A picture containing text, clipart

Description automatically generatedShape, engineering drawing

Description automatically generated **Cairo University**

**Faculty of Graduate studies for Statistical Research**

**Department: Computer Sciences**

A Survey on IoT Security Issues And  
Enabling Technologies For Smart Homes

Pre-Master Graduation Project

**Submitted by**

**Ehsan Zeinhom Gaballah**

Under the Supervision of:

**Dr. Nesrein Abdelazem**

**2021**

**Abstract:**

The Internet of Things is a rapidly evolving technology in which interconnected computing devices and sensors share data over the network to decipher different problems and deliver new services. For example, IoT is the key enabling technology for smart homes. Smart home technology provides many facilities to users like temperature monitoring, smoke detection, automatic light control, smart locks, etc.

However, it also opens the door to new set of security and privacy issues, for example, the private data of users can be accessed by taking control over surveillance devices or activating false fire alarms, etc. These challenges make smart homes feeble to various types of security attacks and people are reluctant to adopt this technology due to the security issues.

In this survey, we throw light on IoT, how IoT is growing, objects and their specifications, the layered structure of the IoT environment, and various security challenges for each layer that occur in the smart home.

This survey not only presents the challenges and issues that emerge in IoT-based smart homes but also presents some solutions that would help to overcome these security challenges.

1. **Introduction:**

IoT-connected devices area unit foreseen to expand to seventy-five billion by 2025; in 2030, it'll bite 500 billion [1]. The net of Things (IoT) may be a well-known paradigm that defines a dynamic setting of interconnected computing devices with completely different elements for seamless property and information transfer. Technologies that area unit typically enforced within the IoT domain area unit machine-to-machine communication (M2M), context-aware computing and radiofrequency identification (RFID). Some typical samples of such proactively sensing and adapting objects include:

1. wearable devices like smartwatches, glasses, or health observance systems, ii)
2. good home appliances like good locks, sensors for temperature, gas, or close lightweight,
3. good vehicles, drones and applications for industrial automation and provision. IoT devices exchange information with scores of different devices round the globe.

Such style of open large-scale communication makes them particularly tantalizing for users with illegitimate intentions. Solely in 2017 there was 600 p.c increase in attacks against IoT devices [2].

1. **Introduction of IoT:**

In 1999, Massachusetts Institute of Technology (MIT), for the primary time, brought the construct of IoT. In recent years, the IoT paradigm has become a lot of widespread. IoT includes completely different hand-held devices like good phones, tablets, laptops, personal computers, and different embedded devices like good watches, good doors, good locks, etc. as shown in Figure 3. In IoT, devices communicate while not human interaction. All information is distributed and processed mechanically per the things, for instance, if some place catches fireplace, then all the sensing devices begin communication per the scene. Fireplace sensors sense the hearth associated trigger an alarm to activate different supporting devices to wipe out the hearth.

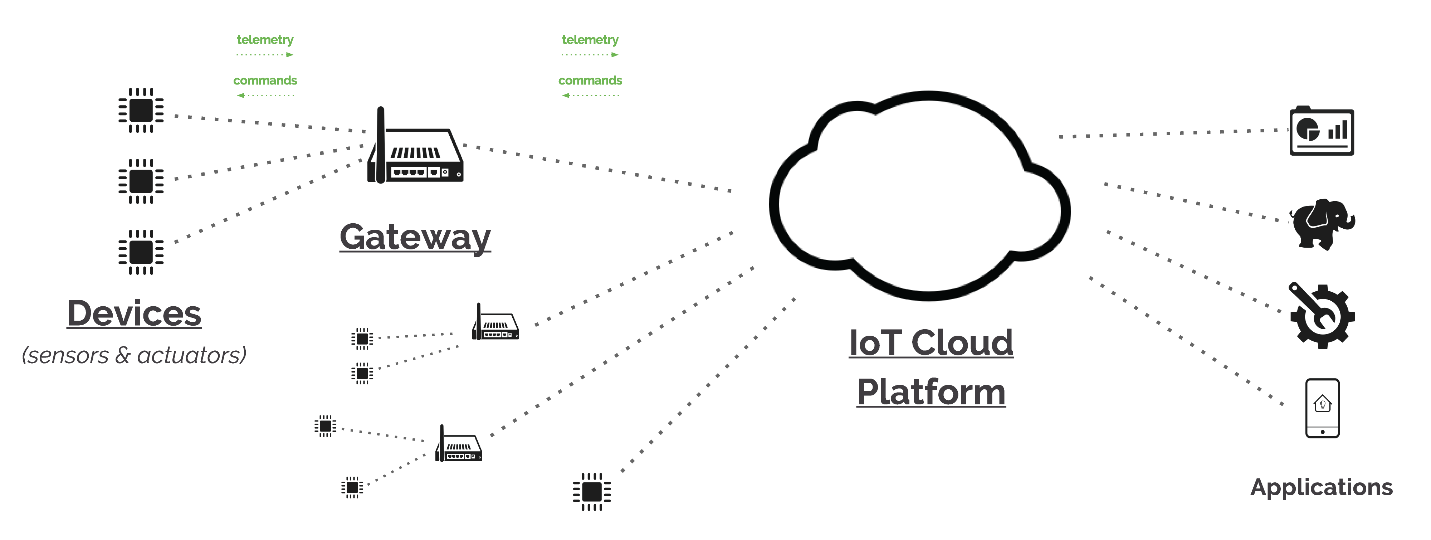


Figure 3: layers of IoT architecture

The meaning of the IoT may be an immense network connected by a spread of objects or processes through varied info sensing devices for intelligent recognition, positioning, tracker, police work, and management with the presence of the net [3]. The aim of the IoT is to attach all physical things in communication in order that they'll be integrated with computer-based systems a lot of directly and therefore the identification, management, and management are often simplified. [4]. The net of Things will bring advantages and services to people, businesses and societies by capturing and analyzing information from sensors at the endpoints of connected devices and mixing this information [5]. What is more, IoT improves comfort and potency through collaboration between good objects [6].

It is usually applied in varied aspects, beside personal health, public safety, industrial observation, intelligent transportation, environmental protection and completely different fields. As associate degree example, inside the manufacturing field, the instrumentality is typically remotely monitored, upgraded associate degree maintained from an extended distance away by fixing IoT based totally sensors on the instrumentality Moreover, the instrumentation makers square measure able to learn the utilization of the merchandise in a very higher manner, collect the information of the merchandise life cycle fully, thereby guiding the merchandise style and after-sales service [7].

This survey aims to alert users before an exploitation IoT services in their daily lives. During this manner, they need adequate data regarding the breaches and therefore will save themselves from hid attacks.

