed by governments and higher authorities. A survey by Sowmiya et al. (2021) [14] found that the major concern of users who use contact tracing apps is privacy (49%). Likewise, the authors also found that contact tracing apps are subjected to major security attacks. This correlates to trust, as to whether the user can trust such apps or not? Unfortunately, given the above circumstances, the answer is negative.

Use Case: Behavioral & Emotion Detection

Challenges: The IoT sector's Emotion detection technology is used in the healthcare industry to improve user emotions [15] or in business sectors for facial recognition. Regardless of the applications, it is a multi-billion-dollar market now.

Despite this, these companies collect and store the user's data without their consent. Another major issue is faulty results; the Association for Psychological Science says that there is substantial room for errors to accurately detect how a person is feeling only using facial and emotion detection. Moreover, the NYU research institute AI Now, in December 2019 called for laws to stop government agencies and businesses from using emotion and facial recognition technology as the foundation of this technology is precarious and poses ethical and privacy risks [16].

3. Smart Wearables

Use Case: Fitness Trackers

Challenges: Smart wearables are the most popular IoT devices. From heart rate monitors, glucose monitors, fitness trackers, GPS, the applications are endless. Take, for example, fitness trackers. IoT enables these devices to track and gather your data, to help you monitor your progress. What most people don't realize is that their data is also stored with the manufacturers of these devices. These wearables transmit highly private information about your health and data. Sadly, these devices are the first to fall prey to potential attackers because they lack necessary security solutions due to their limited hardware resources [17]. To put this into perspective, if you take your tracker with you every day for a run, the attacker can accurately predict and figure out what time will be out and where. Not only the user's security is at stake for this scenario but also their private health data is disclosed. This potential scenario will, unfortunately, lead to the user losing trust in these wearables.

4. Biometrics

Use Case: Biometric Authentication

Challenges: The IoT biometrics system used for authentication like fingerprint scanners, iris scanners, and voice recognition is something that we experience in our daily lives. Imagine for instance, that this data of ours were to be stolen by a hacker. This person will now use this data to pose as to gain access to confidential data [18]. The user's security is now compromised. Besides this, there are numerous ethical and legal concerns as to who owns this biometric data- the individual or the company that accounts for the device? In cases where the individual works with secure or confidential information, should governments and agencies compromise the privacy of the user by tracking their habits?

5. Connected Cars

Use Case: Self-Driving Cars

Challenges: IoT-enabled cars can steer on 'autopilot' without the need for human intervention. This will make life easier, but the negative consequences of this scenario can be detrimental. Consider the 2018 lawsuit filed against Tesla after a fatal crash in autopilot mode killed an individual. This is the fourth person to die when the car was on 'autopilot' mode [19]. This scenario is exactly where these categories of IoT applications draw a thin line on trust and ethics. For one, it may be the driver's conscious mistake or one can argue that it was the machine's fault. Regardless of the answer, trust sure is affected from a negative perspective. Likewise, government intervention in these scenarios does not result in any favorable outcomes as simply current laws fail to keep such sorts of scenarios in check.

6. Retail

Use Case: Shopper Targeting

Challenges: Observing the hike in the retail industry in recent years, and currently due to the pandemic (home-deliveries, social distancing), no wonder that IoT is helping this industry bloom primarily by enhancing customer experience. Consider the 2012 case of Target wherein they mined their customer's data for profiling resulting in a high school girl receiving baby items like clothes and cribs encouraging her to get pregnant even though she was still in high school. It turned out that she was in fact pregnant and had not told her family about it [20]. Now, an immediate question comes to mind that as these companies are collecting information about us so accurately and in sensitive areas as pregnancy, what else do they know about us? The issue in this scenario was that Target and similar companies collect significant data about customers and use it to their advantage. This violates the customer's privacy and will also make the user lose trust as most people will start to worry or over-obsess about choosing what information and credentials should be handed out to these companies and the devices that they manufacture.

7. Smart Cities

Use Case: Surveillance

Challenges: IoT-based smart cities incorporate mass surveillance using real-time monitoring and analytics to enhance public safety. The main problem with mass surveillance is that they pose a threat to the individual's privacy and identity. Imagine for instance, when you come across a CCTV at the local jewelry store, you instantly become self-aware of your actions and become less freewheeling. The same is true for mass surveillance. Citizens tend to act out of time and place when they realize that they're being watched by government agencies and authorities. This prolonged surveillance also

raises privacy issues as information gathered from numerous sources is capable of identifying and labeling the individual. To further heighten the circumstances, there are now laws that protect against privacy infringements caused by CCTV or video surveillance.

Use Case: Smart Parking

Challenges: Smart Parking utilizing IoT frameworks is on the rise. The user receives live updates on the availability of parking spots via a mobile application that enables the user to pick the best spot. This system relies on license plate recognition. Handling of license plates is viewed as private data. As this personal data is being collected, it sets up ethical concerns as to who can demand this data on what grounds. Could police or courts request this data for investigations or court cases? Or whether a reporter and obtain the data for the public interest? Likewise, the individual's identity can be revealed by long-term location tracking. For instance, numerous visits to hospitals can reveal certain health conditions, or visiting political gatherings can uncover the individual's political opinions and so forth violating their privacy [21].

8. Smart Energy

Use Case: Smart Meters

Challenges: Smart meters are IoT devices that have the efficiency to record and report information related to energy consumption, voltage levels, billing, and other corresponding information to the user and the electricity supplier. Although this device is beneficial, it is also frequently subjected to several security attacks like forgery, jamming, or spoofing attacks for a plethora of malicious intentions depending on the attacker. Also, eavesdropping can be used to extract information on which devices are being used at what time such as medical or other appliances [22]. This raises privacy issues as the attacker can also track and figure out the times when someone is at home or not resulting in casualties like burglary or theft.

3. Smart contracts

A smart contract can be defined as a computer program that encodes the arrangement between non-confiding participants that is executed dependent on a set of pre-defined rules. A smart contract is a component of a blockchain transaction that is deployed on blockchain frameworks [23]. Vending machines are referenced as the oldest piece of innovation identical to smart contract execution. Vending machines are independent automated machines that offer services and doll out goods when a form of payment like coins or e-cash is exchanged for the goods. These machines are programmed with specific rules that could be characterized in a contract and can execute such rules [24]. The most popular mainstream platforms supporting smart contracts are Hyperledger Fabric and Ethereum. Smart contracts and blockchain can be applied to IoT for device configurations, the recording of captured data from sensors, and micro-payments [25]. A survey conducted by Panarello et al. (2018) [26] examines the integration of blockchain in the context of IoT. According to the authors, the research involving IoT and Blockchain is in its early stages, a great amount of research needs to be done to cover the specific domains of IoT. And as of 2021, the research covering IoT-specific domains still remains unexplored to a great extent.

3.1. Security

The security of smart contracts is substantially important considering that even a single bug can prompt huge issues like exposed privacy and loss of money. For instance, the Decentralized Autonomous Organization (DAO), Ethereum was under attack in June 2016 because of a bug in their code that resulted in a loss of 60 million USD. A survey by Rouhan and Deters (2019) [25] reviews the four primary vulnerabilities of Smart Contracts. They are discussed briefly as follows:

1. *Transaction Ordering Dependence (TOD):* In Ethereum, if more than one transaction is invoked by the same contract, the new state of the blockchain is affected by the order of these transactions.
2. *Timestamp Dependence:* Block timestamps can be manipulated by the attackers as they are set by the miners dependent on their local system time.
3. *Mishandled Exceptions:* In the event that an exception takes place in the called contract, it returns and terminates and may fail to alert the caller contract.
4. *Reentrancy Vulnerability:* During contract calling, the execution of the current contract has to pause until the called contract concludes. This gives a chance for the attacker to abuse the intermediate state of the caller contract to call its methods multiple times.

Likewise, a survey of potential attacks on Ethereum contracts by Atzei et al. (2017) [27] listed 12 vulnerabilities that are allotted by context to EVM, Solidity, and the blockchain characteristics itself. The attacks presented highlighted the typical cause of insecurities in smart contracts to be the difficulty of distinguishing their intended behavior and the real one. Most of these vulnerabilities can be tended to by following accepted procedures for composing secure smart contracts, which are dispersed all through the Ethereum community and online Ethereum blogs [28].

3.2. Privacy

The user's privacy is a significant challenge in smart contracts, especially while implementing smart contract applications. During transactions, the user initiates the function calls that are processed by the miners- the blockchain's nodes. This can potentially be dangerous as sensitive and confidential data like voting data, medical records, or power consumption data could be leaked endangering the individual's privacy [29].

In order to combat these privacy issues, frameworks like Hawk, Enigma, and Trusted Execution Environment (TEE) have been developed. These frameworks are discussed briefly below:

1. *Hawk:* This framework has developed to create smart contracts that preserve privacy. Hawk receives a smart contract and a cryptographic protocol is automatically generated by its compiler. Privacy is ensured considering that the manager does not uncover the private portion.
2. *Enigma:* Enigma is a Ethereum based decentralized computation network. Privacy is ensured alongside computation to permit parties to share and store private data.
3. *Trusted Execution Environment (TEE):* TEE is able to ensure privacy alongside superior execution for sensitive and private information regarding smart contracts [25].

