1. Introduction

1.1 RELATED WORK - 7-8 Survey Papers on security in IoT, 3-4 lines each: which points they have done in their survey, which points they haven't covered which we have done (their disadvantage - our advantage) [Sudeep sir’s paper - [<https://www.sciencedirect.com/science/article/abs/pii/S088832701930603X>] is ref]

Also make a table for the same

1. Background -
   1. 1st explain IoT (20-30 lines) → [BRIJ SOJITRA](mailto:20bce035@nirmauni.ac.in)
   2. total 5-6 applications samjavo - what is smart home, how is IoT used in it, how do sensors communicate, the challenges of Smart home system (performance, security, vulnerabilities, etc)(15-20 lines each). Jode darek na 3-4 most commonly used protocols (8-9 lines each)
      1. Smart Home → [BRIJ SOJITRA](mailto:20bce035@nirmauni.ac.in)
      2. Healthcare → [BRIJ SOJITRA](mailto:20bce035@nirmauni.ac.in)
      3. IIoT → [DEVANSH SHAH](mailto:20bce055@nirmauni.ac.in)
      4. Autonomous Vehicles → [DEVANSH SHAH](mailto:20bce055@nirmauni.ac.in)
      5. Telecom → [DEVANSH SHAH](mailto:20bce055@nirmauni.ac.in)
   3. Applications no diagram
   4. Protocol no Diagram
2. Table of taxonomy

***Vulnerabilities***1) Name

2) 1-2 Lines explanation about vulnerability

3) How does it take place

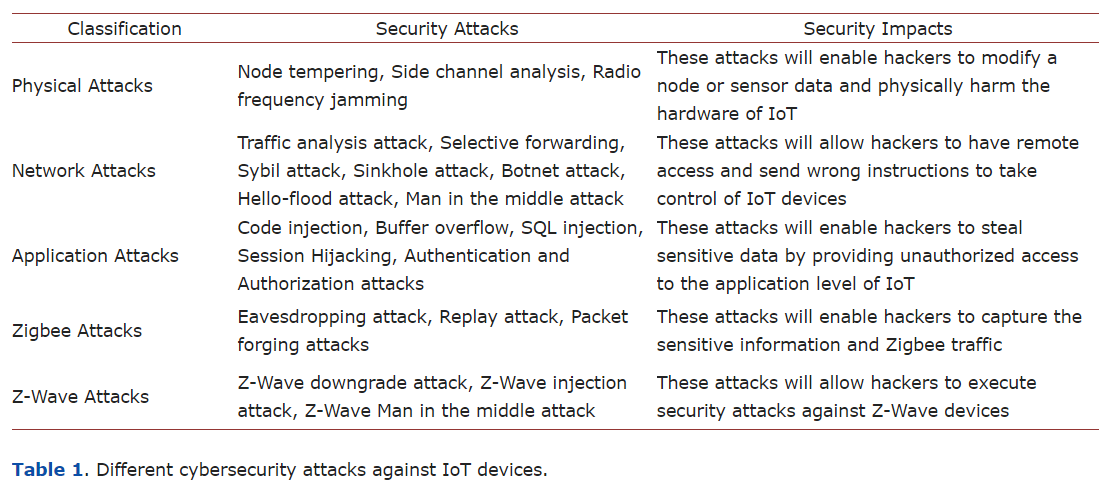
4) 1 real-life example (with citation)

5) Solutions - 2

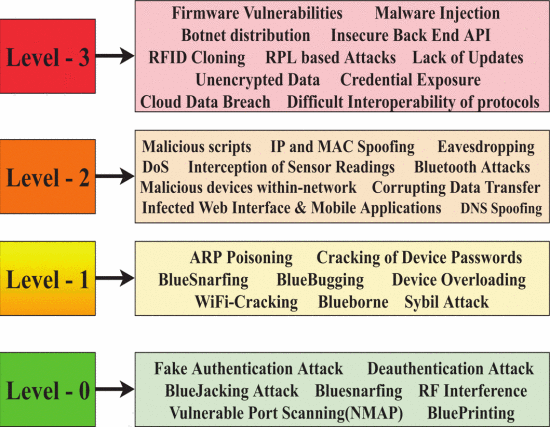
FINAL:

1. Literature review [DHRUV PRAJAPATI](mailto:20bce061@nirmauni.ac.in) - pending
2. Background [DEVANSH SHAH](mailto:20bce055@nirmauni.ac.in) - complete
   1. 1st explain IoT
   2. Applications of IoT
   3. Common protocols used in IoT
3. Smart Home [DEVASY SANJAY](mailto:20bce057@nirmauni.ac.in)
4. Industrial IoT [DHRUV PRAJAPATI](mailto:20bce061@nirmauni.ac.in) - 2 attacks complete, 1 pending
5. Autonomous Vehicles [DEVASY SANJAY](mailto:20bce057@nirmauni.ac.in)
6. Healthcare [DEVANSH SHAH](mailto:20bce055@nirmauni.ac.in)
7. Conclusion

<https://www.scirp.org/journal/paperinformation.aspx?paperid=99316#ref5>

[](https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/8600778)

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9036313>



# Smart Home

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/8600778> → aamathi list levanu che

## 1. Data & identity theft

Data means when someone steals data or your personal information and identity theft means using your identity and your personal data the hacker does anything which could be unlawful and all the blame will be on yours.

In smart home segment the data generated by unprotected wearables and smart appliances are the prime target which are having ample amount of targeted personal information, which can be exploited for identity theft.

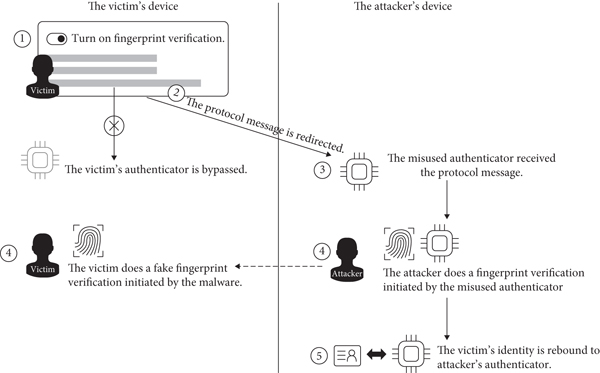
A disturbing [incident](https://www.cnet.com/news/cloudpets-iot-smart-toy-flaws-hacking-kids-info-children-cybersecurity/) happened in February 2017, when smart toys manufactured by Spiral Toys were hacked, leaving children’s voice recordings and personal information exposed. More than 800.000 users were compromised, and the details obtained included email addresses and passwords. The leaked information was stored in an online database that could easily be accessed by anyone without requiring a password. An additional 2.2 million voice recordings were stored online.

SOLUTION:

1. Lindemann R., Baghdasaryan D., Tiffany E. FIDO Universal Authentication Framework Protocol, Version V1. 0-Rd-20140209, FIDO Alliance (2014)

They designed the Fast IDentity Online (FIDO) protocol that offers a password-free authentication technique. The FIDO protocol is the 1st out of 2 factor authentication techniques that use cryptographic keys rather than passwords. The cryptographic keys are saved in an authenticator module, which the user accesses using biometrics or other security measures.

However, the above solution is prone to the Authenticator Rebinding attack as discussed in <https://www.hindawi.com/journals/wcmc/2020/8819790/>. It rebinds the victim's identity to the attacker's authenticator rather than having the victim's authenticator confirmed by the UAF protocol service, allowing the attacker to circumvent the UAF protocol's local authentication process, thus compromising the user’s identity.



1. The “TrustZone-based Integrity Measurement Architecture” (TIMA) proposed by Samsung → the FIDO server validates the integrity of the Operating System. Additionally, the callerID (module calling Authenticator) is also verified which guarantees Privacy. The authenticator uses cryptographic hashing techniques to sign and accordingly, the FIDO server can identify if the device is secure.
2. Intrusion Detection Systems that use various Mac
3. hine Learning & Deep Learning algorithms to detect and flag any suspicious activity.

## 2. Device hijacking

When a device is hijacked for the purpose of carrying out fraud. This is called device hijacking.

In this the attacker does not change the basic functionality the main motive is to infect all smart devices in the home, because of which it is very difficult to detect.

Through this attack the attacker can remotely access the entire network of your home and can for example remotely unlock your door or can change the PIN code for entry, attack your smart appliance which could damage its battery and many other things could be done.