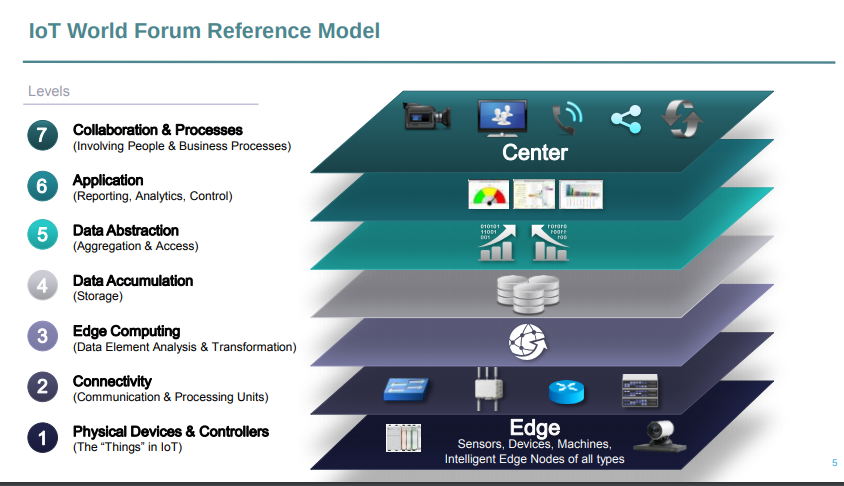
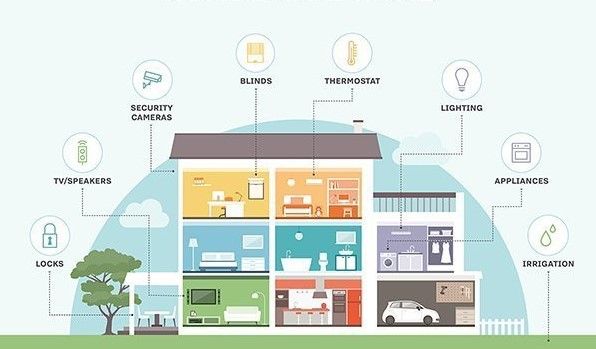


Figure1: layers of IoT architecture

**The smart home environment**

A smart home is an application of IoT environment, that contains of physical parts and web property. These devices communicate with one another and supply innovative and smart services to the user [8]. Smart heaters, smart coolers, smart televisions, smartwatches, mobile devices, and smart locks are IoT based mostly smart home appliances that are connected with the web and build the life of an individual's easier [9]. With a wise home automation environment, we are able to management and monitor the home appliances, like lighting, temperature, the climate of home, doors, and windows [10]. Though smart homes are a lot of convenient to use and management all home appliances, however, thanks to the web property likewise because the dynamic and heterogeneous nature, the smart homes face  
different security issues [11].



As in smart homes environment, superfluity of smart devices is interconnected and need info exchange, the design of IoT environment has become heterogeneous and because of the nonuniformity, these devices are prone to security attacks [24].

ISO 27005 outlined attack because the ability to require over the vulnerabilities of the premises and lead the organization to an enormous loss [61]. Security attack within the digital world is termed as associate degree criminal activity performed by associate degree trespasser against a network and acquire access to the network to form changes  
that can lead users to the loss of their sensitive knowledge. Associate degree assailant will monitor the various activities of the good home user through the data collected by the good devices.

What is more, associate degree trespasser might head of the good home devices remotely and may use the devices for his malicious functions, inflicting a billion greenbacks lost to the owner of a sensible home. Flourishing attacks on numerous businesses of-the shelf merchandise are performed. These attacks don't seem to be solely hypothetical, e.g., in 2014, over 73,000 video cameras were additionally found to be streaming their police work footage on the net.

As discussed, in [4], In 2016, each IoT device was attacked once in each 2 minutes.

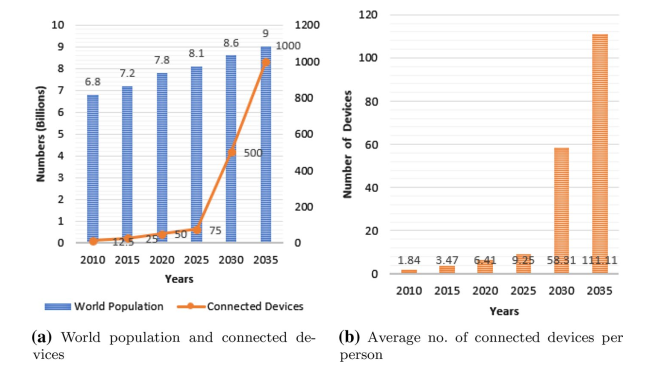


Figure 2: World population, active devices and average no. of connected devices per person

Consistent with a recent study by H.P., currently, nearly seventieth of a sensible devices' an area unit susceptible to security threats. Another study by H.P. reveals that a ninetieth of devices has collected personal data throughout the testing part. This information will be used for malicious functions because of compromised the device or as a result of a cyber-attack. Hence, the user is going to be reluctant to use these sensible devices because of their vulnerability to security attacks.  
The planned work offers a revelation concerning the safety problems in sensible Homes. This work includes the safety issues at the IoT’s layer and discusses the solutions to those issues. In today’s life, wherever the web is swamped, it causes various security issues. Thus, it's required to teach folks concerning malicious activities over the web. This survey aims to alert users before exploitation IoT services in their daily lives.

During this method, they need adequate information concerning the breaches and therefore will save themselves from hid attacks among many issues, wireless network security is that the highest priority issue to be resolved for the IoT. There are a unit various surveys within the literature for IoT’s issues and solutions, however, not all existing surveys cowl all the problems and connected solutions. They typically cover partially every IoT layer relating to security challenges and connected countermeasures. Finding every issue and answer for that issue is that the motivation behind this survey over IoT, security issues, and solutions at every layer.

In this paper, we present an overview of IoT architecture and layer assembly of the IoT network environment. We also elaborate a systematic study of the critical security issues and mitigation approaches.

1. **Related works**

The related work comprised of assorted researches within the field of IoT concerning Intrusion Detection Systems. This portion is created from the works projected between 2010 and 2020 and was supported by scientific publications accessible within the scientific repository (IEEE Explore, ACM Digital Library, Science Direct, Springer Link, Google Scholar). This production provides exposure to the works associated with the required topic. During this regard, the summary of assorted projected analysis works is given with relevance layer’s security problems.  
Table one illustrates the work is completed up to now on the protection issues and mitigation ways in keeping with IoT layer structure.  
In [17], Geneiatakis et al. mentioned that the IoT system provides support to numerous sorts of applications like smart industries, smart cities, and smart homes. Smart objects utilized in these applications move with alternative elements like mobile devices, information collectors, etc. to produce numerous services. Whereas providing services, it additionally takes users to security and privacy threats because of their restricted process.  
So, during this paper, we tend to place some lightweight on a number of the key security and privacy laws victimization of the shelf elements. For this, they apply smart home IoT design and create users able to move with it. Then, they analyze completely different situations that they will simply determine attainable security and privacy issues and projected solutions for them.  
Ali et al. [12] examined that IoT is making day by day and creating a world wherever material things like shrewd cities, keen homes, etc. are providing innovative and savvy administrations to individuals. Keen homes provide varied administrations through electronic communication Innovation (ICT). But thanks to its heterogeneous nature, it leads to some major security problems. therefore, during this paper, they place the investigation on some of the attacks and check their impact on the general system to predict correct solutions.