3.3. Laws

As the applications of smart contracts continue to flourish, they won't be helpful if they are not enforceable legally. Contract law is a convoluted area in the domain of laws as conflicts often emerge over the understanding of terms. The principles of contract law trace all the way back to medieval England. Looking at the current age, the laws like UETA and ESIGN take into account smart contracts to be authorized. Hereby, blockchain-based smart contracts ought to be viewed as a legally binding statement under the UETA and ESIGN laws, and subsequently, be available for novelty and development now [30].

Currently, an international framework explicitly intended for smart contracts does not exist. Arguably, the fact that there's a lack of specific guidelines for smart contracts does not imply that the current legislation does not apply to them or that they are unregulated by any means. Smart contracts face similar issues as conventional contracts in deciding legality as the contract would be interpreted voidable if the contract would be executing illegally. Hence, the currently existing contract law frameworks are adequate to integrate smart contracts without the necessity to forge new legal divisions [31].

4. IoT security

One of the greatest challenges forestalling the growth and implementation of IoT in our lives is security. The security of IoT devices is compromised due to the poorly secured nature of these interconnected devices. Tending to these challenges and guaranteeing security for the user must be of utmost priority. As these innovations are evolving and integrating into our daily lives, the users need to believe and trust in these devices and that their data is secured [32].

4.1. Security attacks

The credits of numerous IoT applications pose unique and advanced security challenges. The full spectrum of security attacks is explored in this section categorized under four major types.

Physical Attacks

1. *Node Tampering:* Attackers use Node Tampering by materially having the complete node or a part of it like the Key Node replaced or taken under control to leak information [33].
2. *Malicious Code Injection:* A Malicious Code Injection is performed by injecting malicious code into the sensor by using a USB stick for instance and gaining control of the user's info.
3. *Malicious Node Injection:* The attacker installs another malicious node interconnecting the original nodes of the IoT system, thereby accessing the data between the nodes [34].
4. *Sleep Deprivation Attack:* The attacker can disturb the sensor's sleep cycle which it employs to enhance its battery life by causing it to stay awake hereby draining its power and inducing a shutdown [35].
5. *Physical Damage:* Attackers can directly damage the IoT component like sensors and tags. For example, at shopping malls, shoplifters can remove, damage, or replace the tags as per their vicious motives [36].

Network Attacks

1. *RFID Spoofing:* The intruders can manipulate RFID tags by carrying out onslaughts such as RFID Spoofing, by successfully imitating legitimate RFID tags [37].
2. *MITM Attack:* The attacker gains access to two nodes thereby controlling and modifying the communication between them remotely.
3. *RFID Unauthorized Access:* The attacker is able to wield the tags and modify it as per their demand as they are accessible by everyone.

Table 3
Summary of IoT Security Attacks and their Layers of Occurrence

Attack Type	Attack Name	Attack References	Layer
Physical Attacks	Node Tampering	[33]	Perception Layer
	Malicious Code Injection	[34]	
	Malicious Node Injection	[34]	
	Sleep Deprivation Attack	[35]	
	Physical Damage	[36]	
Network Attacks	RFID Spoofing	[37]	Network Layer
	MITM Attack	[38]	
	RFID Unauthorized Access	[38]	
	Sinkhole Attack	[38]	
	Traffic Analysis	[39]	
	Sybil Attack	[39]	
	Eavesdropping	[39]	
	Flooding	[40]	
Encryption Attacks	Side-Channel Attack	[41]	Middleware Layer
	Cryptanalysis Attack	[41]	
Software Attacks	Social Engineering	[42]	Application Layer
	Viruses and Trojans	[43]	
	Malicious Scripts	[43]	
	Phishing Attack	[44]	
	DoS Attack	[44]	
	DDoS Attack	[44]	
Software Attacks	Business Logic Attack	[45]	Business Layer
	Zero-Day Attack	[45]	

4. *Sinkhole Attack:* All the traffic from the wireless sensor nodes (WSN) is directed to one point which leads to dropping the packets instead of it reaching their original destination [38].
5. *Traffic Analysis:* Hackers can collect valuable information by deciphering and analyzing communication patterns from messages using Traffic Analysis.
6. *Sybil Attack:* Social media networking sites are falling prey to *Sybil Attacks* wherein a single node can have multiple identities meaning the intruder can be at multiple locations at a given time.
7. *Eavesdropping:* Intruders can listen in on conversations, interpret the messages and read them [39].
8. *Flooding:* The attacker repeatedly floods the IoT system with new connection requests until it has reached its capstone [40].

Encryption Attacks

1. *Side-Channel Attack:* This attack involves the handling of information produced by encryption devices to retrieve the key which the device is using.
2. *Cryptanalysis Attack:* Poorly encrypted devices are subjected to Cryptanalysis Attacks wherein the goal of the attacker is to retrieve the plaintext by finding the encryption key by zeroing in on the ciphertext and then breaking the encryption [41].

Software Attacks

1. *Social Engineering:* The attackers use an attack flow to exploit the cyber vulnerabilities in the IoT system, and by using attack vectors they can gain unwarranted access to the system. They can infect the system with attack vectors like Social Engineering [42].
2. *Viruses and Trojans:* Malware like Viruses and Trojans can get into the system and lead to an array of outcomes such as tampering, stealing the data, and so on.
3. *Malicious Scripts:* Malicious Scripts can exploit the vulnerabilities of the user's system [43].
4. *Phishing Attack:* The user can fall prey to phishing from fake emails or websites.
5. *DoS Attack:* A Denial of Service (DoS) attack can be launched giving the attacker full access to the application layer and conjointly denying access and blocking legitimate users.
6. *DDoS Attack:* A Distributed Denial of Service (DDoS) attack is similar to the DoS attack and works by conjointly denying access and blocking legitimate users [44].
7. *Business Logic Attack:* The intruder takes advantage of the programming, validation, or encryption flaws in the business layer and earns access to the information passed on between the user and the application database.
8. *Zero-Day Attack:* This attack capitalizes a security hole or an issue within the application without the user's knowledge or approval [45].

A summary of the IoT security attacks and their layers of occurrence is demonstrated in Table 3.

5. IoT challenges

5.1. Ethics

Ethics was first established in the 3rd century BC by Aristotle as a philosophical discipline. It stemmed up from the words 'Ethica Docens' which meant teaching a philosophical reflection about critical and analytical action [46]. Ethics may be considered as a Science of Conduct. We guide and define our behaviors via moral values, ethical principles are how these values are applied- whether they are right or wrong, just or unjust, is what is incorporated into ethics [47]. In the realm of IoT, ethics is concerned with the legitimate regulation of human activities towards themselves and others, meaning they define what is right or wrong and good or bad correspondingly.

5.2. Ethical issues

There are certain challenges and issues posed in the ethical domain of IoT. They are derived from the central ICT ethical issues comprising *accessibility, privacy, property*, and *integrity of information*. The primary ethical issues are examined in this section.

1. *Difficult Identification*: Objects need to be identified to connect to IoT. The data collected by these innumerable objects makes it difficult to identify the owner of the particular object accurately. Collecting this data without the user's consent needs to be addressed in the IoT system as it is a significant issue.
2. *Ambiguity*: The growing number of IoT objects makes it difficult to identify and set system boundaries as the contrast between natural and artificial artifacts and beings diminishes as one category can easily transition into another due to the advances of technology.
3. *Unpredictable Behavior*: As humans are getting integrated into the IoT environment of things, devices, and artifacts, these interconnected things may instinctively interfere in their everyday tasks unexpectedly, hereby changing the scheme of events [48].
4. *Public and Private Border Line*: Due to the absence of clear-cut boundaries, the IoT system may fail to distinguish between public data and private data as both are collectively collected by the sensors [49].
5. *Difficult Control*: Due to the consistently expanding number of devices, hubs, switches, and data, centralized governance and control will be ceased. As the amount of information continues to rise, the data transfers will become much quicker and more economical as per the demand which will result in a lack of control that leads to further susceptibilities [48].
6. *Life Threats*: A breach in the IoT network can harm our lives directly as we share a collective environment with the IoT system. For instance, a data breach in a Smart Home can cause thermostat fluctuations putting individuals at risk towards abnormal temperatures, likewise, a breach in a Smart Car may prompt misinterpretations and errors relating to street mishaps [49].

5.3. Privacy

The definitions from the Oxford Dictionary Online and Princeton University recognize two principal parts of privacy; the first alludes to the affected individual and the option to build up a separate space, and the second to the public and the limitations of others admittance to the individual's space. These definitions cooperate to figure an idea of a boundary between an individual and the surrounding area, centering on the delimitation of the individual's boundaries which portrays the idea of privacy [50].

The growth of IoT is consolidated into most uses of our life such as phones, home appliances, sensors, automobiles, smartwatches, medical monitoring devices, and large-scale foundation frameworks. Retaining our privacy becomes a troublesome errand due to this colossal amount of information. As these frameworks continue to grow, they raise privacy issues as these gadgets have their control and monitoring methodologies digitized and associated with the Internet. Hackers can penetrate through critical information effortlessly as it is accessible through the internet. This will lead to casualties as the victim's data is exploited [51]. Hence, the issue of guaranteeing appropriate insurance for the user's privacy is essential.

5.4. Privacy threats

Threats that violate the user's privacy leads to potentially adverse effects. The most widely recognized privacy threats are reviewed in this section.

1. *Identification*: The most prevailing threat associates an identifier, for instance, name, address, personal data with the user. This process termed Identification can empower and provoke other threats like Profiling and Tracking. The user can primarily be identified by camera surveillance, fingerprinting, and speech recognition mechanisms. This newfound identity can be associated with a particular privacy-disregarding setting which is a potential threat to the user's life [52].

