# EVALUATION OF DIFFERENT KINDS OF ATTACKS AND ALSO FEASIBLE SOLUTIONS TOWARDS IOT

**Sudheer Kumar Shriramoju**[1]

[1]Project Manager, Wipro InfoTech, India

## ABSTRACT

The significant requests of wireless interaction systems reside in the military, company, health care, retail, as well as transports. These systems utilize wired, cell, or even Adhoc units. Wireless sensor networks, actuator networks, as well as also automobile devices have acquired a fantastic rate of interest in order and industry. In the last handful of years, the Internet of Things (IoT) has obtained considerable research study rate of interest. The IoT is thought about as future of the internet. In future, IoT will certainly take part in a vital obligation along with will certainly transform our living layouts, criteria, along with company versions. The utilization of IoT in various apps is anticipated to climb swiftly in the happening years. The IoT allows billions of devices, people, as well as remedies, to associate with others and also replacement pertinent info. This paper provides the evaluation of different kinds of attacks and also feasible solutions towards iot

**Index Terms:** Internet of Things, security, attacks

## I. INTRODUCTION

THE internet of things is a kind of network which is produced due to the numerous gizmos conducting different activities for some typical objectives. These gadgets (sensing units) may be electronic camera mounted at a selection of locations in the city to watch on the place website visitor traffic, metrological segmentation, metropolitan firms, banks, a range of noticing devices, individuals, and additionally cellular phones, traffic authorities, urban organizations etc. These devices perform popular along with the pervasive computer. Regardless there is no atypical significance of IoT. A lot of organizations (CCSA, ITU- T, EU FP7 CASAGRAS, IETF etc) have given their meanings. The unattended setting (motion, access, as well as also leave behind), heterogeneity, scalability, smartphone, variety, love, relationship myriad, unattendedness as well as marginal source power are the extensive perception, dependable transmission, as well as smart processing, are actually a few of the buildings or perhaps attributes or top qualities of the IoT. The significant tasks which are performed in IoT are things id, generating an action, product grabbing, as well as i.d. of things:

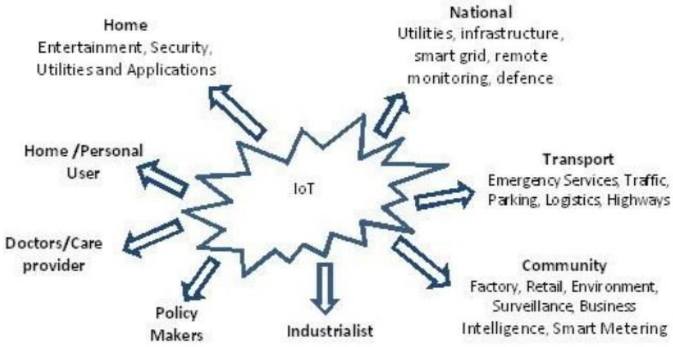

Home
Entertainment, Security, Utilities and Applications
National
Utilities, infrastructure, smart grid, remote monitoring, defence
Home /Personal User
IoT
Transport
Emergency Services, Traffic, Parking, Logistics, Highways
Doctors/Care provider
Community
Factory, Retail, Environment, Surveillance, Business Intelligence, Smart Metering
Policy Makers
Industrialist

**Figure1: IoT overview**

The Internet of Things (IoT) is coming to be ubiquitous as new-- and likewise aged-- gadgets link into a selection of networks. Arising from intelligent coffeemakers in the kitchen space region to sensors embedded in 20-year-old power motors on the manpower, the IoT is increasing quickly as well as continuous, as associations make an effort to capture brand-new performances or maybe acquire all new understandings from fresh attached tools.

Around prudent cities, residential properties, and also vehicles, in industries varying arising from health care to manufacturing, billions of IoT systems stay in the business today as well as likewise billions even more are anticipated to adhere to online in the next few years. Gartner anticipates that higher than twenty billion connected gadgets are going to certainly perform via 2020, climbing coming from 8.4 billion in 2017. Technology analysis study firm IDC anticipates worldwide IoT commiting is going to certainly tot just about $1.4 mountain range by 2021.

However as the IoT opens up brand-new house windows of possibility for businesses, it additionally offers a new type of danger. Several IoT systems may not have been made alongside security in mind. Some are without the onboard processing electrical energy or perhaps mind to offer durable security commands. As much more IoT gadgets are created, the strike surface area, as well as achievable vulnerabilities, will certainly develop and additionally rise, fast outpacing present methods to stop each one of them.