CASE STUDY: Dolphin Attack

G. Zhang et al., "DolphinAttack: Inaudible Voice Commands", *Proc. ACM CCS*, pp. 103-17, 2017.

<https://blog.acolyer.org/2018/05/11/inaudible-voice-commands-the-long-range-attack-and-defense/>

These 2 papers describe how using sound waves, the vulnerabilities in smart home devices are exploited. An attacker generates an inaudible sound that is targeted at a specific device. When the sound is picked up by the device's microphone, it can cause the device to perform a specific action, such as visiting a malicious website or downloading malware.

The attack can be delivered through various methods, including playing the inaudible sound through speakers or by sending the sound through the air using ultrasound technology. The attack can also be delivered through a website or app, where the inaudible sound is embedded in a video or audio file. It has been demonstrated how using Dolphin Attack, a facetime call can also be initiated.

### SOLUTION to Voice Spoofing attack:

The key point to solve this attack is to distinguish between human voice and the attacker generated ultrasound. Several methods have been proposed for the same.

1. H. Feng, K. Fawaz and K. Shin, "Continuous Authentication for Voice Assistants", *Proc. ACM MobiCom*, pp. 343-55, 2017

They observed that when a human speaks, his/her skin vibrates. Hence, based on this idea, the vibration is monitored by a wearable device like smartwatch and accordingly, the command is accepted or rejected. One possible drawback to this is because the wearables are Smart IoT devices with limited security, if they are hijacked / data is manipulated, then this proposed mechanism will fail. (this drawback written out of my own understanding)

1. L. Zhang, S. Tan and J. Yang, "Hearing Your Voice Is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication", *Proc. ACM CCS*, pp. 57-71, 2017

They developed VoiceGesture, which uses the smartphone as a Doppler Radar. The idea is that when a real user speaks, there are mouth movements and to detect those, the smartphone transmits sound at high frequencies and measures the reflections. The signal reflection measurements are then analyzed for authenticating if the user is real. The main advantage over other approaches is it does not require any additional equipment.

1. Y. Meng, W. Zhang, H. Zhu and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures," in IEEE Wireless Communications, vol. 25, no. 6, pp. 53-59, December 2018, doi: 10.1109/MWC.2017.1800100.

WiVo detects human mouth movements using the wireless signals in IoT enabled Smart Home, and then confirms the authenticity of voice search based on the uniformity of voice signal and CSI data.

## 3. Eavesdropping attack

<https://www.naukri.com/learning/articles/eavesdropping-how-to-prevent-it/>

<https://www.mdpi.com/1424-8220/22/21/8564>

Eavesdropping, also called sniffing or snooping attack, is a type of attack where the hacker has access to peoples’ conversations without their knowledge. The hacker takes advantage of insecure & unprotected network communications to access data as it is being sent or received by its use. Once inside the network, hackers can intercept secretive communications & even modify conversations and it is very difficult to detect! Some popular tools include:

1. Wireshark - packet sniffer to intercept and analyze activity
2. Oreka - provides live monitoring and speech analytics

It can have a huge impact on personal reputation where private data is leaked.

If the smart home network is insecure, hackers can eavesdrop & access the password. Recently, studies have also shown that Amazon Alexa, Echo etc are also known to record conversations for their analytics. Ex: We are shown advertisements of what we talk about recently on Instagram.

According to [<https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/>], the mobiles have become an ideal spying tool.

Case Study: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740

### SOLUTION:

1. L. Maglaras, N. Ayres, S. Moschoyiannis and L. Tassiulas, "The end of Eavesdropping Attacks through the Use of Advanced End to End Encryption Mechanisms," IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798072.

They propose an End to End Encryption Mechanism. The current encryption techniques are limited only for communication between the devices and the message is decrypted when received by the receiver device. This is being exploited by attackers who can install malwares through malicious downloads and then spy on the user’s activity. To counter this, the authors propose a solution wherein the message is decrypted only when it reaches the particular application layer to ensure no attacker can eavesdrop on the message.

1. J. Kim, J. Kim, J. Lee and J. P. Choi, "Physical-Layer Security Against Smart Eavesdroppers: Exploiting Full-Duplex Receivers," in IEEE Access, vol. 6, pp. 32945-32957, 2018, doi: 10.1109/ACCESS.2018.2844558.

Exploiting the properties of dynamically changing channels, such as interference, fading and noise is an essential idea in physical-layer security to protect against Eavesdropping. Hence, the concept of Artificial Noise proposed by [S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise", *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.] gains significance because it advocates using artificial noise without degrading the communication. Friendly jamming nodes were used but their only limitation was they couldn't be used if the attacker had complete information of the channel. Hence, the full duplex receiver scheme was advocated at the receiver end so that while receiving confidential data, the receiver can simultaneously send jamming signals to ensure the eavesdropper can't get the message. A main limitation is Increased jamming power might degrade the communication performance owing to residual self-interference.