2. *Social-Based Personalization*: The exponential growth of Social Media Companies over recent years has made a tremendous online vault of real identities. They store rich data about their users, including genuine names, emails, friend lists, socioeconomics, individual photographs, location, and so on. They utilize this data for customizations, search, and internet showcasing. Due to the impact of these networks on our current lives, individuals are frequently ready to uncover more private data than normal. This leads to unwanted circumstances. In 2008, 8% of U.S. organizations employing 1000+ workers had terminated an employee due to unwanted information being released into social media. Large companies permit third-party applications to get to their users' profiles through an Application Programming Interface. Hackers can access the victim's social information through the API easily which compromises their privacy.
3. *Behavioral Profiling*: Behavioral profiling is the act of gathering long-term information about the user's activities and personalizing the user interface from that data. This act has become popular over recent years in web-based search, internet ads, and e-commerce companies. As mentioned earlier, behavioral profiling tracks a wide scope of user actions over a long period of time using browser cookies with practically zero consent of the user. This induces unsolicited marketing. Besides, for promoting products using advertisements, companies like Google connect behavioral profiles to their server accounts for the ads to be shown across computers and mobile devices, resulting in a likelihood of other people gaining access to the user's personalized and private content [50].
4. *Privacy-Violating Interaction and Presentation*: Privacy-Violating Interaction and Presentation relies on passing private data through a public medium and in action uncovering it to an undesirable crowd. Many IoT services are based on substantial user interaction. These interaction and presentation system can be observed by people in the region as it is public. Personal information and private data can be traded by this system and the inherent user which can put the user's private data at stake. In a smart city, for instance when the user may ask for directions to a specific restaurant or medical clinic, if the information is displayed on a nearby public presentation display, visible to the bystanders, now potential delinquents may take notice and use that information for their acquisitions [52].
5. *Location-Based Personalization*: As the technology industry continues to advance, wireless fidelity and GPS services are becoming more and more accurate. This has led to the development of mobile applications that can track the precise location of the user using effective application programming interfaces and frameworks to offer location-based offers at that specific location [50]. A survey by Tsai et al. (2003) [53] computed the likelihood of location-based harms. They found that annoying advertisements, the intrusion of private space, the revelation of the user's house, revealing private activities, being stalked, and being spied on by the government were the top reported concerns.
6. *Localization and Tracking*: Like Location-Based Personalization, Localization and Tracking follows the danger of recording the user's area and location. This is achieved with the help of Identification wherein the user is associated with an identifier. This threat violates the user's privacy when they do not have a command over their location data and are unaware of its revelation. The growing passivity of data collection mechanisms has led to the unawareness of the users as to when they are being followed and tracked. Another challenge includes data trails by revealing the user's identification in addition to their location and activity being tracked hereby putting them at unwanted risk [52].
7. *Lifecycle Transitions*: When IoT items are sold, used by their proprietor, and finally disposed of, the user assumes that all the data is erased by the object. In reality, these smart devices frequently store enormous measures of information about their own history and set of experiences all through their whole lifecycle. This is regarded as a Lifecycle Transition. As the ownership of the device is transferred to another user, the original data of the first user including private documents, photos, and videos may still be existent. This could result in disclosing sensitive information of the user and violating their privacy [54].
8. *Inventory Attacks*: Inventory attacks allude to the unapproved assortment of data about the presence and attributes of individual things. Counterfeit gatherings can query and manipulate this to assemble a stock inventory of things at a particular location. Burglars and criminals can utilize this inventory data for focused break-ins at people's houses, workplaces, factories, and so on. Also, law enforcement and different specialists could utilize this attack to lead unwarranted searches. This leads to the disclosure of private information on things deemed as personal interests.
9. *Linkage*: The danger of Linkage comprises connecting distinctive already isolated systems with the end goal that the combination of information sources uncovers data that the subject did not uncover or did not have any desire to reveal to the previously secluded sources. The dangers of unapproved access and breaks of private data increments when frameworks work together to consolidate information sources by bypassing privacy and security protection systems. Lastly, privacy can be violated by the Linkage of information sources and frameworks by re-identification of anonymized data which possesses additional threats [52].

6. IoT trust

Trust is one of the most important aspects of building and maintaining relationships. A lack of trust can cause the relationship to fail or break. As we know, the Internet is hardly associated with 'trust' or 'trustworthy'. The common people are becoming increasingly aware of the negative aspects of the Internet and technology in general. This lack of trust causes people to be more mindful of their data and to try to avoid or limit exposure to the Internet. But that task is rather impossible in today's age [55]. A survey by Allhoff and Henschke (2018) [56] discusses the foundational ethical issues of IoT. The authors argue that trust is reliant on ethical issues like privacy, informed consent, information security, and physical safety and that these issues exist as concatenation and integrate into myriad ways. This is essential to recognize as when there's

a breach in the user's data, their privacy and security are compromised and informed consent is disregarded. This leads to trust issues amongst the user which in turn can spark a series of questions in the user's mind as to who or what can they trust? or how trustworthy is this particular organization or object? ultimately causing the feeling of panic and insecurity amongst the individual.

Trust dictates the world of IoT alongside as these smart 'things' are being incorporated into our daily routines increasingly. For users to rely confidently on IoT and smart devices, they need to first make sure that these components are trustworthy. They need to believe and trust these devices that their data is secured. To combat this problem of 'untrustworthy' devices, various Trust Frameworks are being incorporated into the markets. These frameworks can be a potential step to bridge the issue of trust. Trust can be deciphered by trading 'assurance' by the involved parties. The U.S. government now plans, fabricates, and deploys Trust Frameworks [57]. Similarly, governments can enact laws to protect their citizens which in turn will allow the users to trust these smart devices knowing that there are laws enacted in their favor.

7. IoT laws

Having a legal framework can diminish potential user risks and ensure a proper flow of the IoT markets. The users will also feel secured as they can trust and rely on this structure of laws in their favor [58]. To ensure security and protection to the user that their data is secure and kept private, the authorities should consolidate distinctive existing laws like the Electronic Communication Privacy Act and other laws like HIPPA, FIPPS and enact new laws that target IoT directly and can minimize the risks and unwanted hostile activities [59].

7.1. Review of IoT laws worldwide

This section will discuss the current laws and standards of nations that extend to IoT. These laws are enacted by individual countries to protect their citizens from the vulnerabilities and threats of IoT.

7.1.1. Asia

India: In India, a particular law planned for Data Protection is non-existent. India's *Information Technology Act, 2011* deals with the affairs of data protection. Under this act, *Section 43A* commits corporate elements to maintain sensible security practices to shield the individual's private data. *Section 72A* ensures the right to privacy and deems the disclosure of the individual's private information without their consent as a punishable offense. Both the sections referenced above do not deal with data protection directly. A set of rules called *Information Technology (Reasonable Security Practices and Procedures) Rules, 2011* characterize individual information and expand on the means to gather and hold such information [60]. However, these rules are inadequate against the enormous data gathered by the IoT system. India does not yet have a committed law overseeing IoT and its operations. India has issued the *Draft Policy on Internet of Things* to make an administrative system and a policy for utilization of IoT in India by different companies and stakeholders. This policy issues a governance structure that incorporates a legal framework, an advisory committee, and a governance committee for providing guidance and to take decisions on the extent of IoT [61]. But this policy is inadequate as it fails to sufficiently cover the extent of IoT activities and to maintain a governance structure for the same. The legal groundwork for IoT in India is lacking in development and not enough to meet the current challenges and threats posed by IoT. A review by Kethareswaran (2017) [62] surveyed the current state of the laws and policies geared towards IoT by the Indian government. The paper implies that the current laws and policies are not assuring enough to counter the vulnerabilities of IoT. The legal structure must be upgraded to meet the current necessities. Up to date, there has been no advancement by the Indian government to enact a law or draft a policy specifically to target the threats of IoT.

China: In 2017, China put forth its primary Cybersecurity Law titled *Cybersecurity Law of the People's Republic of China* in which came into being on 1st June 2017 and covers the preservation and protection of personal information, legal liabilities, operators' commitment for their behaviors, and so forth [63]. Following this, they put forth the *Information Security Technology – Personal Information Security Specification* in May 2018. A revised version of the Specification has been enforced from 1st October 2020. This bill covers privacy policies that enterprises have to follow, enhances the protection of biometrics, and consents along with other recommendations regarding the compliance system that adheres to their Cybersecurity Law [64]. China also has several important laws covering cybersecurity and information security like:

- *CAC: Administrative Measures on Internet Information Services*
- *CAC Rules on Security Protection for Critical Information Infrastructure*
- *Cyber Sovereignty*
- *Security of Product and Service*
- *Security of Network Operation (Classified Levels Protection, Critical Infrastructure)*
- *Data Security (Category, Personal Information)*

Although these laws do cover digital security and IoT indirectly, they do not address specific countermeasures to combat vulnerabilities and threats particularly provoked by the Internet of Things. As of now, there are no laws or guidelines that outline data ownership of data produced by IoT devices. The legal rights on the utilization of this data are still a subject of discussion.

