Quest for Privacy in IoT

Ankrutee Arora IMT2020034

***Abstract*—IoT, Internet of Things is a paradigm that enables us to bridge the gap between digital world and physical world. It provides us with innovative solutions to challenges in developing fields which in turn is changing the face of the world. IoT is becoming an important part of our lives, but with this there is security concerns which is a major issue. There are a lot of challenges that still need to be addressed and overcome. The biggest challenge is to ensure the full potential usage of this technology by the users without any threats or concerns. The following project work will throw some light on the challenges and issues concerned with IoT and also help the reader understand the existing solutions that are followed. Privacy by design (PbD) is by far the most efficient solution which tackles many IoT related privacy issues. This article would also help the readers to understand the IoT and its importance in the real world.**

***Index Terms*—**

1) **Privacy by Design (PbD)**
2) **Radio-frequency Identification (RFID) Data mining**
3) **Wireless sensor networks (WSN)**
4) **Cloud computing**
5) **Privacy-enhancing technologies(PET)**

I. Introduction

The IoT in simple terms means connecting the physical world to the internet. It comprises of heterogeneous networking technologies and devices. The difficulty arises when higher performing devices require some high-level protocol to perform efficiently but at the same time, it would be difficult for the smaller devices to work on such high-level protocols. However, light weight privacy solutions are easily hackable and traceable.

[1]There have been several reports conducted by various organisations proving the adversities of using IoT and how impactful it can on the user's life. For example, Cisco had made a supposition that in the near future, there will be almost more than half a hundred billion Web-enabled devices, but there have already been cases stated, where consumers have come across several privacy concerns due to the use of unescapable products and services. In June 2013, surveys exposed privacy related concerns connected to Planning Tool Integration, Synchronization, and Management (PRISM) program, this is used by the US National Security Agency to gather electronic information of the customers who use key Internet services including top MNC's like Microsoft Outlook, Google, and Facebook. Moreover, an Internet safety concern statement says that smart phones malware outbreaks augmented by almost fifty-eight percent from 2011 to 2012 and almost thirty out of a hundred of the attacks tempted to snip confidential data. In search of a solution, several reports have suggested Privacy by design -PbD to be one of the most prominent solutions for overcoming IoT related privacy issues. This project is an indication of confidentiality concerns and encounters linked to IoT's affiliated technologies as well as the applications. This also provides a wider outline of existing research issues concerned to IoT privacy threats and all PbD solutions from lookouts of several fields, and the universal public. In accumulation to unfolding current resolutions and capable developing tactics, the project discusses issues and guidelines to preserve IoT related security.

II. Layers of IoT Technologies

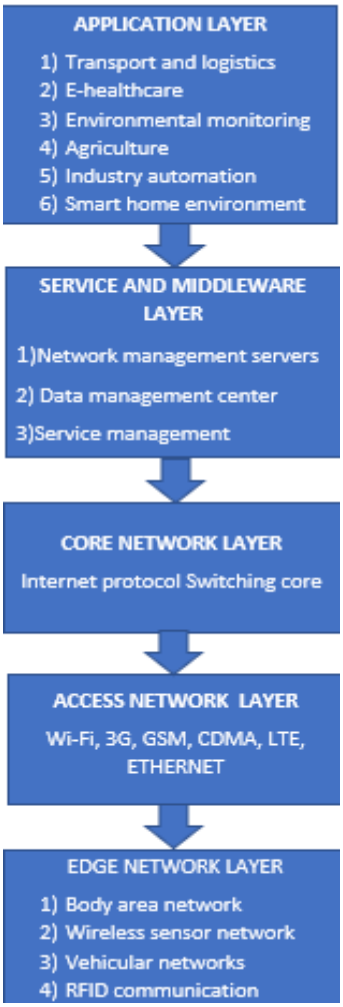

Fig. 1. The OSI model layers

There is still no single, general agreement by the world and the researchers about the architecture of IoT. Researchers have proposed diverse architectures for IoT's models. The constant advancement of the IoT's structure along with the complications of its underlying technologies along with

the prophets included in the development brands it a bit problematic to properly give it a definition. The functionalities of the layers have been represented in the in Fig 1. It is defined w.r.t the OSI (Open Systems Interconnection) model layers. The OSI Model is a rational and abstract model which defines communication between networks by using systems to interconnect and communicate with neighbour systems. It does have its own pros and cons but the most effective way to describe the computer packet transfer is by using different protocol layers. [2]