The main contribution during this paper is that the authors set some security goals, and in a step with that they predict what number attacks a square measure expected to be launched within the returning years. The aim of this analysis is to arrange well before the arrival of attacks.  
In [13], Zarah et al. Proposed that thanks to rise in IoT, smart homes became one in all the essential domains. Moreover, it's associate degree interconnected home wherever things act with one another through the net. It is very beneficial for users and provides several facilities, however at identical time, it also faces several security issues which require to be resolved. Tons of analysis is carried out in that the researchers mentioned these issues and bestowed different forms of approaches to handle these problems. During this paper, we've analyzed the sensible home approaches, security issues and additionally steered the simplest possible solutions to create the sensible homes secure from these forms of attacks.

Table 1 Comparison of existing surveys about smart home security issues and several solutions. ✓ shows fully covered, ✗ shows not covered and \* shows partially covered

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ref. | Year | Topic | App. layer | Phys. layer | Net. layer | Percpt. layer | Security solutions |
| Geneiatakis et al. [17] | 2017 | Smart home | ∗ | ✓ | ∗ | ∗ | ∗ |
| Ali et al. [12] | 2017 | Smart home | ∗ | ∗ | ∗ | ✗ | ∗ |
| Zarah et al. [13] | 2013 | Smart home | ∗ |  | ∗ | ∗ | ∗ |
| Arabo et al. [14] | 2019 | Smart devices | ∗ | ∗ | ∗ | ∗ | ✓ |
| Gendreau et al. [16] | 2016 | IDS | ∗ | ✗ | ✗ | ✗ | ∗ |
| Salman et al. [19] | 2018 | SDN | ✗ | ✗ | ✗ | ✗ | ∗ |
| Zarpelao et al. [20] | 2017 | IDS | ✗ | ✗ | ✗ | ✗ | ∗ |
| Pongal et al. [18] | 2015 | 6LoWPAN and RPL | ✓ | ✓ | ∗ | ✗ | ∗ |
| Elrawy et al. [15] | 2018 | IDS performance parameters | ✗ | ✗ | ✗ | ✗ | ∗ |

Arabo et al. [14] Expounded the patterns and challenges of savvy gadgets in smart homes through cybersecurity. They talked about that these shrewd gadgets offer some practicality to clients. Be that because it might, whereas giving more quality, it too takes users to unused dangers and dangers. During this paper, cybersecurity problems associated with sensible devices are talked about. They considered versatile malware is one of the foremost security issues in shrewd devices. They, too, anticipated that in close future clients will anticipate an outsized range of malware-related assaults because of moveable savvy convenience, particularly on the humanoid stage. The foremost reason of this paper is to focus on conceivable security dangers in keen gadgets, what is more it examined the challenges enclosed in mobile malware, and final one is to propose a security arrangement that may handle these types of dangers.

Gendreau et al. [16] examined that IoT is that the wide making innovation, however with this quick advancement in IoT, it what is more faces varied security issues. These issues become a barrier to high accessibility, dependability of the network, and security of information. During this paper, the authors projected Intrusion Detection systems (IDS) that area unit overwhelming the foremost original ideas to create IoT a lot of secure and guarded. They take begin with the history of IDS systems from wherever they were initiated and the way they're operating of late. They additionally argued on several open-source issues that are encountered by IDS systems.

Salman et al. [19] discussed that the web presents Quality of Service (QoS) and associated security issues, however within the situation of IoT, some of these challenges become additional crucial. During this paper, the authors conferred four leading IoT-specific challenges and additionally anticipated solutions to the issues that facilitate to resolve these challenges. The projected SDN-based solutions are combined with fog computing.

This is as a result of SDN incorporates a universal observation of network and may gift additional economical solutions to create them secure, however on the opposite hand, fog computing is employed to bring cloud within the network. By this, the network becomes climbable and additional responsive.

Zarpelao et al. [20] Deliberated totally different sorts of security problems that IoT is facing and mentioned that their area unit several techniques that area unit want to eradicate these problems to safeguard IoT devices. However, from these techniques, various of them area unit often prone to various attacks. During this survey paper, the authors anticipated IDS to find totally different sorts of attacks. They planned IDS system as a result of they found that this system is pretty appurtenant to safeguard IoT. They conjointly explained however totally different reasonably open issues is changing into a hurdle to IDS enlargement and what area unit the solutions to those problems.

Pongal et al. [18] Discuss that 6LoWPAN is an IPV6 header compression protocol which will squarely become the target of the attackers. To handle these attacks, RPL is designed, that may be a network layer routing protocol. RPL may be a lightweight protocol and may conjointly go under attacks. So, during this paper, they stressed multiple attacks that were dangerous for each RPL and 6LoWPAN. They conjointly provided countermeasures toward these attacks to create a secure network. They conjointly mentioned consequences which will occur because of the network parameters once applying solutions. What is more, they conjointly intimated that their square measure several attacks on RPL that aren't evaluated yet.

Elrawy et al. [15] carried a survey regarding IDS. During this work, they surveyed the IDS as a security answer for IoT. During this work, numerous styles and approaches of IDS area unit conferred that area unit operative within the IoT surroundings. They primarily targeted on the performance factors of IOT instrumentality, like correct detection, energy consumption, time taken for process, and performance overhead. They conjointly lined to some extent IoT systems, what's wise surroundings, and a summary of IDSs. moreover, it's conjointly mentioned that ancient IDSs area unit did not work properly against security attacks thanks to IoT network selection and protocols. They also provided future recommendations on the strengths and weaknesses of current IDS. IoT faces varied security challenges from different aspects, like communication protocols and hardware equipment. IoT devices have less memory, short battery time, that causes them to possess low procedure power devices. Gateways connect IoT devices to the outer world which can cause security problems.

A compromised node might cause associate info breach. Associate trespasser will cause issues by manipulating a device physically. A natural disaster will damage IoT devices, which can produce any security threats. Network layer would be liable to a superfluity of security issues because it plays a crucial role within the IoT surroundings. Figure 5 shows the design of the IoT network. The entrance acts as a threshold between IoT devices (smart A.C., smart locks, smart lights, smoke sensors, and noise sensors) and management devices (laptops and user’s mobile phones). Controlling devices and IoT devices are connected through the cloud.

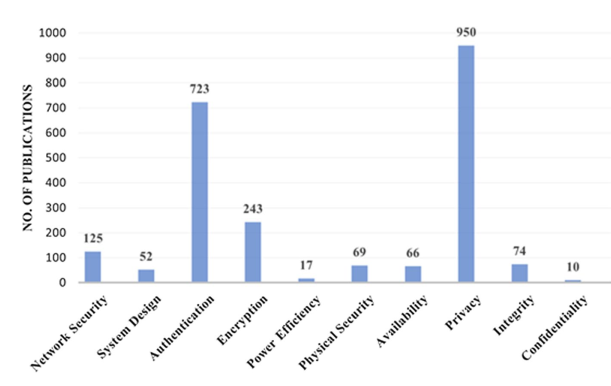


Figure 5 Trends of research studies on the security of IoT devices

1. **IoT layer’s structure**

Figure 6 illustrates the layer's architecture of the IoT environment. These layers accomplish the objective of IoT. Below are the main layers that take part in the IoT objective.

**1. Application layer**

All the applications and services that IoT provides, like smart cities, smart homes, smart hospitals, and intelligent transportation, reside within the Application Layer. The application layer is one among the highest essential layers that should demarcate all applications, wherever the IoT system is deployed. It acts as an interface between network and IoT devices. This is the layer, that has the authority to verify applications are gaining services or not. It also has the authority to deliver different services to different applications per data gathered by sensors. It has many problems, but still, security is on the top of the list.