Japan: T*he Act on the Protection of Personal Information (APPI)* was enacted in 2003 regarding data protection. This took a hit in September of 2015 as a series of eminent data breaches took Japan by storm thereby making the APPI seem outdated. In response to this. Japan put forth an amended *APPI* on 30th May 2017. This APPI extends to all business operators to adhere to strict guidelines incorporating the handling of personal data and states the penalties against future data breaches [65]. Japan also released *The Basic Act on Cybersecurity* in November of 2014. This act set the basic standards of cybersecurity policies alongside explaining the duties of the citizens, private and governmental firms. It also laid out a framework for cybersecurity policies [66]. Alongside, Japan also released a *Cybersecurity Strategy* in July of 2018 intending to enhance economic vitality and a secure society for its citizens. This strategy also touches on the vulnerabilities of IoT by addressing international standards and improving the structural framework of IoT. It also highlights the need to prepare vulnerability countermeasures for IoT [67]. Although, there ' haven't been any specifically planned countermeasures for IoT published by Japan yet.

United Arab Emirates (UAE): The UAE published its *Regulatory Policy titled Internet of Things (IoT)* on 22nd March 2018. This policy encompasses data protection guidelines consisting of storage limitation and data minimization; it enforces high encryption standards that the IoT companies should meet and provides Type Approval regulations and penalties against the policy [68]. By UAE taking a step forward in establishing a legal policy for the IoT ecosystem, other Middle East nations have also begun working on and developing their own policies concerning IoT.

7.1.2. Europe

European Union (EU): The EU has consistently been ahead of the world regarding tending towards privacy and protection concerns of its citizens. They published the *EU Regulation 2016/679* on 25th May 2018, in which they issued a set of rules catering towards informed consent covered in *Article 4(11), Article 6(1)(a),* and *Article 7*. Within the same regulation, *Article 35* focuses on the assessment of impacts regarding data protection; *Article 50* focuses on the term international cooperation and *Article 80* is geared towards efficient judicial countermeasures for organizations and firms [69]. Europe has put forth three directives that cover cybersecurity. They are- *EU Directive 2013/40* that deals with cybercrime [70]; *EU Directive 2014/53* that deals with radio equipment handling [71] and *EU NIS Directive 2016/1148* that deals with cybersecurity [72]. It is noteworthy to mention that none of these three directives mention IoT or its vulnerabilities directly. The EU put forth the *General Data Protection Regulation (GDPR)* on May 25 2018 a broad step towards data protection under which most of these types of issues fall. The GDPR implies a strict exacting cycle that IoT manufacturers have to follow throughout the lifecycle of the IoT device. It has a separate section covering the machine-to-machine area extending the privacy laws towards machine data as well apart from private data. Moreover, the GDPR ensures a smooth flow of information within its territory and gives guidelines to companies towards hiring a Data Protection Officer who looks over data protection and security concerns [73]. EU's new *Cybersecurity Act* of 2019 will fortify the capacity of the European Union Agency for Network and Information Security or ENISA to aid the member states to address the cybersecurity risks. This act addresses IoT devices by urging authorities to take action against the vulnerabilities of IoT [74]. EU's *ETSI TS 103 645* standard based on the UK's *Code of Practice for Consumer IoT Security* touches upon the cybersecurity of user-related IoT devices. It includes a list of provisions to regulate and boost the user's digital security and privacy [75]. Apart from this, the EU also created the *ePrivacy Regulation (ePR)* that will replace the *ePrivacy and Electronic Communications Directive* of 2002. The ePR was set to release on the same date as the GDPR on the 25th of May 2018 but has yet to be implemented. The ePR focuses on data privacy as compared to the GDPR's data protection. The ePR covers over-the-top services, cookies, spam marketing, public Wi-Fi, and IoT. It ensures and promotes a secure electronic communication of information in the IoT system incorporating IoT networks and IoT devices [76].

UK: The Government launched a proposal titled *Regulatory Proposals on Consumer IoT Security* in May 2019 and published a response to the consultation on this same proposal a year later on 27th January 2020. This policy is targeted towards the improvement of the user's data under IoT security and aims to ensure strong cybersecurity built into the IoT devices before the user gets a hold of the device. The UK Government will be able to achieve this by ensuring that the manufacturers must make sure of a unique and strong password to be set, they must ensure a public purpose of contact for reporting vulnerabilities, and a base time of potential security updates should be mentioned at the time of purchase [77]. The Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), published the *Code of Practice for Consumer IoT Security* in October of 2018. It distinguishes 13 priority principles that manufacturers, developers, and retailers ought to follow when they produce and supply IoT services. These principles aim to safeguard user security and privacy, simplifying their safe use [78].

7.1.3. The United States

The US issued the *Federal Privacy Act* of 1974 which indirectly applies to IoT data usage. The *Health Insurance Portability and Accountability Act (HIPPA)*, 1996; the *Children's Online Privacy Protection Act (COPPA)*, 1998 and *Electronic Communication Privacy Act (ECPA)*, 1986 are geared towards regulating Data Privacy. Unfortunately, these laws were not composed in light of IoT, as IoT had yet to be introduced during the enactment of these laws [79]. The US Federal Trade Commission founded on 26th September 1914 looks over consumer protection. This includes cybersecurity and malpractices in the IoT ecosystem [80]. On the 1st of January 2020, California put forth their IoT Law in *Senate Bill No. 327* which is the first law catered specifically to IoT in the US. This bill goes over the IoT devices that are sold in California to be met with reasonable security features by the manufacturers [81]. Following this, Oregon passed *House Bill 2395* that took effect from January 1st, 2020.

Based on California's SB 327, this bill requires manufacturers that sell internet-enabled devices in Oregon to outfit the gadgets with "reasonable security features" intended to ensure against unapproved access, disclosure, or destruction. However, this bill only focuses on home devices [82]. This bill mirrors the country's developing attention to the significance of security and privacy guidelines. The U.S. Department of Commerce's federal laboratory, the National Institute of Standards and Technology (NIST) put forth the *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* in June 2019 which is an introductory report on cybersecurity risks and mitigation measures incorporating IoT targeted towards federal and private companies and establishes a foundation for a planned distribution of reports concerning similar matters [83]. Following this, in May 2020, the NIST put forth their final draft report titled *Foundational Cybersecurity Activities for IoT Device Manufacturers* which contains recommended voluntary activities intended for manufacturers should follow before implementing their respective IoT gadgets [84]. Moreover, US Congress put forth the *IoT Cybersecurity Improvement Act of 2019* on March of 2019 that aims to increase cybersecurity by influencing the Federal Government's procurement power. It aims to reinforce the cybersecurity requirements of IoT devices on a broader spectrum [85]. The UL Safety Test Institute presented an IoT Security Rating with five distinct degrees of security, namely Bronze, Silver, Gold, Platinum, and Diamond in late 2019. This assessment cycle surveys basic security parts of smart devices against regular attack mechanisms on IoT devices to build a security baseline [86]. This will allow users to make better purchasing decisions and create transparency in the IoT market. Although security experts question the validity of these ratings and that these ratings may contribute towards a false sense of security.

7.1.4. Australia

The Australian Government established the *Cyber Supply Chain Risk Management* in November 2019 and the Critical Infrastructure Centre established the *Best Practice Guidance Supply Chains*. The former is geared towards mitigating risks in the cyber supply chain while the latter provides guidance for critical infrastructure operators to manage and mitigate foreign involvement risks [87,88]. Although these two publications cover cybersecurity, they do not cover IoT directly. Following this, a code of practice labelled *Securing the Internet of Things for Consumers* was released in November 2019. This Draft Code contains 13 principles directed towards the IoT system. It focuses on software and communication security, strong password encryptions, secure software updates, and suggests a vulnerability disclosure policy to be used by firms in practice [89]. This draft code put forth by Australia is the only legal document geared directly towards IoT and has the potential of becoming an accepted norm despite it being non-mandatory.

7.1.5. Latin America

Brazil: In June of 2019, the government established the *National Internet of Things Plan*. It is a result of Brazil's sustained endeavors to expand the adoption of IoT for socio-economic profit. This plan is a push to utilize IoT to drive a technological revolution across the economy of Brazil [90]. This plan is the first law that addresses IoT directly but there is a lack of emphasis placed on how to combat IoT's vulnerabilities as more emphasis is placed on the development of IoT.

Argentina: In 2017, Argentina dispatched a *Public Consultation on IoT* to cultivate the improvement of the IoT. The need for IoT regulations and increased security was also discussed but the main aim was to promote the development of IoT [91].

Chile: Chile's primary data protection *Law 19.628* also called the Chilean Data Protection Law or CDPL focuses on privacy protection. Another regulation *Article 19 No. 4 and No. 5* of the constitution addresses data protection to a degree and *Law 19.496* is the Consumer Protection Law also touches on private data processing [92]. There hasn't been a dedicated law for IoT nor it has been addressed directly in any of these data protection laws.

Thus, considering the status of the laws of these countries, the Latin American nations have various levels of growth and this sets up a tremendous deviation between the domestic legal structures. As the level of IoT advancement has not yet flourished in these nations, there have been no laws that address the threats of IoT but instead, a few laws that gear towards driving up the development of IoT as witnessed above.

7.2. International laws and standards

This section discusses the laws covering IoT on a global level wherein several nations have enacted laws and standards together to protect their citizens on an international level.