There is no wonder drug, no solitary remedy that will get the IoT at every volume as well as every touchpoint. It's natural o focus on the "things" when producing an IoT security tactic, however, the extent needs to have to must be a lot broader. The only lasting procedure calls for a multi-layer, end-to-end structure that looks at all connected devices, along with the asks for they run and the internet-tasks they utilize to disseminate relevant information. The framework needs to have to become enhanced emerging outright greatest strategies but is distinctive every organization, equally as every IoT release is unique.

Normally, our team found out that varieties in perspectives were driven much less through basic distinctions in concepts, nonetheless instead through variants in work knowledge as well as concerns. As an example, some specialists were even more competent regarding certain security devices, criteria, or perhaps regulations, along with focused on variables about their place of skill-sets and even their association's purpose. Prior study has exposed that security pros may examine the same artefacts differently depending upon their background carefully security domains.

A lot of variables found out as significant via experts are in fact elements that they believe will teach buyers. Pros furthermore recognized some factors for an overview that could improve pros just, typically to be able to keep service providers responsible.

Previous research studies encourage that crack labels might be trustworthy. A split label features a key layer that offers the best significant and also glanceable content, observed through an additional amount for additional information. In our study, our company talked to professionals to describe the level on which the details ought to be featured on the tag. They primarily urge positioning simply info that would surely be reasonable as well as likewise crucial to most of the purchasers on the crucial amount.

Our experts cultivated a version layered tag based upon our specialist removal investigation. Our pros after that carried out semi-structured conferences with 15 consumers of IoT tools (wise property systems and even wearables) and also supplied our model to them. Our business reveals that every one of our attendees possessed a crystal clear understanding of the relevant info given on the primary level of the tag. Although numerous of the factors on the second layer of the tag was a lot less easy to understand to people that were without individual privacy in addition to security proficiency, each of our individuals mentioned that they still desire such pertinent info to end up being featured on the label generally to become as informed as possible. Also, personal guests mentioned that possessing all the essential personal privacy and also security components, also unfamiliar ones, on the tag will help them merely surf online to situate a lot more relevant information.

Internet of Things (IoT) has drawn in sizable attention during the past number of years. The principle of IoT was first of all suggested via [2] Due to fast developments in cellphone interaction, Wireless Sensor Networks (WSN), Carrier Frequency Id (RFID), and also cloud handling, communications among IoT systems has become much easier than it was previously. IoT tools are capable of co-operating along with one another. The Globe of IoT features a solid variety of devices that include a mobile phone, laptop computers, Personal organizers, notebook computer, tablet computer systems, in addition to numerous other hand-held embedded devices. The IoT gadgets are based upon efficient sensing units as well as wireless communication devices to interact alongside each other in addition to step deliberate details to the main device. The relevant details coming from IoT resources is a lot more honed in the main unit as well as supplied to the assigned areas. In addition to the speedy advancement of interaction as well as additionally internet modern technology, our routine plans are more sturdy on an imaginary space of digital entire world [1] People may operate, store, chat (keep pets as well as vegetations in the internet globe supplied by the network), whereas people keep in the real. For that reason, it is quite challenging to switch out all the personal tasks together with an automated way of life. There is a limiting frontier of the fictitious room that limits the potential growth of the internet for far better business. The IoT has properly blended the make-believe space as well as likewise the true on the similar body. The key aim ats of IoT are the arrangement of an ingenious setting and also uncomfortable private devices like smart lifestyle, prudent things, brilliant health, and also smart metropolitan areas to name a few. Nowadays the cultivating fee of the IoT units is rather higher, a growing number of systems are fastened utilizing the internet. According to analysis [3], there are 30 billion fastened things with family member 200 billion connections that will make an income of roughly 700 billion Europeans due to the year 2020. Presently in China, there are actually nine billion devices that are anticipated to fulfil 24 billion because of the year 2020. In future, the IoT is going to entirely modify our staying styles as well as likewise business versions. It is mosting likely to allow individuals and also devices to communicate anytime, just about anywhere, alongside any kind of resource under ideal afflictions making use of any kind of sort of network along with any kind of type of company [4] The primary target of IoT is actually to generate Top-notch planet for people in future.

Sadly, most of these devices and additional treatments are undoubtedly not made to handle the security and individual privacy attacks as well as also it increases a lot of security as well as personal privacy worries in the IoT networks such as privacy, permission, files honesty, ease of access control, privacy, etc. On daily, the IoT units are targeted through aggressors and also trespassers An appraisal reveals that 70% of the IoT resources are fast and easy to strike. For that reason, a trusted device is amazingly required to protect the tools linked to the internet versus cyberpunks as well as additionally invaders.