1. M. Liu, W. Quan, Z. Liu, Y. Zhang, D. Gao and H. Zhang, "Combating Eavesdropping with Resilient Multipath Transmission for Space/aerial-assisted IoT," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 2230-2235, doi: 10.1109/ICC45855.2022.9839147.

Another solution includes breaking the message into parts and sending those through different paths. Here, the probability of eavesdropping on the entire message is minimized. This is especially useful in space IoT devices. Based on graph theory and Poisson point processes, the authors developed a model of the behavior of spies. Accordingly, they describe how to pick transmission channels that reduce the eavesdropping chance.

## 4. DDOS

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9058087>

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9204688>

B. Tushir, Y. Dalal, B. Dezfouli and Y. Liu, "A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6282-6292, 15 April15, 2021, doi: 10.1109/JIOT.2020.3026023.

The main objective of the DDoS attacks is to disrupt the service. Nowadays, E-DDoS attacks are also gaining significant attention. They seek to use as much energy as possible on the target side via malicious transmission and there have been several attacks on cloud servers using smart home devices. However, E-DDoS attacks on smart home devices are also severe and can lead to a tremendous increase in electricity cost while denying access to service.

A Distributed Denial of Service (DDoS) attack compromises the bandwidth of the whole network by exhausting all of the publicly accessible network resources, thus rendering legitimate users' requests ineffective. Multiple simultaneous requests floods the server and causes the site to slow down or even crash. The Distributed Denial of Service (DDoS) attack is more susceptible than a typical Denial of service attack since there are several sources from which it originated. Hence, users are unable to determine how to identify the attack or where to take action to stop it.

The majority of DDoS attacks use botnets, which are networks of connected computers. These machines will all simultaneously try to visit a website, overloading the server and taking it offline.

DDoS attacks on smart homes are more severe since the embedded operating system is exposed and readily vulnerable, and there is always a danger with the smart home's access control system.

For example the hacker can make multiple requests to the smart bulb to turn on and off at the same time because of which bulb might get damaged.

### SOLUTION:

1. N. Bandi, H. Tajbakhsh and M. Analoui, "FastMove: Fast IP switching Moving Target Defense to mitigate DDOS Attacks," 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 2021, pp. 1-7, doi: 10.1109/DSC49826.2021.9346278.

They use the idea of moving target to confuse the attacker by making the system less static and dynamically changing network address space to increase the time and cost complexity for the attacker to attack.

1. Using Software Defined Networking (SDN) whose main goal is to detect malicious packets and filter them from the network while allowing IoT devices to work normally.
2. <https://www.hindawi.com/journals/scn/2022/1608689/>

## 5. Mirai botnets

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9142798>

One of the major dangers to the availability of Internet services is distributed denial-of-service (DDoS) assaults. These attacks are being carried out by botnets like Mirai, which use weak and default security credentials to gain control of the host and propagate to additional devices.

When ARC-based smart devices are infected with the Mirai malware, a network of remotely controlled bots or "zombies" is created. DDoS assaults are frequently carried out via this network of bots, known as a botnet.

It contains malware that searches across groups of IP addresses for targets to attack, and once it locates an IP address, it uses default login id and password credentials to enter in and take control of the target device. Until the attacker has established a network of controlled devices, this process is repeated. Once a large number of devices are ready, DDoS attack is performed from these devices on the victim network.

A real life example includes when the Mirai botnet employed a hundred thousand hijacked IoT devices to bring down Dyn, a company that controls internet’s DNS Architecture. The remarkable thing to note is that unlike other botnet attacks originating from PC’s and laptops, this attack is performed from smart IoT Devices like even digital cameras, wireless printers and baby monitors!

### SOLUTIONS:

Z. Ahmed, S. M. Danish, H. K. Qureshi and M. Lestas, "Protecting IoTs from Mirai Botnet Attacks Using Blockchains," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 2019, pp. 1-6, doi: 10.1109/CAMAD.2019.8858484. [main paper from which referred several other papers]

According to [K. Rawlinson, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack", *HP.com*.], 70% of all the IoT Devices are susceptible to being attacked and used as proxies to perform large scale DDoS attacks!