Statement of Intent Regarding the Security of the Internet of Things: From 29th to 31st July 2019, the representative ministers from five countries including Australia, Canada, New Zealand, the United Kingdom, and the United States of America, the Five Eyes partner nations signed the *Statement of Intent Regarding the Security of the Internet of Things* to discuss the security and cybersecurity threats posed by IoT and to protect their citizens from these threats. The representatives of these 5 countries acknowledged that the growing spur of IoT devices poses significant vulnerabilities and various security and privacy issues and that the safety of their citizens is the topmost priority. They agreed to collaborate and work together to implement and maintain laws ensuring the improvement of the security of IoT devices and to encourage like-minded nations to engage and contribute towards improving IoT security [93]. This is the only legal document that enforces laws on IoT on a truly international level to date apart from international standards. Although the nations agreed to encourage like-minded nations to contribute, there has been little involvement by other nations so far. A new global law covering IoT has yet to be implemented by these nations together as they had discussed in their statement.

International Standards: These standards are developed by international organizations can provide individuals and organizations a universal stand on IoT security. Four organizations that majorly contribute to the field of IoT with their standards. They are the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), and the Institute of Electrical and Electronics Engineers (IEEE). A review by Miloslavskaya et al. (2019) [94] reviewed all of the current international standards addressing IoT set by these organizations. The complete list of these standards along with a brief description of each is given in Table 4 below.

In addition to these, ISO together with IEC has published more new standards and a few are still under development. They are covered here as follows:

1. *ISO/IEC 21823-1:2019*- This standard gives an outline of interoperability as it applies to IoT frameworks. It empowers peer-to-peer interoperability between independent IoT frameworks [95].
2. *ISO/IEC 23093-1:2020*- This standard portrays the architecture of frameworks for IoT. It also determines application programming interfaces (APIs) and packed portrayal of the data flowing in IoT [96].
3. *ISO/IEC 21823-2:2020*- This standard describes transport interoperability interfaces in order to empower the development of IoT frameworks with data exchange, distributed network, and consistent communication between IoT frameworks and within the system likewise [97].
4. *ISO/IEC TR 30164:2020*- This standard depicts the basic ideas, properties, terminologies, use cases, and advancements of edge computing for IoT. It aids in identifying possible regions of standardization in edge computing in the realm of IoT [98].
5. *ISO/IEC TR 30166:2020*- In this standard, IIoT frameworks, specialized viewpoints and utilitarian components, and other aspects of IIoT are discussed. New advancements, risk analysis, and potential future standardizations are also covered [99].
6. *ISO/IEC 27030*- This standard caters specifically to the privacy & security of IoT. It will provide a guide towards IoT principles, risk, and control. This standard is expected to be published in 2022. The title “Cybersecurity - IoT security and privacy – Guidelines” is under discussion with the possibility of it getting renumbered to ISO/IEC 27400 [100].
7. *ISO/IEC AWI 30147*- This standard deals with system lifecycle processes extending to IoT frameworks. This standard is under development [101].
8. *ISO/IEC AWI 30149*- This standard deals with the Trust framework of IoT. It is under development [102].

All these four organizations have given a good amount of consideration to the issues of IoT. They each have defined their own visions and terms. Compared with the rest, the standards of the ITU offer a much broader and more specific proposition with suitable examples. Most of the standards covered here lack in acknowledging the specific security issues of software and hardware of IoT. This gap can be addressed by making future standards that take this into account. Other international organizations show a lack of interest in developing standards for IoT, they are limited towards their support services when security issues arise.

8. Discussion

This article focuses on bringing forth the often-neglected challenges of IoT into light and presents insights into conducted research on these IoT challenges making it feasible to identify the gaps.

8.1. Gaps & related research

Taking a look at smart contracts, Alharby et al. (2018) [23] conducted a systematic mapping study of the current research in smart contracts to comprehend the various research areas. The authors found that the majority of research (64%) is based on smart contract applications while only 6% of the research is based on the security aspect and 2% on the privacy aspect. This indicates a general lack of research focusing on the vulnerabilities of smart contracts. A survey by Panarello et al. (2018) [26] analyzed the current research focusing on Blockchain-related methodologies in the context of IoT. The authors indicate that there is a lack of research focused on IoT-specific domains as the research towards IoT and Blockchain is in the initial stage. Considering the rate of expansion of IoT, security is concerningly underdeveloped. A study by Nawir et al. (2017) [40] surveys the taxonomy of IoT security attacks and suggests that security is a major concern given the nature of IoT. Security attacks may disrupt networks leading to adversities for the user. A survey focusing on IoT security by Zhao and Ge (2013) [33] advocates that the security challenges of IoT are increasing in severity due to the underlying security framework still being in a preliminary stage. Likewise, research by Ahemd et al. (2017) [34] and Iqbal et al. (2017) [32] analyze the security element of IoT. Both papers propose that security challenges are a major concern for the future of IoT and that further steps should be taken to ensure the user’s security. Overall, there is a lack of research focusing on dealing with network layer-related security attacks as compared with the physical layer that is geared towards the actual hardware.

In the case of emerging technologies, it is always the ethics that impedes technological modernization. IoT falls victim similarly as the security of IoT is comparatively underdeveloped which corresponds to an unreliable IoT security without any prominence on the meaning from an ethical standpoint. A study by Popescul and Georgescu (2013) [38] surveyed the ethical issues of IoT focusing on ICT ethical challenges. The authors point out that IoT poses a threat from an ethical standpoint to the common user. The user is unaware of the ongoing threats and this can lead to potentially adverse situations for the user.

Table 4
Summary of International Standards covering IoT

ISO/IEC		
No.	**Standard**	**Description**
1	ISO/IEC 20924:2018 (IoT definition and vocabulary)	This document defines the Internet of Things alongside providing relevant definitions and terms forming the foundation of IoT
2	ISO/IEC 21823-1:2019 (Interoperability for IoT systems – Part 1: Framework)	It gives an outline of interoperability for IoT systems, and also a framework for interoperability
3	ISO/IEC 22417:2017 (IoT use cases)	It identifies IoT use cases and scenarios that are based on real-life applications and necessities
4	ISO/IEC 29161:2016 (Unique identification for the IoT)	It indicates the common rules relevant to unique identification for any virtual or physical object to guarantee compatibility across various identities
5	ISO/IEC 29181-9:2017 (Future Network – Problem statement and requirements, Part 9: Networking of everything)	It depicts a conceptual NoE model and its overall attributes that can be applied to future networks from the IoT viewpoint
6	ISO/IEC 30141:2018 (IoT reference architecture)	It gives a normalized IoT reference architecture utilizing common technical definitions, reusable plans and industry best practices
ITU		
No.	**Standard**	**Description**
1	Y.4000/Y.2060 (Overview of the IoT)	It highlights the future standardization of IoT. Generic and explicit security capacities are also discussed
2	Y.4050/Y.2069 (Terms and definitions for the IoT)	It indicates the relevant terms and definitions applicable to the IoT to explain IoT-related activities
3	Y.4100/Y.2066 (Common requirements of the IoT)	It provides functional requirements for information gathering, sharing, processing, handling, and arrangement of services
4	Y.4103/F.748.0 (Common requirements for IoT applications)	A list of common requirements centered on IoT applications is covered in this document
5	Y.4552/Y.2078 (Application support models of the IoT)	It gives the configurable, adaptable, and reliable application support models with their premise
6	Y.4111/Y.2076 (Semantics-based requirements and framework of the IoT)	It contains necessities for security capacities with the utilization of semantic technologies or security-decision making
7	Y.4113 (Requirements of the network for the IoT)	It presents a basic model of the IoT network, general qualities, smart sensors, and the network vulnerabilities
8	Y.4453 (Adaptive software framework for IoT devices)	It addresses the adaptive software framework (ASF), a reference architecture for smart IoT devices is provided alongside
9	Y.4101/Y.2067 (Common requirements and capabilities of a gateway for IoT applications)	Discusses IoT gateways in brief, along with their prerequisites, normal capacities, framework, and use cases
10	Y.4112/Y.2077 (Requirements of the plug and play (PnP) capability of the IoT)	It portrays the idea of PnP furthermore, along with its requirements and components. Firewall protection, access control, and gateway PnP capabilities are also discussed
11	Y.4401/Y.2068 (Functional framework and capabilities of the IoT)	It portrays key IoT abilities dependent on the functional framework of IoT to satisfy the requirements of Y.2066
12	Y.4806 (Security capabilities supporting safety of the IoT)	It presents dangers to confidentiality, integrity, and availability that affects safety and suggests methods to mitigate them
IEEE		
No.	**Standard**	**Description**
1	P2413 (Architectural framework (AF) for the IoT)	It characterizes the AF, including details of different IoT domains and gives a blueprint for protection, security, privacy & safety- the quality “quadruple” trust
2	P1451-99 (Harmonization of IoT devices and systems)	It characterizes a strategy for information sharing, interoperability, and message security over the networks where IoT devices operate. It makes use of the high-level capacities of Extensible Messaging and Presence Protocol
3	P1931.1 (AF for real-time onsite operations facilitation for the IoT)	It characterizes an AF, conventions, and APIs to provide Real-time Onsite Operations Facilitation or ROOF. overs interoperability, coordinated effort, and self-governing activity of the IoT system
4	P2668 (Maturity index of IoT: evaluation, grading and ranking)	It provides the basis for measuring the maturity of IoT devices and things and defines an evaluation mechanism using an indicator value IoT Index or IDex

Acknowledging this, there is a lack of research focusing on interventions needed to secure IoT from an ethical standpoint. Furthermore, Allhoff and Henschke (2018) [56] highlight that the ethics focused on emerging technology are generally made to cover a broad aspect as in abstract ideas and that these broad discussions have failed to identify the new and unique features that IoT has to offer. We know that factors like uncertainty and risk count, therefore it is important to address that insights into particular domains have not yet been performed as in-depth addressing is lacking. Likewise, the authors also state that informed consent, privacy, information security, physical safety, and trust have set up literature and are valuable outsets that have short to mid-term applications thus making these five factors foundational for ethical concerns.