## II. LITERATURE REVIEW

Within this segment, our professionals first describe prior research study on recognizing buyersprivacy as well as security connected complications for IoT devices. Next off, our team supply history on only how tags have been used in numerous circumstances to inform individuals' choices. Inevitably, we go over documents along with recommendations on privacy as well as additionally security absolute greatest techniques for individual IoT gadgets.

### Consumers Privacy and also Security Problems

Plenty of discovers have presented that customers are an expanding variety of concerned about privacy as well as additionally security of IoT bodies. Experts have shown that the measurement of these worries relies on aspects including the kind of relevant information picked up, the goal of data option, and additionally the commitment of gotten hold of documents. [3] checked out aspects associating with IoT relevant information collection along with uncovered that folks are a whole lot so much more worried concerning records being gathered secretive spots contrasted to social places. Atop that, they found out that people's problems depend upon the sort of documents being collected. In a previous analysis study, Naeini et al. utilized stories to investigation study simply exactly how various variables may assess alternatives nicely tot related to pertinent info acquired through sensing units. They located that variables like the target of records variety as well as furthermore the commitment possibility particularly affect people' privacy-related concerns.

Despite such troubles, customers are still purchasing IoT units, generally as a result of their realized simplicity as well as likewise attributes. This resides in many cases associated with as a "privacy secret," due to the distinction in between privacy worries as well as also activities needed to minimize those worries. One resource for this could be that clients are supplied in addition to little of, or possibly usually no, privacy and security details panicking IoT gadgets before acquire. This stays free from clients coming from helping generate upgraded IoT-related resources assortments and likewise enhances the danger of privacy as well as additionally security sensitivities, which might result in first-class and massive attacks targeting IoT units.

### Product Labels

Product tags, like meals products health and wellness as well as wellness along with nutrients along with likewise energy tags, have been utilized to assist individuals' acquisition assortments. Food products nutrients labels, primarily, were built to decrease bodyweight issues utilizing helping customers to protect a lot more healthy meals. A selection of other objectives of meals nutrition tags features prompting meals things firms to contend to create healthier things as well as also allow- ing authorizations to help people' health-related practices without mandating particulars dietary requirements.

The functionality of foods wellness, along with nutrition tags, has been shown to rely upon variables featuring people' enthusiasm at the point of investment, whether the client is purchasing the thing for kids, striving to burn fatty tissue, and/or getting the product for the surprisingly very first time, their nutrition-related expertise, health and wellness and wellness health condition, and also socio-demographic elements. Research study looks into have additionally divulged the restraints of sustenance labels unnecessarily socializing nutrients details to customers to enhance eating programs. Regardless of these disadvantages, these consider clarifying that foods items nutrients tags greatly educate people' financial investment possibilities.

In the realm of privacy, analysts have uncovered the effect of privacy "health and nutrition labels" on the internet site. They found out that privacy tags assist consumers to find out essential relevant information a lot faster as well as furthermore a whole lot additional accurately, as paired to find such details in common privacy plannings.

### Privacy along with Security Guidelines in addition to Downright Top Practices

[3] conducted a complete literary works analysis on freely available files stemming from field hookups and also likewise worldwide providers on their security-related suggestions and also suggestions for customer IoT gadgets. They reviewed 17 company files (including from Intel, HP, as well as additionally Specific Modern Innovation Institution) and also likewise policy reports (featuring emerging from International Percentage, International Supplier for Regulation (ISO), as well as Cooperation for the Internet of Things Improvement (AIOTI)). This consumer review remembered 19 overarching concepts connected to security downright finest methods that were shown a minimum required of two attend these records. The most well-liked recommendations (discussed in at the minimum 10 papers) were sturdy authentication by default, reputable aside from cryptographically certified security updates, the cover of report encryption using nonpayment, besides observance in addition to threat assessment. A volume of the different other regulations was connected to physical security, susceptibility coverage and also recognitions, in addition to safe device footwear. The security aspects that our pros produced based upon our specialist source research study took care of every one of the best steady security rules discussed in this particular details compositions study [5]

Tanzer et al. identified that often, the industry acknowledges the usefulness of advertising protected as well as likewise secure and additionally protected IoT systems on the market and will like running together with the federal government as an area of their efforts. Having explained that, they are a lot even more interested in personal-demand than liable aids. For instance, providers might self-certify their IoT units using a unit created with IoT Security Foundation that reveals 5 volumes of awareness.

A latest UK authorities record debated personal- tip, considering the lack of incentives for IoT organization to consent to security optimum procedures when developing IoT products. The documentation recommended that the authorities mandate details needs for IoT products as a unit to build up the security of buyer IoT things. These necessities are no delinquency requirement, accessibility of a weak point acknowledgement plan, as well as also security updates. These suggested demands all are included in our privacy in addition to likewise security label.