1. G. Kambourakis, C. Kolias and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies", *IEEE Military Communications Conference (MILCOM)*, pp. 267-272, 2017.

A technique to mitigate Mirai botnet attacks by passively monitoring the network traffic is presented.

1. C.D. McDermott et al., "Botnet Detection in the Internet of Things using Deep Learning Approaches", *Proceedings of the International Joint Conference on Neural Networks (IJCNN)*, pp. 1-8, 2018.

The authors have proposed a novel solution to predict the botnet in consumer networks using deep learning approaches. They have developed a detection model based on “Bi-directional Long short-term memory based recurrent neural network (BLSTM-RNN)”. However, a major disadvantage of this proposed approach is the increase in processing time.

1. C. Frank, C. Nance, S. Jarocki and W. Pauli, "Protecting IoT from Mirai botnets: IoT device hardening", *Journal of Information Systems Applied Research*, vol. 11, no. 2, pp. 33-44, 2018.

IOT Device Hardening: changing the password and blocking the port

1. A. Kumar et al., "Early Detection of Mirai-Like IoT Bots in Large-Scale Networks through Sub-Sampled Packet Traffic Analysis", 2019.

The authors have proposed a network-based algorithm to detect botnets in a large-scale network. The novelty of the algorithm is to identify the malicious node when it is scanning for its target.

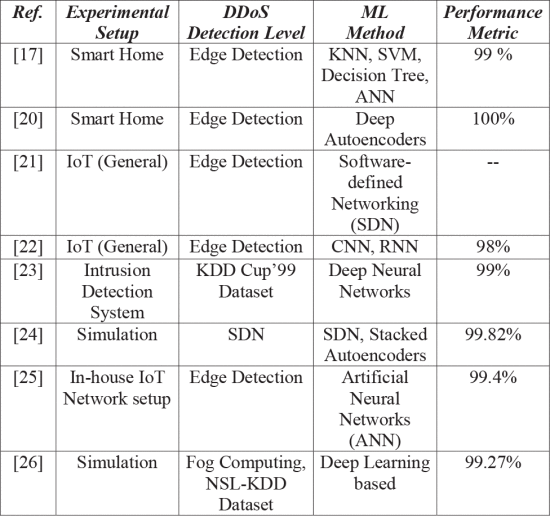
1. U. Javaid, A. Siang, M. Aman and B. Sikdar, "Mitigating loT Device based DDoS Attacks using Blockchain", *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock’18)*, pp. 71-76, 2018.

an IoT blockchain system model is proposed in which there are gateways, and different servers/miners. The goal is to protect the devices that are connected to gateways and every request is passed through a centralized smart contract. Every device is allocated a gas resource, and a device cannot send more requests than its gas resource. There are different servers/miners who are responsible for verifying the transactions and the exchange of data through smart contracts. The bandwidth available on the server cannot be exhausted even if all the devices start sending requests simultaneously. The idea of the proposed approach is to protect the servers/miners from DDoS attacks.

1. J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2017, pp. 1-5, doi: 10.1109/CCWC.2017.7868464.

This paper modifies the original Mirai Botnet Code and instead, designs an approach wherein the code can be used by the government officials to find vulnerable IoT Devices and send a mail asking the owners to take immediate mitigating measures to ensure no such large-scale DDoS attack can happen!

1. M. Snehi and A. Bhandari, "Apprehending Mirai Botnet Philosophy and Smart Learning Models for IoT-DDoS Detection," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. 501-505.



One of the major reasons where IoT devices are vulnerable is because most devices dont have the ability to check if traffic is legitimate. Hence, big data will play a major role in analyzing the massive real-time data in the quickest way possible

This paper explores the various Machine Learning Approaches used to detect DDoS attacks along with the accuracy! It also proposes a fog-computing based DDoS Defense Framework for future research.

## 6. Jamming

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/8600778>

A jamming attack can disrupt the communications between a smart device and the controlling hub, by intentionally transmitting interfering signals on a wireless network. The attacker targets the physical layer of the hub by sending radio signals at the same frequency at which the network is operating which paralyzes the entire Smart Home Network. Moreover, because of the high noise, the smart device batteries drain out extremely fast, hence no communication is possible.