**2. Perception layer**

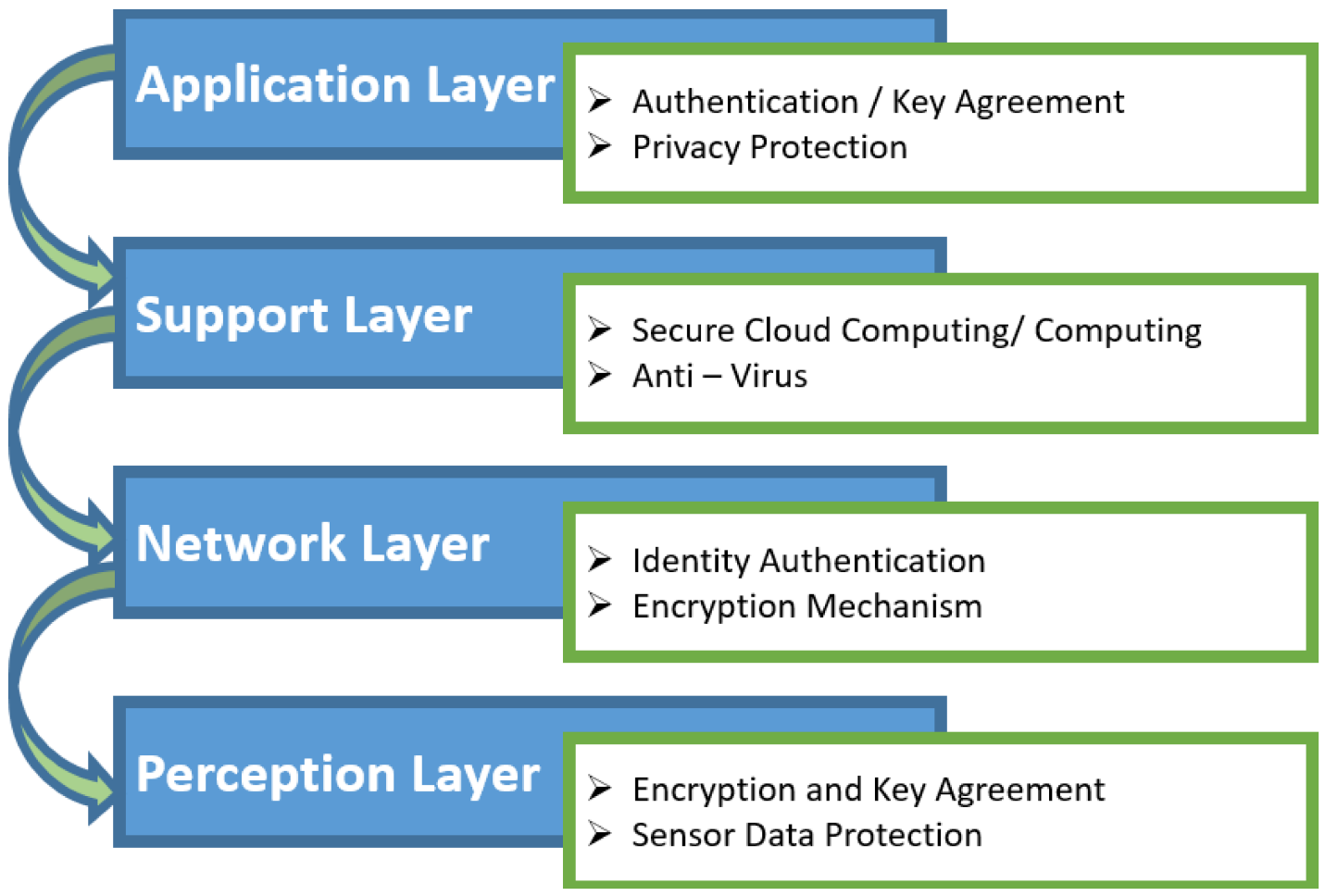
Different devices or technologies that perceive the input from the setting are an area of a perception layer. These devices and technologies are pressure sensors, smoke sensors, vibration sensors, and RFID sensors. The foremost perform of the perception layer is to conjointly modestly technique data, which will be a fraction of a scholar. It's put together to recognized as conjointly extension layer. Varied problems exist on this layer. The foremost draw back that must be resolved could be an assortment and capturing data.

Figure 6 IoT layers structure

**3. Network layer**

The network layer consists of network communication software (like topologies) and network devices (like servers and network nodes) that help totally different devices to communicate with each other. It's also acknowledged as a transmission layer. The key feature of this layer is to send knowledge to finish devices and the devices in between the top nodes. It's established on mobile telecommunication and the one of. One among the foremost persistence of this layer is to deliver information through in depth distance. In different words, it acts as a bridge. The most objective of this bridge is to move knowledge from objects through sensors. The medium provided during this layer may be wired or wireless. Networks and network devices area unit related to one another through this layer.

**4. Physical layer**

**T**he physical layer includes hardware devices or physical parts like power provides, smart appliances, and smartphones. These are the backbone of

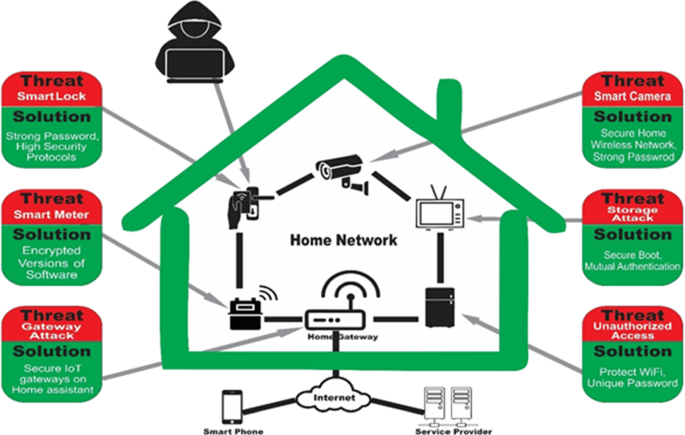
the IoT world. This layer includes sensors that facilitate in sensing the environment, consequently gather info from the environment. This layer additionally senses different objects within the environment. IoT environment involves smart devices and web property. Each connected device communicates to a different device to perform the specified task. Smart devices embody laptops, personal computers, mobile phones, tablets, smart A.C., smart TV, and different wearables.

Figure 4 Smart home architecture

Table 2 Application layer security issues

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. | Application layer security issues | Sol. | Tools and techniques |
| 1 | Phishing attack | [21] | Visual similarity and data mining |
| 2 | Manipulation of an unstable confguration | [22] | Markov model |
| 3 | Reconfiguring remote devices attack | [23] | Point to point encryption |
| 4 | Hacking into the smart meter/grid | [24] | Rabin encryption cryptosystem |
| 5 | Malicious code attack | [25] | Status-based detection |
| 6 | Attacks on access control | [26] | Role-based authentication |
| 7 | Tampering with node-based applications | [27] | Proactive digital forensics, Holochain and fog computing |

**Smart home problems**

The flexibility and arrangement of IoT innovation are expanding day by day, thus, more and more smart gadgets are associated to the Web [28]. As examined in Sec.B, the IoT environment is based on four layers. In this way, to guarantee the security of the smart home, we must send security at each layer. Figure 4 portrays a smart home format in which smart gadgets are associated to a portal that interfaces the devices to the Web. The portal acts as the bridge between the Web and smart gadgets. Different security assaults are too highlighted in Figure 6 that appear how a gatecrasher can take advantage of security vulnerabilities and seizes the network. In addition, the security issues related to each layer are talked about. Besides, an overview of the security challenges at each IOT layer is highlighted in Tables 3, 4, and 5 alongside the arrangement of each issue and tools/techniques.