Considerably, all the examined reports over-concentrated on devices' security systems together with a handful of suggestions to data privacy factors. As purchasers are troubled involving both the privacy and likewise security of their units, in our job our provider talked to pros and also people concerning each privacy policies in addition to security mechanisms that need to be featured on a tag.

## III.IOT SECURITY

There are a bunch of susceptibilities in IoT due to its characteristics of the network. The security needs durability to the attacks, access administration, documents authorization, and customer privacy. Some privacy-enhancing actions i.e. digital unique network, transport layer security, red onion broadcasting, DNS security developments, in addition to exclusive information retrieval and some state rule as well as legal technique are recommended. Since a lot of the amount of time its IoT devices are kept dismissed (bodily protection is needed to have), interaction is, in fact, wireless, along with its very own gadgets has restricted resources, because of this innovative measures are hard to be applied:

i) Item Recognition as well as also Settling in IoT: for distinct awareness of things in the IoT network there is called for ONS (product network body) like the DNS is asked for. The headline details social network (NDN), as well as FIA (Potential Internet Design), are proposed.
ii) Info trustworthiness and Authorization in IoT: Notifications need to have to become unhampered along with discovered as a result of the needed.
iii) Privacy, trust, as well as information privacy: Behavior of client while he was connected to IoT network is compiled to ensure that he was a routing consumer or perhaps someone else. Lack of consent, transportation security, receive access to control, unconfident software and so on
. Lightweight Cryptosystems and also Security Methods: a range of information including invaluable information is accessible for going over and also additional managing. Therefore such important sources are defended through cryptosystem and also necessary strategies must be prepared for the very same.
iv) Course Weak point as well as Backdoor Research: there might be several weakness and also exploitation or even violations into device security. These breached must be enclosed order that infiltration may be protected against.
v) Malware: There are needless systems mainly composed of hurting or maybe knowing they think about company competitors. They at times eat our system sources as well as occasionally accident or even dishonest the portion of the device of our body. A high-quality anti-virus, anti-spammer and so on must be established to quit all of them.
vi) Android Device: Most of the smartphones offered today are Android body located. As a result, an increasing amount of ingenious devices as well as likewise a good idea functions are created to connect along with these devices.

There are some security criteria of IoT; privacy enhancing modern-day technologies VP, Besides the requirements, there are some concerns secretive plans also; choice of privacy offences, superior of details and circumstance, the id of clarity as well as additional documents minimizing, interoperability and also connection. Interoperability is found out as the flexibility to parts to communicate and likewise can quickly change on its own thus if you want to satisfy the recommended scenario. They could be specialized and also cross-domain interoperability.

**Attacks as well as Vulnerabilities.**

Different kind of attacks at different coatings like hair efficiently pass, snooping secretive records, Disk Operating System, and impersonation, are significant manages to the security. These hazards as well as additionally susceptibility might be handled by using cryptosystems, checking, violation medical diagnoses, as well as also antiviruses, i.e. Diffie-Hellman, RSA, ECC, electronic trademark, in addition to Hash functionality and so forth approaches. Attacks are categorized as energetic or maybe static as well as many of the handles of IoT are represented in below figure 2:

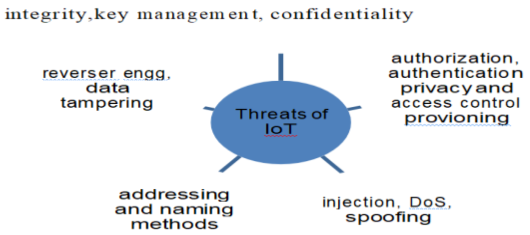
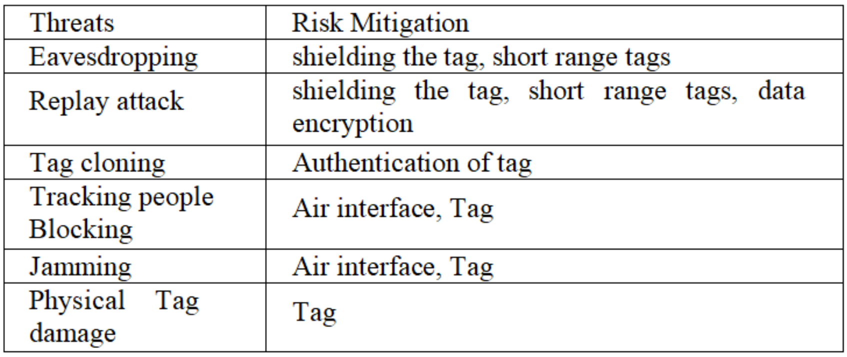

integrity,key management, confidentiality
reverser engg, data tampering
authorization, authentication privacy and access control provioning
Threats of IoT
addressing and naming methods
injection, DoS, spoofing