For example in this attack the hacker do the jamming attack so that you can’t control your smart home appliances remotely because your actual signal is not able to reach to the appliance because of this attack

### SOLUTION:

1. change the communication frequency to prevent jamming
2. <https://link.springer.com/article/10.1007/s11277-020-07965-0>
3. T. Hamza, G. Kaddoum, A. Meddeb and G. Matar, "A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 2016, pp. 1-5, doi: 10.1109/VTCFall.2016.7880885.

The authors of this paper survey the different types of jamming attacks and also propose the counter-measures with its Strength and Weakness analysis. If an attacker is transmitting malicious signals during the slots of super frame, a solution would be to randomly permute slot time and dynamically manage the network.

1. H. Zhu et al., "You Can Jam But You Cannot Hide: Defending Against Jamming Attacks for Geo-Location Database Driven Spectrum Sharing", *IEEE jSAC*, vol. 34, no. 10, pp. 2723-37, 2016.

They propose a defense mechanism that uses an adaptive jamming detection and mitigation technique which can detect jamming attacks in real-time and mitigate its effects by quickly finding alternative channels. It is especially useful in geo-location driven spectrum sharing wherein the extra bandwidth is allocated to secondary users and can be taken advantage of by the attackers due to the availability of channel information from the spectrum queries.

## 7. Traffic Analysis Attack

X. Yu, Y. Zhang, X. -Y. Li and X. Guo, "The Truman Show: Attack On The Privacy Of Smart Homes Through Traffic Analysis," 2021 7th International Conference on Big Data Computing and Communications (BigCom), Deqing, China, 2021, pp. 121-128, doi: 10.1109/BigCom53800.2021.00033.

Although the IoT Smart home devices are light-weighted encrypted, the unencrypted information such as the length of the packet, the direction of the packet, the type of the content and various other headers can easily be accessed and monitored by an attacker. Continuous monitoring and analysis can inevitably compromise the user’s privacy.

Vijay Srinivasan, John Stankovic and Kamin Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack", *Proceedings of the 10th international conference on Ubiquitous computing*, 2008.

Based on the sequence of events and responses, private information of the smart home like when the owner is coming, going can be estimated from the opening of doors and windows and monitoring the usage of other smart devices. This attack can be 1st traced back to 2008.

### SOLUTIONS:

1. Using better encryption techniques (IoT Hub and all smart home devices can communicate using public key and private key mechanism wherein only the device having private key can access data). However, they arent very efficient in protecting against traffic analysis attacks.
2. Charles V. Wright, Scott E. Coull and Fabian Monrose, "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis", *NDSS*, vol. 9, 2009.

They proposed traffic morphing, a technique where noise traffic is also added to change the traffic fingerprint and thereby, fooling the hacker based on the false traffic.Using packet stuffing and packet splitting, the signature of the target website is translated to the signature of the nearest web page, and communication anonymity is secured at the lowest possible cost.

1. Noah Apthorpe et al., "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic", *arXiv preprint arXiv:1708.05044*, 2017.

Noah Apthorpe et al., "Keeping the smart home private with smart (er) iot traffic shaping", *Proceedings on Privacy Enhancing Technologies 2019.3 (2019)*, pp. 128-148.

These are the 2 methods recently proposed, namely ILP (Independent Link Padding) & STP (Stochastic Traffic Padding).

“1. Upload and download traffic during user activities is shaped equivalently, so an adversary cannot differentiate different types of user activities (Figure 3, traffic periods 1–3).

2. Additional periods of equivalent shaping are injected randomly into upload and download traffic (Figure 3, traffic periods 0 & 4–5). An adversary cannot distinguish these periods from real user activities, reducing confidence in activity inferences.”

## 8. Malicious Node Insertion

It leads to false data injection attacks.

Case Study + Solution: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740

At the beginning of 2019, a homeowner [reported](https://www.nbcchicago.com/investigations/My-Blood-Ran-Cold-as-Smart-Cameras-Thermostat-Hacked-Homeowner-Says-505113061.html) that his smart cameras and thermostat had been hacked. When he approached his baby’s room, he heard someone talking in a deep voice to the child, and his wife also noticed that the thermostat had been turned up to 90°F (32.2°C). And just as she brought his son to the living room, a smart camera automatically turned on and someone began cursing at them. All of these devices were made by the Nest brand, which is now owned by Google. The company said its systems had not been breached and accused the customers of using “compromised passwords that were exposed to breaches on other websites.