i) The edge network layer, resembles OSI's architecture layer i.e. the physical layer. It is information discernment layer. It accountable to classify objects, sense the environment and collect real time data from them. Various types of sensors that are connected to objects have the functionality to gather data such as 2-D bar-code, sensors and RFID. Common sensor that is accessible nowadays is the mobile phone. There are several features available on the smartphones. For instance, according to the requirement of applications, the sensors are chosen. This data which is gathered by the sensors can track confidential data of the user and their surroundings. The technologies and devices which run on these technologies have a short-range communication, they tend to have less storage.

ii) The access network layer signifies data link layer. It comprises a range of communication technologies which are quite diverse and they allow the initial stage of data communication. This layer amends errors that can arise at physical layer. It helps the protocol to implement the routing of packets and publishes, subscribes via different networks. It also helps to structure the favourable path. This permits data transfer from the source to the destination.

iii)The core network layer resembles to OSI's network layer. This comprises of conservative Internet protocol (IP) along with the Multi-protocol label switching (MPLS). It performs like a connection between the perception layer and application layer. The information collected from the physical objects with the help sensors is transmitted and stored with the help of this layer. It is accountable for dispensation of the networking data. It very well permits the network safety.

iv) The service and middle-ware layer looks a lot like the OSI model's three layers. It resembles the transport, session, and presentation layers. These communication protocols support high-level communication services. Unlike the OSI model, this layer has been substituted by a solitary middle-ware layer. This also contains application-independent protocols. [3] The layer precises and thereafter forwards various data formats along with the technologies to be used via some communication protocols of underlying layers. It deals with managing, filtering, accumulating data with the help of servers that ease cloud computing along with data mining technologies.

v)The application layer, resembles the same as application layer in OSI model defines all applications that use the IoT technology. OSI application layer permits customers to interrelate with other software application. Eventually the main aim is to safeguard the serviceability of IoT applications with less complexity and higher trustworthiness.

III. Applications of IoT in various fields and their concerns:

IoT technologies have numerous applications, it is adaptable to various technologies that are capable of supplying data about their operations, performance and even about the environmental conditions that we need to monitor. IoT networks can include unimaginable count of strategies with diverse features connected to resource limitations, flexibility, scalability and self-sufficiency. [4] Privacy concerns in IoT differ extensively w.r.t the applications included. The most dangerous part of IoT is that consumers are conceding their privacy, bit by bit, without realizing it, because they are uninformed of what data is being collected and how it is being used. Privacy gives right to users to preserve their confidential data as well as have control it in case of third-party discrepancy.

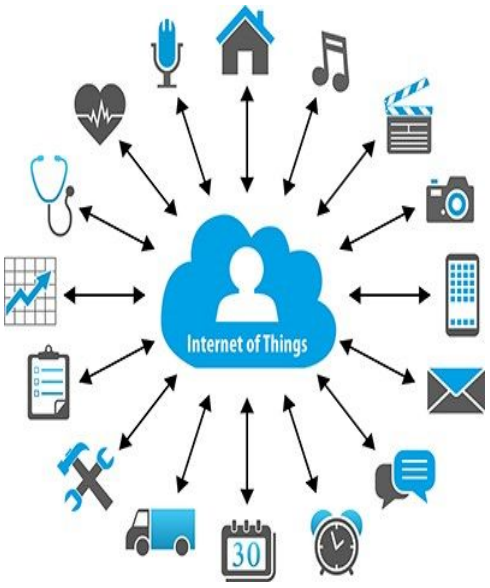

Fig. 2. Usage of IoT in daily life

A. Healthcare

IoT appliances have proven really beneficial in the health and wellness domains. Many wearable devices for monitoring health wellness levels are being developed. They help in monitoring user's health. It enables doctors to remotely monitor their patients. IoT applications can turn sensitive medical-based systems into proactive wellness-based systems. Although, making the personal health records easily available on the net is dangerous. There have been several cases proving

for privacy threats in this sector. The risk of using IoT in this field is vast, they can be cut down by making the privacy frameworks for IoT eHealth applications open to their patients as well as let them know the reasons for gathering their health data. It should maintain precise and accurate data, and ensuring safety of patient's data and their medical records. [5]