**Figure 2**

Many kinds of attacks have been encouraged i.e. event, recreation, locking out, privacy

| category | Attack | Result | Solution |
|---|---|---|---|
| Gathering | Tampering, skimming, eavesdropping, analysis of traffic | Confidentiality divulging | Steganography and cryptosystems, CRC, MAC |
| Imitation | cloning, spoofing, replay, | Confidentiality divulging | Anti-virus, anti-jammer, firewall |
| Blocking | DoS, Malware, jamming | Confidentiality divulging | Data transmission, digital signature |
| privacy | Group and individual | Confidentiality divulging | Distortion, data disclosures, equivocation |

Man_in_the_middle, eavesdropping is actually of lowered to transport risk management and also furthermore celebration, privacy, disturbance, duplicate and also broadcasting diversion are in a simple fact of a lot greater hazard risks, security hazards at various levels, and also putting together, Disk Operating System, together with blocking out remain in fact of quite high-risk risks. Many of the risks, as well as additionally decrease, are noted right here:



| Threats | Risk Mitigation |
|---|---|
| Eavesdropping | shielding the tag, short range tags |
| Replay attack | shielding the tag, short range tags, data encryption |
| Tag cloning | Authentication of tag |
| Tracking people Blocking | Air interface, Tag |
| Jamming | Air interface, Tag |
| Physical Tag damage | Tag |

**SecurityMechanism**

A handled and also intellectual approach [3] is prepared tetrahedron-based strategy which possesses 4 blemishes specific, clever things, procedure, in addition to the technological eco gadget. The brilliant things handle human beings, sensing systems, RFID tags, operating system, personal computers, interaction therapies, as well as network tools. The hyperlinks attaching to these nodules are sturdy besides deal with the distinction in addition to furthermore co-operation between blemishes. These sides stand for trust, integrity, obligation, motor vehicle- immunity, safety as well as security, and recognition and also obtain accessibility to control.

## IV. IOT DEVICEATTACK LAYERS

What makes it possible for cyberpunks to compromise IoT gadgets from the beginning? One variable is actually that security has certainly not appeared developing coming from the concept interval of numbers of IoT gadgets on the market place. An added is the unsatisfactory deal of several internet units, which might be created relying on the consumers' convenience as opposed to because of the simple fact that security. The deficiency of security intentionally may result in even more weak spot along with also disappointing create may trigger thin security referrals. The willpower of these 2 parts intensifies the problem, primarily due to the simple fact that lots of cyberpunks are determined to find susceptibilities from all doable angles.

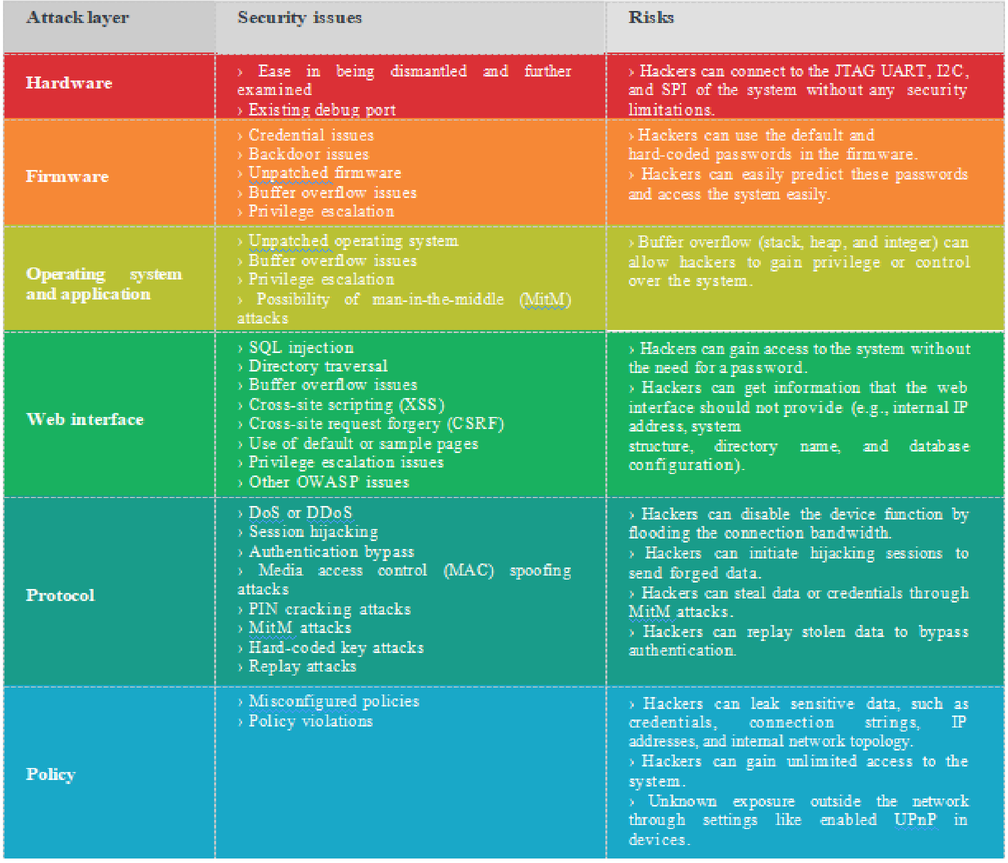
Cyberpunks may begin occurring coming from the innermost finishing of an IoT gizmo, the physical motherboard. There they can effortlessly find the parts debug port and even interaction port, e.g., JTAG UART, I2C, and also furthermore SPI. Occurring coming from there, they might seek hard-coded codes, hid backdoors, along with sensitivities in its own ditched firmware.