Table 3 Smart devices with specifications

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sr. | Device type | chipset | RAM(GB) | | Power | Network protocol | Flash memory (GB) | Core freq. (GHz) |
| 1 | Wink hub 2 | ARM cortex-M3 | 0.512 | Battery | | WIFI 802.11 | 0.064 | 1 |
| 2 | Samsung smart things hub | ARM cortex-A7 | 0.256 | Battery | | WIFI, Bluetooth | 4 | 0.528 |
| 3 | Amazon echo | ARM cortex-A8 | 0.256 | Battery | | WIFI 802.11 | 4 | 0.8 |
| 4 | Philips hue | Ambiance A19 | 0.004 | AC | | WIFI 802.11 | 64 | 1.7 |
| 5 | TP link HS200 | AR7240 | 0.032 | Battery | | WIFI, Bluetooth, NFC | 0.04 | 0.4 |
| 6 | LG smart TV | ARM cortex-A53 | 2 | Battery | | WIFI, Bluetooth | 8 | 1.1 |
| 7 | Samsung smart cam | Micro SDXC | N/A | AC | | WIFI, NFC | 32 | Up to 0.54 |

Table 4 Application layer security issues

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. | Application layer security issues | Solutions | Tools and techniques |
| 1 | Phishing attack | 21 | Visual similarity and data mining |
| 2 | Manipulation of an unstable configuration | 22 | Markov model |
| 3 | Reconfiguring remote devices attack | 23 | Point to point encryption |
| 4 | Hacking into the smart meter/grid | 24 | Rabin encryption cryptosystem |
| 5 | Malicious code attack | 36 | Status-based detection |
| 6 | Attacks on access control | 25 | Role-based authentication |

Table 5 Perception layer security issues

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. | Perception layer security issues | Solutions | Tools and techniques |
| 1 | Eavesdropping | 29 | Visible light communication |
| 2 | Booting attacks | 30 | Field programmable gate array |
| 3 | Side-channel attacks | 31 | Rekeying and masking |
| 4 | Noise in data | 32 | ANR (automatic noise reduction) |

**Application layer security breaches**

The application can be prematurely ended or can be utilized within the off-base way due to blur security. Consequently, the application fails to achieve desires for which it is to be programmed. As a result of the attack, this layer can create bugs within the application program that leads it to operate strangely. Underneath are common dangers at the application layer. Table 4 gives a diagram of the assaults within the Application layer.

* **Phishing attack**

In this attack, the gatecrasher gets access to organize using the mail of high-ranking staff of the organization. Assailants get access to delicate data and may harm the confidentiality of the organization which may lead to huge misfortunes. In [33], Nirmal et al. examined that these assaults are most expected within the gadgets that are associated to the Web. This attack is on the rise for the past few a long time. The reason of this rise is that aggressors are empowered with a huge sum for the incitement of the assaults. Various creators announce phishing as personality burglary since the assailant confounds the guest either by giving an identical web page to the first one or imagine himself as a genuine client [34, 35].

* **Malicious code attack**

This type of assault can be a pernicious worm circulating over the Web that can hit the implanted gadgets running a specific operating system such as Linux. Such a worm can target an extend of little gadgets having an Online association, like security cameras and switches. This may to break into the car’s Wi-Fi and take control over the controlling wheels and let it crash, resulting in several wounds to the guiltless [28].

In [36], Dongdi et al. talked about such kind of assaults and summarized into three categories. Botnet Mirai assault falls within the category where interlopers tune in to the network activity and sniff the traffic [37]. Ransomware assault could be a sort of pernicious code that sends parcels either for assault or communication. It gets access to the application and spreads itself into the casualty application. Subsequently, it scrambles the target framework and at the conclusion locks the framework. The final category bargains with equipment or sensor control [38].

* **Attacks on access control**

The IoT environment is altogether confidential. Any compromised gadget or individual can harm the confidentiality, and the complete environment gets to be helpless to various attacks. Get to control may be a handle that guarantees as it were an authentic individual can get to the information [39]. According to Bhawna et al. [40], get to control attacks take put when a true method for get to control is damaged.

This procedure gives permission to as it were true clients, forms, or applications to use the framework. Get to control attack is one of the basic assaults. Once access control is compromised, at that point the entire system becomes helpless to attackers.

* **Hacking into the smart meter/grid**

Utility bills of smart homes are powerfully produced through the smart meter; it sends the utilization of the control utilization and other resources to the concerning specialists. So, it must be secured since one can track the accessibility of the individual within the home based on power utilization. So, this may fetch billions of dollars. In [41], Zhiwei et al. characterize keen meter assault as the duplication of the bona fide shrewd meter by the aggressor. The unessential information shared by the compromised meter devour the transmission capacity for no reason.

* **Noise in data**

As gadgets within the smart home are associated through a remote medium, so when information covers a critical distance, it is very possible that it can contain inadequate, insignificant, and wrong data. Such unessential data can cause smart home gadgets to perform undesirable or indeed more regrettable activities that can lead to hurtful comes about. Noise in information in IoT means that it could be a risk to the sensor’s information. As the gadgets are connecting increasingly to the arrangement, this issue is additionally rising with them. Electric components that are interior or exterior of the IoT gadgets cause this sort of noise [42].

* **Manipulation of an unstable configuration**

Usually, in the IoT environment, a few components like inaccessible servers, operating systems, and capacity servers are used for running IoT applications. It is very conceivable that these administrations are arranged disgracefully and may lead to security issues within the application layer [1].

**Security problems in the perception layer:**

Hackers target the hub level, as these are a buildup of sensors and are favorite to hackers. Hackers make utilize of these to replace the device software with their own. Generally, dangers at discernment come from exterior substances and the gadgets with sensors play a key part to form it happen. Table 5 summarizes perception layer’s issues. A few common issues within the perception layer are talked about below.

* **Eavesdropping**

The devices inside the smart home communicate with each other and also with the server through the Internet. This will lead to spying since these devices are ordinarily left unattended. In this case, reliable devices can send push notifications to the smart home client and would be able to assemble private data [43]. In IoT networks numerous sorts of devices are communicating with each other through a nearby communication station in which a third party can involve and access their private data and this strategy is known as eavesdropping [44].

* **Booting attacks**

In edge devices, built-in security components don't work at the time of the boot prepare. During this process, devices gotten to be helpless to different security attacks. Attackers take advantage of this weakness and target the devices for their noxious purposes. Subsequently, it is essential to make devices unsettled against vulnerabilities during the booting process [39]. A booting attack is applied at the start of the system when devices are getting prepared to communicate or security algorithms are not installed yet. Through physical communication protocols, the attackers can do their job indeed on the off chance that devices are not in communication mode. These protocols are UART or JTAG [45].