Moving on to privacy, the number of studies published to deal with privacy threats is currently inadequate corresponding to the number of privacy threats that stem up every year. A review by Aleisa and Renaud (2017) [54] analyzed the gaps in the literature concerning IoT privacy and privacy-preserving solutions. The authors indicate that the majority of the research covering the vulnerabilities of IoT is focused on the security aspect neglecting the equally crucial privacy crisis. They suggest that research evaluating privacy perceptions of IoT is required. The authors also point out a need for legislation to combat these privacy threats faced by the user. Similarly, Ziegeldorf et al. (2013) [52] and Tawalbeh et al. (2020) [103] surveyed the privacy challenges of IoT and have suggested a need for legislation. Ziegeldorf points out that in order to cope up with the evolving nature of IoT, an equivalent legal framework is required. Tawalbeh suggests that currently there is a lack of standardization for data sharing and assortment mechanisms performed by IoT devices. This is essential as standardization may help decrease the number of erratic vulnerabilities of IoT.

Coming to the legal aspect of IoT, currently, only a handful of nations have enacted IoT-specific laws. In Asia, the legal groundwork for IoT in countries like India, China, and other nations is lacking in development due to the lack of IoT-specific laws. In the Middle East, except for UAE, the other Middle East nations do not have any policies concerning IoT. Asia lacks significantly behind Europe and other western nations in terms of IoT-specific legal frameworks. IoT is vastly underdeveloped in Latin America and so the few nations like Brazil, Argentina, and Chile that do have laws on IoT, these laws focus on driving up the production of the IoT ecosystem. No laws to cover the vulnerabilities of IoT have been proposed yet. There are no significant laws concerning any aspect of IoT in Africa and other undeveloped countries as the development of IoT has yet to flourish in these nations. Apart from international standards, there is a general lack of IoT laws from a global standpoint. Likewise, there is quite limited research focusing on and analyzing the legal framework of IoT of individual nations around the globe.

8.2. Research explanation

As we are witnessing the growth of IoT skyrocket in recent years, they bring along several challenges. This study supports that the security, privacy, ethical and legal challenges of IoT are the greatest threat considering the amount of influence that IoT has on our daily lives. These results build on existing evidence of research focused on the threats and vulnerabilities of IoT. The majority of the research directed on highlighting the challenges of IoT only focuses on one or two major challenges like security and/or privacy. Therefore, taking this into account, this study discusses the challenges of smart contracts along with security, privacy, and ethical challenges of IoT whilst analyzing the current laws and standards around the globe addressing IoT to provide a clear overview of the current situation. Alongside, a myriad of use cases is discussed to cover how all of these IoT challenges impact our daily lives significantly through real-life applications and scenarios. The common user must be made aware of the security, ethical, and privacy threats imposed by modern IoT devices. As witnessed, the research focusing on the security and privacy aspects of smart contracts is quite limited considering that these two aspects are of major concern to the user. Regarding the need for specific laws, smart contracts won't be necessarily replacing conventional contract laws as they are enforceable under the current existing laws. Coming to IoT, as the number of IoT devices continues to crank up, they fall prey to an ever-increasing number of security attacks by the day. Hackers are figuring out more complex and innovative ways to attack these devices to steal and manipulate the user's data. The majority of the research on IoT vulnerabilities is focused on security. However, the proposed solutions in these papers have not yet been implemented to a greater extent leading to an increase in the number of security-related casualties. In the realm of ethics concerning IoT, the current literature on ethics exclusively focuses on the technological field and does not extend to cover the domain of IoT. This results in ethical issues being overlooked leading to an increase in moral dilemmas. Regarding the privacy of the user, the number of privacy threats is on the rise that renders the user's private data at stake. The current research highlighting privacy is inadequate considering that privacy is the main concern of the common IoT user. The bulk of the security attacks and privacy threats reviewed in this paper deal with user's data being collected and used to harm the user or used for unfair purposes and theft. This can lead to a lack of trust from the common users towards IoT. This is concerning as trust is an important aspect of IoT and is reliant on issues like security, privacy, informed consent, and safety together. So, this leads us to question how are our authorities handling this situation. The only solution is to enact laws and standards to combat these vulnerabilities of IoT. Hence, we dive into the IoT-specific laws that governments of nations around the globe have begun enacting in order to protect their citizens from these vulnerabilities. However, as we have witnessed, only a handful of nations have implemented IoT-specific laws. The nations that do have internet laws only cover general cybersecurity and leave out the area of IoT. These nations need to start implementing laws to curb IoT malpractices as this would lead to better safety of the user's data. In India, Canada, and other major nations, the current legislation does not extend to IoT. Asian countries like China, Japan, and UAE have started implementing independent laws about IoT, but specific countermeasures to combat the threats of IoT have not been focused upon. Australia, UK, the EU, and The US on the other hand are ahead of

the rest of the world in terms of IoT laws. The development of IoT in Latin American nations has yet to flourish for them to enact laws specifically catered to IoT. Looking at Africa and other underdeveloped nations, the majority of the population does not have widespread access to technological devices yet alone IoT, so the aspect of laws remains out of question. Most of the regulations in use today fall under the EU's GDPR, but we have seen that it would be much better for an international committee to set the standards than just Europe as IoT can be covered on a global standard. The ISO, IEC, ITU, and IEEE contribute to almost all of the international standards set for IoT. Standardization continues to grow moderately, this is promising as an international approach is indispensable to combat these challenges of IoT.

8.3. Limitations

This article has primarily focused on reviewing and investigating the challenges of IoT. Although a number of papers that focus on privacy, security, or other threats of IoT also incorporate or propose solutions to overcome these challenges, this study chiefly deals with analyzing and examining the challenges without focusing on the solutions. Thus, it is beyond the scope of this study to review the existing and present-day security and privacy solutions proposed by researchers.

8.4. Future research

A further review should be implemented in an effort to evaluate the current solutions for these IoT challenges. Future studies should take into account the lack of research on smart contract vulnerabilities and IoT incorporation in smart contracts and build upon this. Similar is the case for ethical and privacy challenges of IoT; in-depth addressing into specific IoT domains in the realm of ethics should be carried out to establish a strong ethical background for IoT. Considering IoT security, research should focus on not only the security attacks occurring at the physical layer but also the often neglected and susceptible network layer to cover all the potential and related casualties. The literature would also benefit if potential legal frameworks to tackle the vulnerabilities of IoT from a global perspective be suggested as this would have a huge impact on the handling of IoT devices and their implications.

9. Conclusion

IoT continues to prosper as we see in the 21st century. As our focus shifts on incorporating more of these devices in our lives to make it smoother, the greatest downsides of these devices usually tend to go under our radar. By analyzing the security, privacy, ethical and legal challenges of IoT, this paper has shown how these challenges have a significant impact on our daily lives and that research focusing on these negative aspects is quite limited given the substantial growth of IoT in the past couple of decades. The architecture of IoT along with its plethora of applications are discussed in this paper to give the reader a key overview of the Internet of Things. The use cases discussed in this paper provides an insight into how the issues of security, ethics, privacy, trust, and laws have an impact on society and our day-to-day lives. Due to the lack of research highlighting the drawbacks of smart contracts, this study considers this and discusses smart contracts and its security, privacy, and legal challenges. The spectrum of security attacks occurring across the architectural layers and the cluster of ethical issues and privacy threats faced by the user as well as trust has been discussed. A way to combat these issues is to enact IoT-specific laws. Therefore, governmental and international laws and standards have been reviewed. This study clearly illustrates the threats and vulnerabilities of IoT, but it also raises the question of the current and potential solutions to overcome these challenges. Building on this, researchers should consider reviewing the current and existing security and privacy solutions to provide an overview of the current situation. Taking into consideration the need for a comprehensive overview of the security, privacy, and ethical challenges of IoT alongside addressing trust and laws, this paper delivers a clear overview of all these challenges and analyzes the current and upcoming laws and standards across different countries to provide a coherent insight into the current situation of IoT.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

I would like to thank Clyde J. Vincent for his support and guidance throughout the submission process.

References

[1] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, Brief History of the Internet, Internet Society, Aug. 2000.

[2] P. Wang, R. Valerdi, S. Zhou, et al., Introduction: Advances in IoT research and applications, Information Systems Frontier 17 (Mar. 2015) 239–241, doi:10.1007/s10796-015-9549-2.

[3] Javad Pourqasem, Cloud-based IoT: integration cloud computing with internet of things, International Journal of Research in Industrial Engineering 7 (2018) 482–494, doi:10.22105/riej.2018.88380.

[4] C. Perera, C. H. Liu, S. Jayawardena and M. Chen, "A Survey on Internet of Things From Industrial Market Perspective," in IEEE Access, vol. 2, pp. 1660-1679, Jan. 201, doi: 10.1109/ACCESS.2015.2389854.

[5] S.G. Tzafestas, Ethics and Law in the Internet of Things World, Smart Cities 1 (Oct. 2018) 98–120, doi:10.3390/smartcities1010006.