They may conveniently moreover find entrance components including running unit and also operation insects. Besides they may head to the internet interface of the gadget to seek internet bugs.

Far more, they can easily attempt finding a weakness in interaction operations, like Bluetooth, Zigbee, Z-Wave, NFC, 4G, 5G, and also IEEE 802.1 x. Hackers can conveniently furthermore choose the plans, which may consist of fragile details or perhaps maintain configurations that could show the device outside the house network.

Our team complete the several attack layers of an IoT device in Figure 3

.



| Attack layer | Security issues | Risks |
|---|---|---|
| **Hardware** | › Ease in being dismantled and further examined<br>› Existing debug port | › Hackers can connect to the JTAG UART, I2C, and SPI of the system without any security limitations. |
| **Firmware** | › Credential issues<br>› Backdoor issues<br>› Unpatched firmware<br>› Buffer overflow issues<br>› Privilege escalation | › Hackers can use the default and hard-coded passwords in the firmware.<br>› Hackers can easily predict these passwords and access the system easily. |
| **Operating system and application** | › Unpatched operating system<br>› Buffer overflow issues<br>› Privilege escalation<br>› Possibility of man-in-the-middle (MitM) attacks | › Buffer overflow (stack, heap, and integer) can allow hackers to gain privilege or control over the system. |
| **Web interface** | › SQL injection<br>› Directory traversal<br>› Buffer overflow issues<br>› Cross-site scripting (XSS)<br>› Cross-site request forgery (CSRF)<br>› Use of default or sample pages<br>› Privilege escalation issues<br>› Other OWASP issues | › Hackers can gain access to the system without the need for a password.<br>› Hackers can get information that the web interface should not provide (e.g., internal IP address, system structure, directory name, and database configuration). |
| **Protocol** | › DoS or DDoS<br>› Session hijacking<br>› Authentication bypass<br>› Media access control (MAC) spoofing attacks<br>› PIN cracking attacks<br>› MitM attacks<br>› Hard-coded key attacks<br>› Replay attacks | › Hackers can disable the device function by flooding the connection bandwidth.<br>› Hackers can initiate hijacking sessions to send forged data.<br>› Hackers can steal data or credentials through MitM attacks.<br>› Hackers can replay stolen data to bypass authentication. |
| **Policy** | › Misconfigured policies<br>› Policy violations | › Hackers can leak sensitive data, such as credentials, connection strings, IP addresses, and internal network topology.<br>› Hackers can gain unlimited access to the system.<br>› Unknown exposure outside the network through settings like enabled UPnP in devices. |