* **Noise in data**

As devices in the smart home are connected through a wireless medium, so when data cover a significant remove, it is very possible that it can contain incomplete, unimportant, and false information. Such unimportant information can cause smart home devices to perform unwanted or indeed worse actions that can lead to harmful results [45]. Noise in data in IoT means that it is a threat to the sensor’s data. As the devices are connecting increasingly to the network, this issue is additionally rising with them. Electric components that are interior or exterior of the IoT devices cause this type of noise [44].

* **Side‑channel attacks**

Side-channel attacks are another source of leakage of sensitive information. Factors like power usage, architecture, and way of communication of sensor devices uncover information to attackers. Side-channel attacks are triggered through power usage, timing attacks, electromagnetic attacks, and laser-based attacks [39]. According to [46], side-channel attack is one of the foremost popular techniques to break down the security of an encrypted system. It breaks the security by using valuable information that's gotten away by the physical devices.

**Security issues in the network layer:**

The network layer is dependable for the trade of data between the devices. As a result, blockage of data moreover happens at this layer. The foremost security issues of this layer are the astuteness and confirmation of information that's to be conveyed to concerned devices. Noticeable security dangers over the network layer are talked about underneath. Table 6 gives a diagram of attacks inside the network layer.

Table 6 Network layer security issues

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. | Network layer security issues | Solutions | Tools and techniques |
| 1 | DoS attack | 47 | IDS framework |
| 2 | Unauthorized access | 48 | Role-based access control authorization |
| 3 | Man-in-middle attack | 51 | IDS and IPS (instruction prevention system) |
| 4 | Data transit attack | 52 | Multi-factor device authentication |

* **DoS attack**

A large amount of data is sent to servers or devices; as a result, those are incapable to reply to anything other than this bombarded data. An overflow of data is sent over the channel, and it produces blockage over the link, and the sender and receiver gotten to be dumb [49]. When a DoS attack happens, it shuts down the network and the user’s get to is denied. It accomplishes this by allowing the nourishment to track on the target or sending the information that did a crash. In both cases, it takes the access of clients from the service they expected [50].

* **Unauthorized access**

If the smart home devices are cleared out open and the owner expects that these are in safe hands. These devices can be available by unauthorized clients. An unauthorized client can utilize these sensible devices for flute purposes. In [53], Hossain et al. examined that unauthorized get to the medical environment is horrible, because it can murder the patients. Unauthorized get to actuators or sensors can control the patient’s records which can damage the safety measure cycle. Hussain et al. discussed in [52] that unauthorized get to the RFID hubs can lead to information spillage. The gatecrasher can get access to the sensitive information and possibly alter the node data. When an attacker gets access to the RFID nodes, he can easily read or write the node information. This wonder may lead to encourage fatal attacks on the IoT network.

* **Man‑in‑middle attack**

In this type of attack, the attacker does not bother to be physically present at the victim’s place. The attacker gets the information through IoT protocols. By utilizing protocols, he disturbs the communication between two gadgets and collects wanted data. Agreeing to Kim et al. in [54], this sort of attack, the malicious actors (attackers) create a hurdle between the communication of two systems. They can get access to the information that these two systems were attempting to share. In this way, the attackers can take the private data of these systems.

* **Data transit attack**

A large amount of information trades among IoT applications, like sensors, actuators, and capacity servers. Data is the foremost important resource of any client and hence attackers continuously target private data for malicious purposes. Stored data includes a security risk, but the type of data between communication channels has most extreme chances to become helpless. Along with sensor devices, different technologies are utilized within the data exchange, which increments the chances of making the IoT environment a data breach [39].

**Physical layer security breaches:**

Power supplies are the backbone of smart home devices. There must be such a mechanism through which these devices can survive during a power interruption. At this layer, devices must be kept safe from the weather and the individual. New technologies should be implemented to ensure the safety of power resources and physical attacks [28]. Table 7 summarizes Physical layer’s issues.

Table 7 Physical layer security issues

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. | Physical layer security issues | Solutions | Tools and techniques |
| 1 | Physical damage | 64 | Puf-based protocols |
| 2 | Jamming | 62 | Identity verification protocol |
| 3 | Duplication of a device | 63 | SDN-based approach |
| 4 | Duplication of tags | 47 | Quantum key distribution |

* **Physical damage**

This may be a direct approach of attackers to damage the physical devices of the smart homes, like, sensors, nodes and actuators. Consequently, these devices are unable to take part in the network and failed to work smoothly [56]. According to [55], this may concern with physical devices which can occur by a malicious actor of abnormal environment. By this vulnerability, the devices may lose their functionality and can generate other risks.

* **Jamming**

In jamming, radio signals are assaulted on the victim network or device to disturb the communication. Much thicker jamming can paralyze the complete network. Due to jamming, battery drain rate of the devices increments because it should re-transmit the data due to disturbed communication [29]. In [65], the creators discussed that sticking is one of the foremost dangerous security attacks in wireless sensor network (WSN)-based IoT. By blocking the channel, it breaks the circulation of a network. An attacker can easily jam the track on the wireless channel.

* **Duplication of a device**

Features of a genuine network device can be changed by malicious manufacturers, like hardware, software, and configurations. The affected device could run malicious software to target genuine device or damage the operations of other network devices. A malicious actor (like an attacker) makes a clone device in an IoT network. By that device, they have almost full access to the network and consequently damage the network [57].

* **Duplication of tags**

Gatecrashers can effectively capture the tags that are conveyed on different objects. Attackers create clones of such tags and deceive RFID readers by compromising the RFID framework. All the objects having labels on them are powerless to physical attacks. According to Data et al. [58] in specific RFID systems, the attacker tries to understand the security protocols. With this information, the attacker tries to blank the tags by composing gotten information within the same format.

1. **Some Solutions of smart home’s problems**

* **Application layer**

The application layer is dependable for the administrations conveyed by the IoT environment, such as shrewd cities, smart homes, smart hospitals, and shrewdly transportation. Such applications can be chosen, or an interloper may use them in an awful way to hurt the masses. Subsequently, the application fails to achieve the needs for which it was modified. Arrangements for the application layer’s issues are discussed below.

* Fighting against phishing

Gupta et al. in [21] proposed various schemes to fight against phishing like network protection based on blacklist scheme, or schemes such as heuristic, in which erroneous emails are blocked either on client-side or server-side. Users should be educated to such an extent that they can differentiate between a phishing website and a normal website. Other solutions like network-level protection and user authentication can help to diagnose phishing attacks.

* Tamper resistance

IoT devices should be designed as tamper resistance. Sensors that can detect tampering should be deployed on devices. If devices are not tampering with resistance, they should be kept in a secure place where devices are inaccessible for irrelevant people.

* Secure smart meter

Gawade et al. in [24] used Rabin encryption that helps to ensure that data is sent to legitimate authorities, and data delivery is safe from attackers. The sensor should be deployed to make the meter tamper resistance and measure the parameters (current, voltage) regularly. A certain threshold can be fixed to avoid the overflow of parameters.