B. Smart Home:

Smart home is an umbrella term for the automation, digitization and interconnecting of several home automation areas, which have existed since quite some time. They can have features like controlling lighting of the room, blind control, solar shading, audio and video control, security and entry control, the list goes on. In smart home atmosphere, clients have the right to regulate, monitor, as well as measure power consumption of their home appliances. This can be done remotely with the help of Internet. This application of IoT has its own flaws, as Internet Service Providers might have access to all the operations done by the user and can collect important data about users' behaviours with or without their consent. This postures a potential threat to the users' confidentiality. However, there is a way by which this issue can be curbed; residents can use Radio-frequency Identification (RFID) and several detection devices which can trace and track objects. It can monitor the smart home environments and situations. There is still a high chance that intelligent challengers can spy and gather data communications over wireless stations. They can fetch inferences on behavioural patterns of the surroundings and use it for their own benefits. There is a loop hole in the solution of using sensors and RFID because they have tags which have exclusive radio wave patterns as well identifiers, with this additional info, invaders can analyse the transmission patterns. If needed they can disclose confidential information about the home's interior.

C. Public Safety:

IoT presents undeniable implications for public safety communications as they offer cheap substitutes to extensive arrangement of embedded monitoring units. IoT-enabled devices can provide numerous benefits to public safety. IoT exponentially expands the realm of the possible while providing ubiquitous network connectivity, real-time response and control of autonomous systems, enhanced situational awareness, and process optimization. However, the flaw here is, there are several connected modules which are used, but the users don't have complete access over them. This leaves governments and corporations with no other option but to trail users moves based on their consent. [6]

D. Supply Management:

This permits unified interoperability amidst RFID based claims and all steps followed throughout a lifespan of a product. This information is noted outside the manufacturing level to the procuring levels. Subsequently, information of the customer can be traced by the companies. Furthermore, vanets show a key part in the IoT via intelligent conveyance. Customers give out confidential information. This information can be not only be used to reveal their habits and behaviours but also threaten them to have confidentiality attacks and disclose their private data. The data about a user's electricity ingesting can be recruited from wherever in the world via the internet. Customers generally have fewer control over their own information that they supply to IT businesses and so, there are higher chances of confidentiality abuses.

IV. Privacy Problems and Encounters:

Several industries can obtain assistances from the Internet of Things (IoT).But more the number of devices affiliated, more complex is the IoT ecosystem. But this that security susceptibilities from edge to cloud is high. Developing an understanding of IoT cybersecurity issues with performing a strategy to alleviate the risks related and will help protect industries from losses and build confidence in digital transformation processes. The fig. 3. explains the four important features of IoT privacy.

Fig. 3. Challenges faced

A. Customer/User privacy:

In past few years user privacy has played a significant part in the development of the IoT services because of their privacy invasive nature. But still, there hasn't been a significant change in the research so far. That aims to understand users' idea of secrecy in connection with IoT. However, one serious issue can be identifying user's confidential data over the transmission via the internet. The purpose for the privacy apprehensions is because of the ubiquitous intellect combined artifacts where the selection process and the information distribution in the IoT may be done nearly in any place. Unless there is an exclusive mechanism put in place, then it will be definitely easier to access the personal information from anywhere in the internet. This can be done via the devices linked to net that customer uses on a daily basis. Because of the vast range of IoT's usage, privacy risks or applications should be measured before organizing a request.

B. Data mining:

Three key enablers of IoT secrecy from data concerned point of view are scalability, real-time analytics and distributed processing. The IoT environments are smart enough to generate large bulk of data which initially is raw data that has to be handled well before making it of any use. This information fits to environmental parameters that's of IoT's constructed environment.

A thought-provoking part of any IoT enabled smart environment is to the data mining algorithm. This algorithm can help produce valuable analytics, predict future events precisely and manage the network and services efficiently within all constrains.

[7] Scalability matters for IoT applications which have personal information of the users as it must be stores, processed and published in enormous volumes. Distributed processing can cause unrequired challenges which include liability for data breaches. It is certain that, collection of large files of data is difficult to manage and IoT has to ensure that it doesn't lose its data quality. Collection of data, sharing it is one of the most critical privacy issues of this applications.