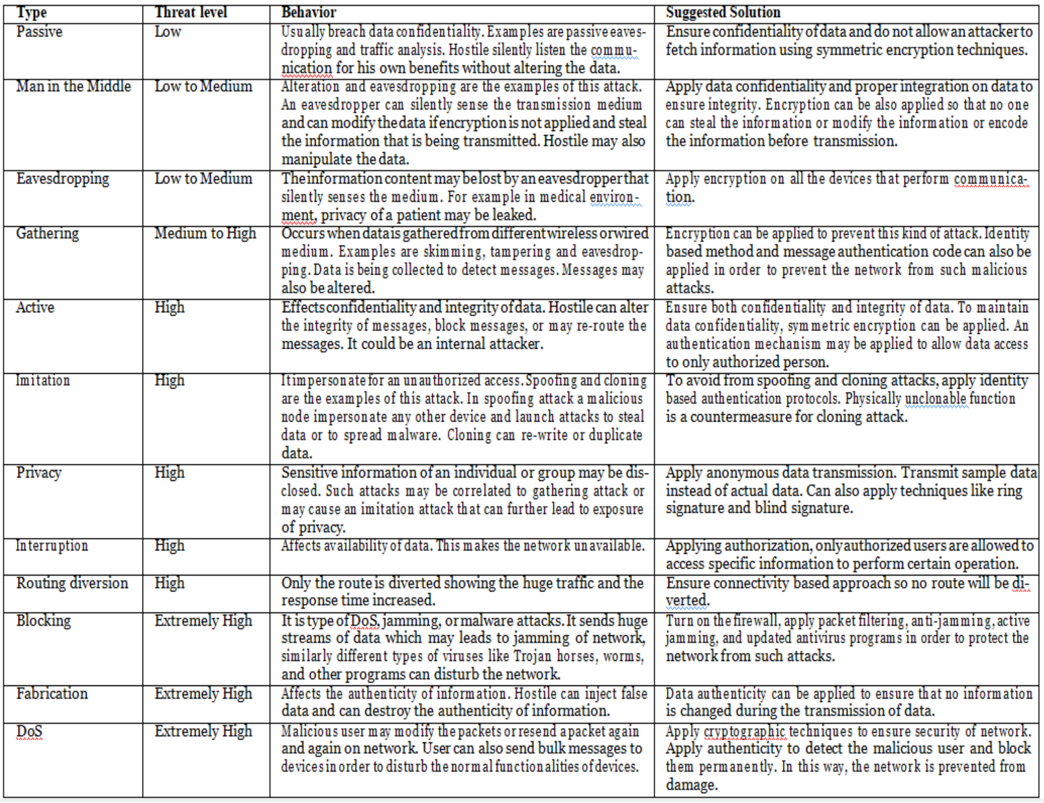
**Figure 3: The attack layers of an IoT device and their security issues and risks**

## V. EVALUATIONOF ATTACKS ANDPOSSIBLE SOLUTIONS

The IoT resides in truth meeting different form of attacks featuring energetic attacks in addition to stationary attacks that might merely interrupt the functionality- ability as well as additionally eliminate the benefits of its solutions. In a fixed strike, an intruder merely pinpoints the acne or maybe could clean the details nonetheless it never before attacks. Nevertheless, the energised attacks interrupt the functions almost. These exciting attacks are identified directly into 2 a lot more classifications that are inner attacks besides outdoors attacks Such vulnerable attacks may easily remain away from the information to engage smartly. Therefore the security restrictions have to remain related to stop devices coming from malicious attacks. A variety of sort of strike, nature/behaviour of attack as well as additional risk degree of attacks is coped with within this particular area. Various volumes of attacks are assembled straight into 4 kinds depending upon to their routines and additionally recommend practical substitutes to threats/attacks.

1) Low-level attacks: If an assailer tries to strike a network along with also his strike is ineffective.
2) Medium-level attacks: If an attacker/intruder as well as also an eavesdropper remains in simple fact just taking note of the stations, however, do certainly not possess an effect on the reliability of appropriate details.
3) High-level attacks: If an attack is moved on an internet- operate in enhancement to it tailors the security of reports and also changes the relevant info.
4) Extremely High-ranking attacks: If an intruder/attacker attacks on a network through obtaining unauthorized gain access to as well as additionally carrying out a restricted functionality, make the internet- job evasive, sending out mass tips off, and also even obstructing network.

Table 1 offers several types of attacks, their hazard quantities, their nature/behaviour, as well as doable remedy to take care of these attacks.



| Type | Threat level | Behavior | Suggested Solution |
|---|---|---|---|
| Passive | Low | Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data. | Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques. |
| Man in the Middle | Low to Medium | Alteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data. | Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission. |
| Eavesdropping | Low to Medium | The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked. | Apply encryption on all the devices that perform communication. |
| Gathering | Medium to High | Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered. | Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks. |
| Active | High | Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker. | Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person. |
| Imitation | High | It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data. | To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack. |
| Privacy | High | Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy. | Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature. |
| Interruption | High | Affects availability of data. This makes the network unavailable. | Applying authorization, only authorized users are allowed to access specific information to perform certain operation. |
| Routing diversion | High | Only the route is diverted showing the huge traffic and the response time increased. | Ensure connectivity based approach so no route will be diverted. |
| Blocking | Extremely High | It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network. | Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks. |
| Fabrication | Extremely High | Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information. | Data authenticity can be applied to ensure that no information is changed during the transmission of data. |
| DoS | Extremely High | Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices. | Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage. |