* Countermeasure of misconfiguration

IoT devices should be shipped with up-to-date software and replace with devices that are running outdated software. As in the IoT environment, heterogeneity exists; therefore, interoperable devices can reduce the chances of misconfiguration

* Countermeasure of remote reprogramming attacks

User authentication ensures that only legitimate user can reprogram devices through the remote source. Ant-replay protocol, which is a subprotocol of IPsec, prevents the network packets by an intruder to make changes in packets.

* **Perception layer**

The perception layer consists of the devices that act as sensors in IoT. Information perceived from the environment is a thorough production of the perception layer. This layer needs much security compared to other layers. Several security solutions regarding the perception layer are discussed below.

* + Security against eavesdropping

Li et al. in [59] proposed a system in which activities of eavesdroppers are monitored. In this work, channel specifications are known in advance, and different antennas are also deployed. For analysis purposes, a formal analytical model is suggested by taking into account different effects like path loss effect, shadow fading effect, and Rayleigh fading effect.

* + Sniffing detection

To avoid sniffing, the devices should be connected to trustworthy networks and must not be connected to public places network. Wi-Fi offered by public places is not monitored properly and may contain bugs. Attackers sniffing these networks or build a new network on their own and use names of public places such as Free Airport Wi-Fi and Free Bus Stand Wi-Fi. Nearby users connect with this malicious node and send data through this service. Encryption plays an important role in securing network track that encrypts all the data which leaves the IoT system. However, data capture intruders would not make sense of it.

* + Secure boot process

Insecure boot process when the device is turned on, it operates cryptographic code signing techniques. A code developed by a trustworthy vendor or original equipment manufacturer (OEM) is executed on the device. By utilizing a secure boot mechanism, one can minimize the chances of replication of firmware code by an attacker.

* + Defensive mechanism against side‑channel attacks

On the hardware level, information-aware hardware, randomization, and partitioning are used to prevent information leakage. On software-level algorithms like leakage resilient public-key encryption scheme is run that guarantee the confidentiality of information even when some bits are lost.

* **Physical layer**

The physical layer comprises the hardware devices or physical components like, power supplies, smart appliances and smartphones. Power supplies are the backbone of smart home devices. There must be such a mechanism through which these devices can survive during a power interruption. On this layer, devices must be kept safe from the weather. Solutions to such problems are discussed below.

* + Countermeasure of tag cloning

Kamaludin et al. [60] proposed an accurate and effective method to detect cloned RFID tags in RFID systems. The suggested approach is built on the accuracy of dual hash collisions and a count-min sketch vector. A dual independent hash function is used to map streaming tag reading data. In this system, the combined functionality of dual hash collection and tag reading frequency is carried out to detect duplication of tags.

* + Network monitoring

Denial of service (DOS) mostly targets network protocol running on the Io based smart homes. An intrusion detection system (IDS) plays an important role in detecting, monitoring, and classifying these attacks. IDS also generates alerts to the responsible authorities regarding these attacks.

* + Secure key management

Usually, network devices are come up with built-in security keys. There should be a comprehensive security key management mechanism to protect smart home devices from intruders to use legitimate devices for their malicious purposes.

* + Security against DoS

Usually, in the DOS attacks such as jamming or coding, the communication channel is almost useless to perform any communication tasks. Hence, nodes having the IDS installed are unable to perform the detection tasks. Kasinathan et al. in [47] proposed a solution regarding DOS attacks. It can perform the detection activities against the DOS attacks, while not suffering from the same attacks. In a real environment, wireless sensor networks demand an analysis of the physical parameters in real-time. In this regard, service availability is the main need. Consequently, the proposed IDS should detect any kind of DoS activity. The proposed system is evaluated through the Pen Test, an evaluation system, and produced expected results against the attacks.

**Future directions**

In this section, an overview of the future work is discussed in the form of points. In the future, we will extend our study to other security solutions concerning technology and techniques. As IoT is evolving, it consequently faces the most sophisticated issues. So, the mitigation of such issues must be done similarly.

– Cyber insurance is gaining enlarged consideration these days. From this, more organizations agonize from problems similar to data leakage, data loss, etc. The impairment happens through these proceedings’ charges extremely to the organizations. So, these organizations need to combine defensive intrusion detection and prevention in their structures.

– To detect intrusion and hurriedly implement on the system becomes gradually problematic. So, traditional methods of IDS are not used. The prevention and detection methods are insecurely gathered in Moving Target Defense (MTD). In comparison with NIDS and HIDS, MTD constantly altered the surface of attacks and make the system protected from enemies that enter the first place.

– Cyber criminals are discovering new ways and techniques for security threats to destruct the system. So, in this situation, there is not only necessary to fix the threats as they occur, but also it is essential to learn how to predict and prevent new threats. Modern cloud indicative services are hot topics that are used to predict security concerns intelligently. The AI-powered diagnostic technique is also an interesting field, but it is slightly complex than the former.

**Conclusion**

A smart home is an emerging application of IoT, where devices communicate and share confidential information. In such an environment, several components join hands to complete the objective of IoT, such as smartphones, smart A.C., and smart heater, and sensors like smoke sensors, temperature sensors, etc., and different protocols at the backend. As IoT is new in the market and thus has no security measurements have been done so far by the manufacturer of the devices. Smart devices manufacturers mainly focus on the less computational and low energy consumption devices consequently left behind the security approaches for the devices.

As IOT comprises plethora of devices, when these numerous devices get connected, they face various security and privacy issues. A survey is carried out about the most common security threats and privacy challenges for IoT smart devices. All the issues are categorized according to the layered architecture of the smart home environment. Furthermore, several kinds of literature are surveyed for security solutions and countermeasures against the mentioned challenges. This work gives exposure to the readers about the current and future challenges.

**References:**

1. Girard, M. Standards for Cybersecure IoT Devices: A Way Forward. *JSTOR* **2020**, *160*, 1–13.
2. S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le-Khac, “Internet of Things forensics—Challenges and a case study,” in Proc. IFIP Adv.Inf. Commun. Technol., vol. 532, 2018, pp. 35–48.
3. "Poster Abstract: An Implementation of an Internet of Things System for  
   Smart Hospitals," 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), Sydney, Australia, 2020, <https://ieeexplore.ieee.org/document/9097614>
4. Smart Home based on Internet of Things and Ethical Issues

<https://www.researchgate.net/publication/351235738_Smart_Home_based_on_Internet_of_Things_and_Ethical_Issues>

1. The Integrity Challenge of the Internet-of-Things (IoT): On Understanding its Dark Side

<https://www.researchgate.net/publication/298786592_The_Integrity_Challenge_of_the_Internet-of-Things_IoT_On_Understanding_its_Dark_Side>

1. Enabling Internet of Things for Smart Homes Through Fog Computing

<https://www.researchgate.net/publication/321302670_Enabling_Internet_of_Things_for_Smart_Homes_Through_Fog_Computing>