[6] M. Burhan, R.A. Rehman, B. Khan, B.-S Kim, IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, Sensors 18 (Aug. 2018) 2796, doi:10.3390/s18092796.

[7] Pallavi Sethi, Smruti R. Sarangi, Internet of Things: Architectures, Protocols, and Applications, Journal of Electrical and Computer Engineering 2017 (Jan. 2017), doi:10.1155/2017/9324035.

[8] X. Liu, et al., Overview of Spintronic Sensors With Internet of Things for Smart Living, IEEE Transactions on Magnetics 55 (11) (Nov. 2019) 1–22.

[9] B. Omoniwa, R. Hussain, M.A. Javed, S.H. Bouk, S.A. Malik, Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues, IEEE Internet of Things Journal 6 (3) (June 2019) 4118–4149, doi:10.1109/JIOT.2018.2875544.

[10] Hany Fathy Atlam, Robert Walters, Gary Wills, Internet of Things: state-of-the-art, challenges, applications, and open issues, International Journal of Intelligent Computing Research (IJICR) 9 (3) (Sep. 2018) 928–938, doi:10.20533/ijicr.2042.4655.2018.0112.

[11] Porkodi Dr.R, Bhuvaneswari Velumani, The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview, in: Proceedings - 2014 International Conference on Intelligent Computing Applications, ICICA, Mar. 2014, pp. 324–329, doi:10.1109/ICICA.2014.73.

[12] Niraj Chokshi, Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation, The New York Times (May 25, 2018) Available https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html .

[13] Abdur Razzaq, Mirza, Sajid Habib, Saleem Ullah, Security Issues in the Internet of Things (IoT): A Comprehensive Study, International Journal of Advanced Computer Science and Applications 8 (2017), doi:10.14569/IJACSA.2017.080650.

[14] B. Sowmiya, V. Abhijith, S. Sudersan, et al., A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19, SN COMPUT. SCI. 2 (Mar. 2021), doi:10.1007/s42979-021-00520-z.

[15] S. Tivatansakul, M. Ohkura, S. Puangpontip, T. Achalakul, Emotional healthcare system: Emotion detection by facial expressions using Japanese database, in: 2014 6th Computer Science and Electronic Engineering Conference, CEEC 2014 - Conference Proceedings, Institute of Electrical and Electronics Engineers Inc., Sep. 2014, pp. 41–46, doi:10.1109/CEEC.2014.6958552.

[16] Charlotte Jee. "Emotion recognition technology should be banned, says an AI research institute", MIT Technology Review, Dec. 2019. Available: https://www.technologyreview.com/2019/12/13/131585/emotion-recognition-technology-should-be-banned-says-ai-research-institute/.

[17] Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, Aruna Seneviratne, A Survey of Wearable Devices and Challenges, IEEE Communications Surveys & Tutorials (99) (Jul. 2017) 1-1, doi:10.1109/COMST.2017.2731979.

[18] Peter Corcoran, Claudia Costache, Biometric technology and smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts, in: 2015 IEEE International Symposium on Technology and Society (ISTAS), Nov. 2015, pp. 1–7, doi:10.1109/ISTAS.2015.7439439.

[19] Sean O'Kane, Tesla hit with another lawsuit over a fatal Autopilot crash", The Verge (Aug. 2019) Available https://www.theverge.com/2019/8/1/20750715/tesla-autopilot-crash-lawsuit-wrongful-death .

[20] Kashmir. Hill, How Target Figured Out a Teen Girl Was Pregnant before Her Father Did, Forbes (Feb 16, 2012) Available https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#1c7ae5696668 .

[21] K. Batistic, Privacy in Smart Parking, Dissertation, Stockholm, Sweden, 2020 Available http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-272998 .

[22] , SMART METER: APPLICATIONS, SECURITY ISSUES AND CHALLENGES, in: Proceedings of the 5th International Conference on Computing and Informatics, ICOCI 2015, Aug. 2015.

[23] M. Alharby, A. Aldweesh, A.v. Moorsel, Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research, in: 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), Fuzhou, China, 2018, pp. 1–6, doi:10.1109/ICCBB.2018.8756390. Nov. 2018.

[24] Alexander Savelyev, Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, Information & Communications Technology Law 26 (2) (Apr. 2017) 116–134, doi:10.1080/13600834.2017.1301036.

[25] S. Rouhani, R. Deters, Security, Performance, and Applications of Smart Contracts: A Systematic Survey, IEEE Access 7 (Apr. 2019) 50759–50779, doi:10.1109/ACCESS.2019.2911031.

[26] A Panarello, N Tapas, G Merlino, F Longo, Puliafito, A. Blockchain and IoT Integration: A Systematic Survey, Sensors 18 (8) (Aug. 2018) 2575, doi:10.3390/s18082575S5.

[27] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli, "A Survey of Attacks on Ethereum Smart Contracts SoK," In Proceedings of the 6th International Conference on Principles of Security and Trust, vol. 10204, pp. 164–186, Apr. 2017, doi: 10.1007/978-3-662-54455-6_8.

[28] M. Wohrer, U. Zdun, Smart contracts: security patterns in the ethereum ecosystem and solidity, in: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, Mar. 2018, pp. 2–8, doi:10.1109/IWBOSE.2018.8327565.

[29] Samuel Steffen, Benjamin Bichsel, Mario Gersbach, Noa Melchior, Petar Tsankov, Martin Vechev, Zkay: Specifying and Enforcing Data Privacy in Smart Contracts, in: In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, Nov. 2019, pp. 1759–1776, doi:10.1145/3319535.3363222.

[30] A. Cohn, T. West, C. Parker, SMART AFTER ALL: BLOCKCHAIN, SMART CONTRACTS, PARAMETRIC INSURANCE, AND SMART ENERGY GRIDS, Georgetown Law Technology Review (Apr. 2017).

[31] Riccardo De Caria, The Legal Meaning of Smart Contracts, European Review of Private Law 26 (6) (2018) 731–751.

[32] M.A. Iqbal, O.G. Olaleye, M. Bayoumi, A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches, Global Journal of Computer Science and Technology 16 (2017).

[33] K. Zhao, L. Ge, A Survey on the Internet of Things Security, in: 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 663–667, doi:10.1109/CIS.2013.145.

[34] M.M. Ahemd, M.A. Shah, A. Wahid, IoT security: A layered approach for attacks & defenses, in: 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, 2017, pp. 104–110, doi:10.1109/COMTECH.2017.8065757.

[35] M. Alam, M.M. Tehranipoor, U. Guin, TSensors Vision, Infrastructure and Security Challenges in Trillion Sensor Era, Journal of Hardware and Systems Security 1 (Nov. 2017) 311–327, doi:10.1007/s41635-017-0028-8.

[36] J. Kim, C. Yang, J Jeon, A Research on Issues Related to RFID Security and Privacy In: Wang W., Li Y., Duan Z., Yan L., Li H., Yang X. (eds), Integration and Innovation Orient to E-Society Volume 2. IFIP International Federation for Information Processing, 252, Springer, Boston, MA, 2007, doi:10.1007/978-0-387-75494-9_50.

[37] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A Ribagorda, RFID Systems, A Survey on Security Threats and Proposed Solutions, in: Personal Wireless Communications. PWC 2006. Lecture Notes in Computer Science, 4217, Springer, Berlin, Heidelberg, 2006, pp. 159–170, doi:10.1007/11872153_14.

[38] Daniela Popescul, Mircea Georgescu, Internet Of Things – Some Ethical Issues, The USV Annals of Economics and Public Administration, Stefan cel Mare University of Suceava, Romania, Faculty of Economics and Public Administration 13 (Jun. 2013) 210–216.

[39] R. C. Shit, S. Sharma, D. Puthal and A. Y. Zomaya, "Location of Things (LoT): A Review and Taxonomy of Sensors Localization in IoT Infrastructure," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2028-2061, Jan. 2018, doi: 10.1109/COMST.2018.2798591.

[40] M. Nawir, A. Amir, N. Yaakob, O.B. Lynn, Internet of Things (IoT): Taxonomy of security attacks, in: 2016 3rd International Conference on Electronic Design (ICED), Phuket, 2016, pp. 321–326, doi:10.1109/ICED.2016.7804660. Jan. 2017.

[41] S. Babar, A. Stango, N. Prasad, J. Sen, R. Prasad, Proposed embedded security framework for Internet of Things (IoT), in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), Chennai, 2011, pp. 1–5, doi:10.1109/WIRELESSVITAE.2011.5940923.

[42] Y. Pan, J. White, D. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, C Williams, Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems, Int. J. Interact. Multim. Artif. Intell. 4 (2017) 45–54, doi:10.9781/ijimai.2017.437.

[43] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997. Available: http://www.rogerclarke.com/DV/Intro.html, (accessed 14 October 2020).

[44] K. Renaud, D. Gálvez-Cruz, Privacy: Aspects, definitions and a multi-faceted privacy preservation approach, in: 2010 Information Security for South Africa, Sandton, Johannesburg, 2010, pp. 1–8, doi:10.1109/ISSA.2010.5588297. Aug. 2010.

[45] M. Burhan, R.A. Rehman, B. Khan, B.-S Kim, IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, Sensors 18 (Aug. 2018), doi:10.3390/s18092796.

[46] Patrão Neves, Maria, Ethics, as a philosophical disciplineEncyclopedia of Global Bioethics, inger - International Publisher Science, Technology and Medicine, Jan. 2016, doi:10.1007/978-3-319-05544-2_177-1.