**TABLE1: Different Types Of Attacks And Their Threat Levels**

## VI. CONCLUSION

Privacy protection is among the best considerable challenges in IoT bodies as a result of the legal criteria in several use domains such as home atmospheres, smart grids, as well as health and wellness systems. There are boosting stipulations and constraints on the selection, storing, and processing of personal details involved in all applications, including IoT. Privacy protection options might need to have to include a stable of techniques and strategies, such as time-limited storing of vulnerable information, gain access to management systems to allow accessibility meThis paper provided the evaluation of different kinds of attacks and also feasible solutions towards iot

## REFERENCES

*1. Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. Computer Networks, 31(23–24), 2435–2463.*

*2. Pearson, S. (2002). Trusted computing platforms: TCPA technology in context. USA: Prentice Hall.*

*3. Peng, T., Leckie, C., & Ramamohana-Rao, K. (2007). Survey ofnetwork-baseddefensemechanismscounteringtheDoSandDDoSproblems.ACMComputingSurveys,39(1),Article3.*

*4. Perrig,A.,Stankovic,J.,&Wagner,D.(2004).Securityinwirelesssensornetworks.Communications of the ACM, 47(6), 53–57.*

*5. Quisquater, J. J., & Samyde, D. (2001). Electromagnetic analysis (EMA): Measures and counter-measuresforsmartcards.InProceedingsoftheInternationalConferenceonResearch in Smart Cards: Smart Card Programming and Security, Springer LNCS-2140, pp.200–210.*

*6. Roesch, M. (1999). Snort – lightweight intrusion detection for networks. In Proceedings of the 13th USENIX Conference on System Administration (LISA '99), pp. 229–238.*

*7. Sugandhi Maheshwaram, "An Overview towards the Techniques of Data Mining", RESEARCH REVIEW International Journal of Multidisciplinary, Volume04, Issue02, February 2019*

*8. Sudheer Kumar Shriramoju, Surya Teja N, "Security in Different Networks and Issues in Security Management", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 8, Issue 2, February 2020*

*9. Sudheer Kumar Shriramoju, "Access Control and Density Based Notion of Clusters", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 1 Issue 3, pp. 215-220, July-August 2015.*

*10. Sudheer Kumar Shriramoju, "Review on NoSQL Databases and Key Advantages of Sharepoint", International Journal of Innovative Research in Science, Engineering and Technology, ISSN(Online): 2319-8753, ISSN (Print): 2347-6710, Vol. 7, Issue 11, November 2018.*

*11. Sudheer Kumar Shriramoju, "Capabilities and Impact of SharePoint On Business", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2, Issue 6, November-December-2017.*

*12. Sudheer Kumar Shriramoju, "Security Level Access Error Leading to Inference and Mining Sequential Patterns", International Journal of Scientific Research in Science, Engineering and Technology, Volume 2, Issue 4, July-August 2016*

*13. Sudheer Kumar Shriramoju, "An Overview on Database Vulnerability and Mining Changes from Data Streams", International Journal of Information Technology and Management, Vol. VII, Issue No. IX, August-2014*

*14. Sudheer Kumar Shriramoju, "A Comprehensive Review on Database Security Threats and Visualization Tool for Safety Analyst", International Journal of Physical Education and Sports Sciences, Vol. 14, Issue No. 3, June-2019*

*15. Sudheer Kumar Shriramoju, "Integrating Information from Heterogeneous Data Sources and Row Level Security", Journal of Advances and Scholarly Researches in Allied Education, Vol. IV, Issue No. VIII, October-2012*

*16. Sudheer Kumar Shriramoju,, "A Review on Database Security and Advantages of Database Management System", Journal of Advances in Science and Technology, Vol. V, Issue No. X, August-2013*

*17. Sudheer Kumar Shriramoju, "Cloud computing service models towards authentication in cloud", International Journal of Research and Applications, Volume 7, Issue 25, Jan-Mar 2020*

*18. Sudheer Kumar Shriramoju, "Security Challenges of Service and Deployment Models", International Journal of Scientific Research in Science and Technology, Volume 4, Issue 8, May-June2018*

*19. Sudheer Kumar Shriramoju, "A REVIEW ON DIFFERENT TYPES OF VIRTUALIZATION AND HYPERVISOR", Alochana Chakra Journal, Volume VIII, Issue II, February 2019*

*20. Sudheer Kumar Shriramoju, "Cloud security - A current scenario and characteristics of cloud computing", International Journal of Research and Applications, Volume 5, Issue 18, Apr-Jun 2018*

*21. Sudheer Kumar Shriramoju, "SECURITY ISSUES, THREATS AND CORE CONCEPTS OF CLOUD COMPUTING", Airo International Research Journal, Volume IX, Feb 2017.*