1. Internet of Things Security - Multilayered Method For End to End Data Communications Over Cellular Networks  
   <https://www.researchgate.net/publication/334627388_Internet_of_Things_Security_-_Multilayered_Method_For_End_to_End_Data_Communications_Over_Cellular_Networks>
2. Abdul-Ghani HA, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on  
   a building-blocked reference model. Int J Adv Comput Sci Appl (IJACSA) 9(3):355–373
3. Ahemd MM, Shah MA, Wahid A (2017) IoT security: a layered approach for attacks and defenses.
4. Gupta Brij B, Arachchilage Nalin AG, Psannis Kostas E (2018) Defending against phishing attacks
5. Wei D, Qiu X (2018) Status-based detection of malicious code in internet of things (IoT) devices.
6. Ali W, Dustgeer G, Awais M, Shah MA (2017) IoT based smart home: security challenges, security requirements and solutions.
7. Almusaylim ZA, Noor Z (2019) A review on smart home present state and challenges
8. Arabo A, Pranggono B (2013) Mobile malware and smart device security: trends, challenges and solutions.
9. . Faisal EM, Ismail AA, Hamed HFA (2018) Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput 7(1)
10. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end-to-end secure internet of things.
11. Geneiatakis D, Kounelis I, Neisse R, Nai-Fovino I, Steri G, Baldini G (2017) Security and privacy issues for an iot based smart
12. Pongle P, Chavan G (2015) A survey: attacks on rpl and 6lowpan in IoT.
13. . Salman O, Elhajj I, Chehab A, Kayssi A (2018) Iot survey: a sdn and fog computing perspective. Comput Networks 143:221–246
14. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion detection in internet of things. J Network Comput Appl84:25–37
15. Gupta Brij B, Arachchilage Nalin AG, Psannis Kostas E (2018) Defending against phishing attacks: taxonomy of methods, current issues and future directions
16. Rizvi S, Kurtz A, Pfefer J, Rizvi M (2018) Securing the internet of things (IoT): a security taxonomy for IoT.
17. Hossain MM, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges, and open problems in the internet of things.
18. Khan F, Gawade A Secure data management in smart meter as an application of IoT
19. Wei D, Qiu X (2018) Status-based detection of malicious code in internet of things (IoT) devices.
20. Thangavel C, Sudhaman P (2017) Security challenges in the IoT paradigm for enterprise information systems
21. Kanwal J, Ali SM, Ahmad A, Ali KH, Carsten M, Din IU (2020) Proactive forensics in IoT: privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies.
22. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering
23. Classen J, Chen J, Steinmetzer D, Hollick M, Knightly E (2015) The spy next door: eavesdropping on high throughput visible light communications.
24. Liu Y, Briones J, Zhou R, Magotra N (2017) Study of secure boot with a fpga-based IoT device.
25. Vuppala S, Alie El-Din M, Kuenzi A (2019) Moving target defense mechanism for side-channelattacks
26. Zeng X, Martinez T (2003) A noise fltering method using neural networks.
27. Nirmal K, Janet B, Kumar R (2020) Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection.
28. Ramesh G, Krishnamurthi I, Sampath Sree Kumar K (2014) An efcacious method for detecting phishing webpages through target domain identifcation.
29. Whittaker C, Ryner B, Nazif M (2010) Large-scale automatic classifcation of phishing pages
30. Wei D, Qiu X (2018) Status-based detection of malicious code in internet of things (IoT) devices
31. Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J (2017) Ioddos-the internet of distributed denial of sevice attacks
32. connected vehicles against malware: Challenges and a solution framework.
33. Vikas H, Vinay C, Vikas S, Divyansh J, Pranav G, Biplab S (2019) A survey on IoT security: application areas, security threats, and solution architectures.
34. Ahlawat B, Sangwan A, Sindhu V. IoT system model, challenges and threats
35. Wang Z (2019) Identity-based verifable aggregator oblivious encryption and its applications in smart grids
36. Hariri Reihaneh H, Fredericks Erik M, Bowers Kate M (2019) Uncertainty in big data analytics: survey, opportunities, and challenges.
37. Classen J, Chen J, Steinmetzer D, Hollick M, Knightly E (2015) The spy next door: eavesdropping on high throughput visible light communications. In: Proceedings of the 2nd International Workshop on Visible Light Communications Systems
38. Kaur M, Kalra S (2018) Security in IoT-based smart grid through quantum key distribution. In: Advances in computer and computational sciences Gavra V-D, Dobra I-M, Pop OA (2020) A survey on threats and security solutions for IoT.
39. Siddiqui ST, Alam S, Ahmad R, Shuaib M (2020) Security threats, attacks, and possible countermeasures in internet of things. In: Advances in data and information sciences
40. Das D, Maity S, Nasir SB, Ghosh S, Raychowdhury A, Sen S (2017) High efciency power sidechannel attack immunity using noise injection in attenuated signature domain.
41. Kasinathan P, Costamagna G, Khaleel H, Pastrone C, Spirito MA (2013) An ids framework for  
    internet of things empowered by 6lowpan.
42. Liu J, Xiao Y, Chen CLP (2012) Authentication and access control in the internet of things.
43. Savola RM, Abie H, Sihvonen M (2012) Towards metrics-driven adaptive security management in  
    e-health iot applications.
44. Arış A, Oktuğ SF, Berna Örs YS (2015) Internet-of-things security: denial of service attacks.
45. Farouq A, Tarek S, Shakshuki EM (2018) A detection and prevention technique for man in the middle attack in fog computing.
46. Hussain F, Hussain R, Hassan SA, Hossain E (2020) Machine learning in IoT security: current solutions and future challenges.
47. Mahmud Hossain SM, Riazul I, Farman A, Kyung-Sup K, Ragib H (2018) An internet of thingsbased health prescription assistant and its security system design.
48. Kim Y-P, Yoo S, Yoo C (2015) Daot: dynamic and energy-aware authentication for smart home appliances in internet of things.
49. Ida IB, Jemai A, Loukil A (2016) A survey on security of IoT in the context of ehealth and clouds.
50. Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. In: Digital twin technologies and smart cities
51. Rodrigues Luis, Guerreiro Joel, Correia Noélia (2020) Reload/coap architecture for the federation of wireless sensor networks.
52. Datta P, Sharma B (2017) A survey on iot architectures, protocols, security and smart city-based applications.
53. Li X, Wang H, Dai H-N, Wang Y, Zhao Q (2016) An analytical study on eavesdropping attacks in wireless nets of things. Mob Inform Syst
54. Hazalila K, Hairulnizam M, Abawajy JH (2018) Clone tag detection in distributed rfd systems.
55. ISO/IEC. Iso/iec 27005:2018 (2018). <https://www.iso.org/standard/75281.html>
56. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures.
57. Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O (2015) Network-level security and privacy control for smart-home IoT devices.
58. Wallrabenstein JR (2016) Practical and secure IoT device authentication using physical unclonable functions.
59. Tang X, Ren P, Han Z (2018) Jamming mitigation via hierarchical security game for IoT communications.

**Figures**

1. Figure1: layers of IoT architecture, IoT world forum reference model.
2. Figure 2: World population, active devices and average no. of connected devices per person.
3. Figure 3: layers of IoT architecture, Internet of Things: Architectures, Protocols, and Applications
4. Figure 4 Smart home architecture, Smart home security issues.
5. Figure 5 Trends of research studies on the security of IoT devices, Current Research Trends in IoT Security: A Systematic Mapping Study
6. Figure 6 IoT layers structure, A study on security issues and challenges in IoT.