Computational and proposed boundaries can be related to privacy conservancy over dimensional datasets. This is so, as individuals who are obliging users will have various secrecy restraints. Accounts in particular dataset should be treated differently for resolutions. Access control and conservation of certain type of data, should be provided with a privacy safety for the corresponding data owner. Computer storage mediums have capacities to store humongous bulk of data. [9]They also offer obtainability at minimal price. Subsequently, data which is generated, is most likely to be stored substantially, and thus digital overlooking may lead to privacy defilements from the customer's viewpoint.

C. Underlying IoT technologies:

Context-aware digital objects can be allowed by integration of RFID objects and IoT, which can represent physical objects. They will have skills and intellect to feel, connect, relate unconventionally. Authoritative rivals can be present and they can track all communications, track tags and mishandle them. They can get the channel data on the reader output all within a limited time period. Privacy issues of RFID technology related to customer's privacy and stalking as well as confining. This permits the making, misappropriation of complete customers profiles. Hence, it's necessary for RFID systems to offer obscurity, even if the tag is revealed.

Wireless sensor networks (WSNs) is important technology of the IoT network architecture. WSNs have intrinsic encounters in shielding confidentiality and avoid, secure existing techniques from being resettled in resource-constrained devices. They have self-organizing features and work in a wireless transmission medium. Privacy in WSNs can be taken care through information and context alignment.

Cloud computing provides a virtual infrastructure for IoT. Usage of the IoT in cloud at such a great extent has definitely enhanced the development ascendable IoT applications and business models. This virtual substructure can have and let omnipresent detection devices, objects, CSPs and users link via the network and work together on an individual virtual platform. They have become very closely allied upcoming internet technologies where one of them provides the other success. With cloud computing, users whether working individually or in cooperative stream, have access to all the cloud services at a minimum expenditure. They don't require to possess skilled familiarity of the fundamental technologies. Nonetheless, privacy defilements can occur. The customers won't have zero control over the data dispensation. Hence, the makers must take accountability for privacy protection by protecting users' personal information like identity, confidential data like policy commitments, transaction histories, etc. They should ensure that the users are provided a sense of transparency in their actions. It is really difficult to control user lock-in scenarios if the customers are too relied on a particular IoT CSP especially when they want to shift between IoT CSP's. This can be intimidating as due to the reliability and dependency customers have revealed enough important information to a particular CSP.

Vanets implant an on-board unit (OBU) into the automobile arrangement. It ensures safe communication links and provides validation to permit security and privacy in vanets. It behaves like a detection layer node in the IoT. Here, the node communicates to infrastructure as well as the rest of the peer vehicles. Therefore, the OBU requires extra units to sustenance data safety to specially to ensure user privacy equally to identity privacy and location privacy.

D. Establishment of Lawful Rules for IoT Privacy:

[8]Privacy is an obedience problem leaning at the joint of communal rules, human rights, and lawful dictates. Usually, the active countries' legislation is obligatory to support elementary confidentiality values and this can be best achieved over an association of constitutional and private organizations. A legal framework should be strong enough to ensure the queries and awareness of the customers. They also have to check up on the control of the users over the IoT products and services. A satisfactory and global framework should ensure that the complaints with the global legislation supplemented by the private sector are dealt with ease. In order to do so, the IoT's worldwide law makers are trying to find a common ground that can be set up for addressing these issues but also empower the existing ones. [10] A national level regulation cannot be acceptable because of its universal nature. The most challenging cases can be dealing with problems connected to setting up legal and lawful reserves in IoT safety protection. These can be the global market and its segregated nature, the participation of persistent environments and further development's complex nature.In this case, a self-regulated framework could work as its much simpler and cost friendly solution to preserve the privacy. However, this has a setback as its not enough for the applications and data provided by IoT as it a cluster of large-scale heterogeneous network developments.