[47] Prabhakar Krishnamurthy, An Introduction to Ethics, SSRN (2011) MarchAvailable https://ssrn.com/abstract=1781502 . (accessed 14 October 2020).

[48] Daniela Popescul & Mircea Georgescu, "Internet Of Things – Some Ethical Issues," The USV Annals of Economics and Public Administration, Stefan cel Mare University of Suceava, Romania, Faculty of Economics and Public Administration, vol. 13, pp. 210-216, Jun. 2013.

[49] H.F. Atlam, G.B. Wills, IoT Security, Privacy, Safety and Ethics, in: M. Farsi, A. Daneshkhah, A. Hosseinian-Far, H. Jahankhani (Eds.), Digital Twin Technologies and Smart Cities, Internet of Things (Technology, Communications and Computing, Springer, Cham, Jul. 2019, doi:10.1007/978-3-030-18732-3_8.

[50] E. Toch, Y. Wang, L.F. Cranor, Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems, User Model User-Adap Inter 22 (220 Mar. 2012) 203, doi:10.1007/s11257-011-9110-z.

[51] Hany Atlam, Robert Walters, Gary Wills, Internet of Nano Things: Security Issues and Applications, in: 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018), Barcelona, Spain, Aug 2018, p. 7, doi:10.1145/3264560.3264570.

[52] Jan Ziegeldorf, Oscar Morchon, Klaus Wehrle, Privacy in the Internet of Things: Threats and Challenges, Security and Communication Networks 7 (Dec. 2014) 2728–2742, doi:10.1002/sec.795.

[53] Janice Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, Location-Sharing Technologies: Privacy Risks and Controls, TPRC, SSRN (Aug. 2009) Available https://ssrn.com/abstract=1997782 . (accessed 16 October 2020).

[54] Noura Aleisa, K. Renaud, Privacy of the Internet of Things: A Systematic Literature Review, ArXiv (2017) vol. abs/1611.03340, doi:10.24251/HICSS.2017.717.

[55] Internet of Things (IoT) Trust Concerns, NIST Cybersecurity White Paper, Oct. 2018.

[56] Fritz Allhoff, Adam Henschke, The Internet of Things: Foundational ethical issues, Internet of Things 1-2 (Sep. 2018) 55–66, doi:10.1016/J.IOT.2018.08.005.

[57] H. Sato, A. Kanai, S. Tanimoto, T. Kobayashi, Establishing Trust in the Emerging Era of IoT, in: 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), Oxford, UK, May 2016, pp. 398–406, doi:10.1109/SOSE.2016.50.

[58] schider, Charlotte, "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age," 96 DENV. U. L. REV. 87, SSRN, Feb. 2018. Available: https://ssrn.com/abstract=3129557, (accessed 16 October 2020), doi: 10.2139/ssrn.3129557.

[59] A. AboBakr, M.A. Azer2017 12th Intern, IoT ethics challenges and legal issues, in: ational Conference on Computer Engineering and Systems (ICCES), Cairo, 2017, pp. 233–237, doi:10.1109/ICCES.2017.8275309.

[60] Sourav Naug, Internet of Things, The Indian Journal of Law and Technology (2018) Available http://ijlt.in/index.php/2018/09/11/internet-of-things/ . (accessed 16 October 2020).

[61] *Draft Policy on Internet of Things*, Department of Electronics & Information Technology (DeitY), Ministry of Communication and Information Technology, Government of India, 2015.

[62] V. Kethareswaran, An Indian Perspective on the adverse impact of Internet of Things (IoT, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 6 (2017) 35, doi:10.14201/ADCAIJ2017643540.

[63] *Cybersecurity Law of the People's Republic of China*, Standing Committee of the National People's Congress, People's Republic of China, Jun. 2017.

[64] *Information Security Technology – Personal Information Security Specification*, State Administration for Market Regulation (SAMR), Standardization Administration of China (SAC), People's Republic of China, Oct. 2020.

[65] *Act on the Protection of Personal Information (APPI)*, Personal Information Protection Commission (PIPC), Japan, May. 2017.

[66] *The Basic Act on Cybersecurity,* Act No. 104, Japan, Nov. 2014.

[67] *CYBERSECURITYSTRATEGY*, Japan, Jul. 2018.

[68] *Internet of Things Regulatory Policy, Telecommunications Regulatory Authority (TRA)*, P O Box 26662, Abu Dhabi, United Arab Emirates (UAE), Mar. 2018.

[69] U. Pagallo, M. Durante, S. Monteleone, What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT, in: Data Protection and Privacy: (In)visibilities and Infrastructures, 36, Law, Governance and Technology Series, 2017, pp. 59–78, doi:10.1007/978-3-319-50796-5_3.

[70] *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA,* Official Journal of the European Union, Sep. 2013.

[71] *Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance*, Official Journal of the European Union, May. 2014.

[72] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union*, Jul. 2016.

[73] A. Tăbuşcă, S. Tăbuşcă, G. Garais, IoT and EU Law – E-Human Security, Valahian Journal of Economic Studies 9 (Mar. 2019) 25–32, doi:10.2478/vjes-2018-0015.

[74] *Standardisation and the EU Cybersecurity Act*, ENISA, Feb. 2020.

[75] *ETSI TS 103 645*, "Cyber Security for Consumer Internet of Things", ETSI, Feb. 2019.

[76] "ePrivacy Regulation", European Commission, Europe.

[77] *Government response to the "Regulatory proposals for consumer Internet of Things (IoT) security consultation*, Minister for Digital & Broadband, Department for Digital, Culture, Media & Sport by Command of Her Majesty, United Kingdom, Jan. 2020.

[78] Code of Practice for Consumer IoT Security, Department for Digital, Culture, Media & Sport, United Kingdom, Oct. 2018.

[79] Chike. Chike, The Legal Challenges of Internet of Things, Jan (2018), doi:10.13140/RG.2.2.31475.84004.

[80] Nishith Desai Associates, "Internet of Things Legal & Tax Issues," Jan. 2017. Available: https://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Internet_of_Things.pdf, (accessed 17 October 2020).

[81] *Security of Connected Devices*, Senate Bill No. 327, CHAPTER 886, California, United States, Jan. 2020.

[82] *Enrolled House Bill 2395*, 80th OREGON LEGISLATIVE ASSEMBLY, Chapter 193, Oregon, United States, 2019.

[83] *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, NISTIR 8228, Jun. 2019, doi: 10.6028/NIST.IR.8228.

[84] *Foundational Cybersecurity Activities for IoT Device Manufacturers*, NISTIR 8259, May. 2020, doi: 10.6028/NIST.IR.8259.
[85] *S.734 -IoT Cybersecurity Improvement Act of 2019*, 116th Congress, United States, Sep. 2019.
[86] IoT Security Rating Levels, Identity Management & Security, UL. Available: https://ims.ul.com/iot-security-rating-levels.
[87] *Cyber Supply Chain Risk Management*, Australian Government Signals Directorate, Australian Cyber Security Centre, Australia, Nov. 2019.
[88] *CIC Best Practice Guidance Supply Chains*, Department of Home Affairs' Critical Infrastructure Centre, Australian Government, Australia.
[89] *Code of Practice. Securing the Internet of Things for Consumers*, Department of Home Affairs, Australian Government, Australia, Nov. 2019.
[90] DECREE NO. 9,854, OF JUNE 25, 2019, OFFICIAL GAZETTE OF THE UNION, Brazil, Jun. 2019.
[91] Marval O'Farrell Mairal. "Public Consultation on Internet of Things", Argentina, May. 2017.
[92] Diego Rodríguez. "Data protection and cybersecurity laws in Chile", CMS, Feb. 2021. Available: https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/chile.
[93] *Statement of Intent Regarding the Security of the Internet of Things*, London, United Kingdom, Jul. 2019.
[94] N. Miloslavskaya, A. Nikiforov, K. Plaksiy, A. Tolstoy, Standardization Issues for the Internet of Things In: Rocha Á., Adeli H., Reis L., Costanzo S. (eds), New Knowledge in Information Systems and Technologies, 931, WorldCIST'19 2019. Advances in Intelligent Systems and Computing, Springer, Apr. 2019, doi:10.1007/978-3-030-16184-2_32.
[95] *Internet of things (IoT) — Interoperability for IoT systems — Part 1: Framework.* ISO/IEC 21823-1:2019, Feb. 2019.
[96] *Information technology — Internet of media things — Part 1: Architecture.* ISO/IEC 23093-1:2020, Feb. 2020.
[97] *Internet of things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability.* ISO/IEC 21823-2:2020, Apr. 2020.
[98] *Internet of things (IoT) — Edge computing.* ISO/IEC TR 30164:2020, Apr. 2020.
[99] *Internet of things (IoT) — Industrial IoT.* ISO/IEC TR 30166:2020, Apr. 2020.
[100] *Guidelines for security and privacy in Internet of Things (IoT).* ISO/IEC 27030, Unpublished.
[101] *Information technology — Internet of things — Methodology for trustworthiness of IoT system/service.* ISO/IEC AWI. *30147*, Unpublished.
[102] *Internet of things (IoT) — Trustworthiness framework.* ISO/IEC AWI 30149, Unpublished.
[103] L Tawalbeh, F Muheidat, M Tawalbeh, M Quwaider, IoT Privacy and Security: Challenges and Solutions, Applied Sciences 10 (12) (Jun. 2020) 4102, doi:10.3390/app10124102.