V. Privacy Framework Features:

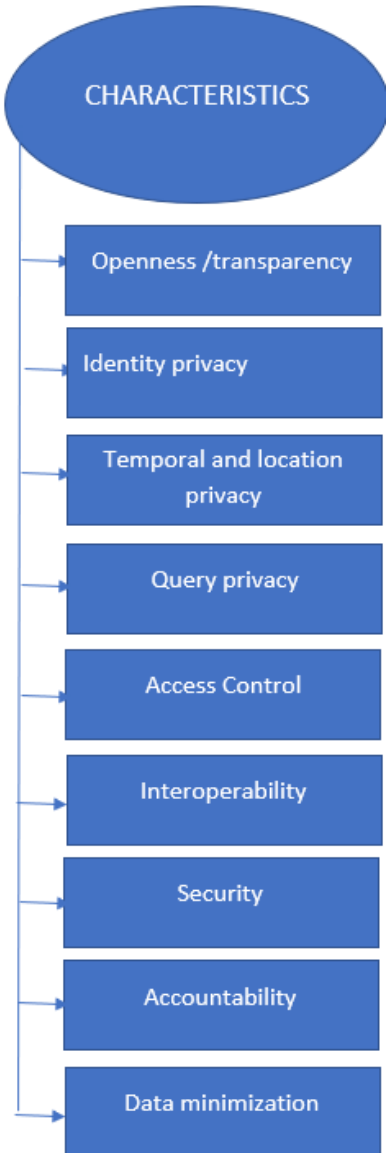

Fig. 4. Framework Characteristics

Some important features of an IoT privacy framework are [11]:

- Transparency with the user: This ensures that the users of this service are much aware of how their devices data is going to be collected during usage, the reason for it being collected and the transitions between different parties who can have access to their data along with knowing where and how is their data stored
- Identity privacy: Tracing the users based on their actual user identity shouldn't be easily hack able.
- Location privacy: Tracing users based on actions or geolocation shouldn't be easily hack able.
- Query privacy: Recognizing the users based on the inquiries they make to service providers shouldn't be easily available.
- Access control:The customers require and deserve to be given complete authority and control over the data they provide to the service providers. They should be manageable based on the users and their queries on data access.
- Interoperability: Ensure support of privacy policies worldwide.
- Data minimization: Collection of the data should be law abiding and done in all fair means with limitations to uploading personal data collection.
- Accountability: There should be a mutual agreement between the user and service provide about the authoritative rights, and discernibility of provider's accountability w.r.t the data provided by the user.
- Security: safeguard confidential information against any losses or illegal access or any alterations, or revelation.

The significance of these values might be varying liable on the frameworks of the IoT applications, their situations and customer requirements. Like healthcare, smart home, and surveillance applications require and expect high sensitivity regarding privacy-related issues. Most importantly, all the above-mentioned technical characteristics of the IoT privacy frameworks, should always ensure that it is in balance with the human and legal rights requirements.

VI. Present Solutions:

There are many privacy-enhancing technologies (PETs) are for IoT affiliated applications. Solutions related to the privacy-orientations have been introduced for confidentiality attacks occurring in WSNs. However, skilled attackers can hack into the cryptographical puzzles. They can violate the user's privacy by posing threats to the systems. Present PETs for RFID technologies comprise of restraining the path between tags and the reader, minimal cryptography. Also includes renaming the tags and deactivation and data's access control, and re-encryption. Minimalist cryptography is planned to enhance reader's end cryptographic computations. It stores the outcome of the information in the tags. The unique feature is that the reader can anytime re-encrypt the tag with different key sets and yet write it into its memory. This can be done in a method where a spy gets unique encrypted tag signals at uneven time periods.

There can a new approach to this. We can use different level of devise ranging from moderate to high-performance. This would help with RFID tags to safeguard the user's privacy. There are two main objectives of PETs in RFID. One is to ensure that the access to RFID tags via some unauthorized source is not allowed. This can be done by enabling protected tag-reader communication, which can safely secure the user privacy.

The "privacy coach" is a thought-provoking impression for ensuring user privacy in the IoT. It is a smart phone app that shows the customers how to make privacy decisions specifically concerned with RFID tags which are entrenched in objects.

Additional method is by using a proxy as a confidentiality broker for ensuring the privacy amongst service providers and users. This conveys that both the provider and user can know required data about one another. Moreover, privacy proxies can create scalability and interoperability problems.

Documents with high level abstraction of data and advanced software supplies of IoT privacy policies can use "The Unified Modelling Language" for the services provided by all the heterogeneous sources.

By trying the methods obtainable for individuality and location-privacy protection of the users. Customer's privacy in the IoT can be skilful by misusing public-key cryptographic algos and forwarding agents.

There are several privacy-preservation technologies for data mining which are inclusive of statistical methods. This can have a disclosure control. Privacy preserving is a data-centric perspective which is used to approach IoT.

On the other hand, cloud computing tries adapting various privacy-preserving methods which not just ensure data-centric, responsibility but also access control, the data authentication, and identity management. Above all in cloud computing, one must ensure that the services level agreements should be taken care and adjusted between the investors. This will help them preserve each individual party's privacy. The setback to this can be, that it always doesn't provide mechanisms with perfect solutions for a generic and worldwide perspective of IoT privacy preservation.

VII. Privacy by Design

The PbD is an effective approach because it provides a security requirement procedure which deals with the privacy concerns especially at plan stages of application disposition and considers it as structural in different identification and business processes. This is a judgement supported by both the European Commission and the FTC. It tries to safeguard IoT privacy by emphasising on various domains like sensing technologies, big data analysis, cloud computing, and legal regulations.

PbD comprises and works on seven fundamental principles:

- Forestall and prevent privacy-invasive events at the initial design stage.
- It should be aware and inform the raised queries by stating the purpose, the data collected and disclosure curb.
- Implant privacy into the key design.
- With a high success rate, it should achieve complete functionality.
- Ensure end-to-end security.
- Openness and transparency is the key.
- User's privacy should be given utmost importance.

VIII. Future scope and design guidelines:

Internet of Things (IoT) is mostly going to be the fundamental base to the next gen technologies coming up like 5G,6G and so on. But in order for it to go successful in the long run there are certain procedures and principles to followed because present PETs aren't very compatible with multiple underlying technologies. Privacy should be given utmost importance in the IoT applications especially from the viewpoint of people.

Two key principles that if followed, would help preserve policies. They are: User privacy should never be violated and it is important for maintaining user control of the operations. IoT technology workers should always know that if they can't get their consumers' trust and make them have confidence in the providers, the development of innovative utilizations of these new technologies gradually deteriorates. The crucial service providers of eHealth and surveillance applications should take a leap higher to ensure the preservation of their customers data and privacy.

We must know that IoT privacy cannot be completely relied on PbD's as it is still in its infant stage and a proper development is in process. But, to enforce the PbD solutions, we should:

i)Build and follow a easy and basic model for IoT privacy.

ii)Work on creative PET's so that we can enable PbD scalability in IoT.

iii)Implement solutions that are the best and most suitable for different IoT applications catering to all their privacy related needs.

The social IoT is an upcoming IoT model which helps thing create an autonomous social network. This has almost negligible human interference. It imposes all the rules in order to protect its consumers privacy especially when they are retrieving the outcomes of independent communications between objects.

There might be many unsolved privacy issues that might have come to light due to the sudden change in the use of genomic datasets as well as some software packages related to medical activities. It is very important to face and acquire control over mechanisms and policies.

There is a unique way to see through the privacy concerns by thinking about how we can use the concept of game theory. Game theory can be useful as its concept would give us a new look at analysing the privacy issues of the users and would also cut down on the economic expenditure there by striking a perfect balance between the trust of the user on the provider and safeguarding their privacy. By getting used to a network virtualization solution, like software-defined networks, this can be an effective way to preserve user privacy in huge scale data treatment IoT deployments and cloud management. Moreover, it is important to go approach and follow PETs as they can help IoT reach higher heights in research level and meet its goal along with having a practical use.

Nevertheless, finally there can be a set of research issues that might be raised to voice the privacy concerns accustomed to s other emerging technologies. The future is beholding magnificent possibilities which are ready to be unfolded.

IX. Conclusion:

The privacy issues we have faced and looked into in this research project require trustworthy applications to deal with them. Development of sophisticated privacy models will definitely give a practical and privacy-oriented security protocols

which are very important especially for further development in this field. Having a strong base by ensuring privacy assurance at the design level would not just ensure security amongst users but also would solve most of the challenges faced. It is very rare that these technical answers would suffice to more or less provide security in IoT related applications. So, we must strike a perfect balance by considering a blend of technical and legal means. This helps them attain privacy-enhancing solutions in IoT.

REFERENCES

[1] https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/
[2] https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2
[3] https://www.guru99.com/layers-of-osi-model.html
[4] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6165453/
[5] https://www.hindawi.com/journals/jece/2017/9324035/
[6] https://www.edureka.co/blog/iot-applications/healthcare
[7] https://www.cisa.gov/sites/default/files/publications/CISA
[8] https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats: :text=Insufficient
[9] https://www.sciencedirect.com/science/article/pii/S131915782030416X: :text=IoT
[10] https://www.iot-now.com/2020/06/03/103228-5-challenges-still-facing-the-internet-of-things/
[11] https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/