### SOLUTION:

1. <https://www.sciencedirect.com/science/article/pii/S0167404821003643>

It focuses on malicious FDI assaults, in which attackers generate erroneous data to affect node detection and system choices. As a result, detecting these attacks in Wireless Sensor Networks (WSNs) is critical. This article provides a method for detecting FDI assaults in WSNs using correlation theory characteristics, because data acquired by sensing nodes is connected to temporal, geographical, and event-based correlations. The authors design a solution that analyzes sensor data real time and detects anomalies. Then, based on spatial analysis, the malicious nodes are identified and they are verified based on the event correlation.

# Healthcare

## 1. Message modification attack

Modification of messages – It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or to modify the data on a target machine. Message modification attacks are commonly email-based attacks.

Healthcare is one of the most critical sector where the attack like message modification could cost hundreds of lives.

For example the attacker can change the important data like past history of the patient because of change in such critical data doctor might give patient which is allergic to the patient which has been altered in the medical history of the patient.

### SOLUTION:

1. https://www.mdpi.com/1424-8220/19/2/326

Using Blockchain to store healthcare records - Blockchain is a shared data structure that is used to store e-records, in this case of patients' medical history and reports. It is very important to ensure that none of the patient's data is modified, otherwise the medicinal treatment might change and it may prove to be fatal. Blockchain is based on Proof of Work (PoW) wherein a transaction is regarded legitimate only after the system receives verification that sufficient computational effort has been performed by authorized nodes. This paper also uses light, encryption techniques to make sure the identity remains anonymous.

## 2. DDOS attack

DDoS, or distributed denial-of-service, attack is an attempt by a cybercriminal to flood a server with traffic to overwhelm its infrastructure. This causes a site to slow to a crawl or even crash so legitimate traffic won’t be able to reach the site.

Most DDoS attacks are done with botnets – groups of computers all acting together. These computers will all attempt to access a website simultaneously, overwhelming the server and bringing it down.

This was the case with Boston Children's Hospital in 2014. Anonymous (a well-known hacktivist group) targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their patients, a 14-year-old girl, be admitted as a ward of the state and that custody be withdrawn from her parents.

Specially during the covid-19 pandemic, hospitals across the globe were hit by DDoS attack, the most recent being the AIIMS Delhi.

### SOLUTION:

1. <https://www.mdpi.com/1424-8220/19/2/326>

Based on the above paper, even if hacker tries DDoS:

1. He won't get access to network without proof of Authority
2. Even if he somehow gained access, if its address is not registered with the cluster head, then its communication won't be recorded & hacker will eventually be blocked

2) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8422839/>

Kalkan FAK. A distributed filtering mechanism against ddos attacks: scoreforcore. *Comput Netw.* 2016;108:199.

the collaborative filtering technique employs a distributive strategy for identifying and filtering harmful packets. However, its main disadvantage is it cant differentiate DDoS traffic from flash crowd.

This paper uses Packet Score, a technique given by (Kim Y, Lau WC, Chuah MC, Chao HJ. PacketScore: a statistics-basedpacket filtering scheme against distributed denial-of-service attacks. *IEEE Trans Dependable Secure Comput.* 2006;3(2):141–155.) where the score of each incoming packet is calculated and if less than the set threshold, it is discarded. Along with PacketScore, it also uses Entropy calculation module to differentiate between legitimate and DDoS requests.

## 3. Session stealing attack

Session hijacking is a technique used by hackers to gain access to a target's computer or online accounts. In a session hijacking attack, a hacker takes control of a user's browsing session to gain access to their personal information and passwords.

Various approaches include:

1. Reroute traffic using DNS Spoofing or ARP Spoofing
2. Replacing HTTPS with HTTP
3. Creating a WiFi hotspot

<https://healthitsecurity.com/news/cvs-health-faces-data-breach1b-search-records-exposed>

In 2021, more than 1 Bn healthcare records were compromised when CVS Healthcare was attacked. Their websites had incorrectly setup databases, which allowed an attacker to obtain crucial data via session hijacking attacks.

### SOLUTION:

1. 11<https://www.researchgate.net/profile/Arnob-Paul-2/publication/324448404_Survey_of_the_Protection_Mechanisms_to_the_SSL-based_Session_Hijacking_Attacks/links/6022f588299bf1cc26b5462d/Survey-of-the-Protection-Mechanisms-to-the-SSL-based-Session-Hijacking-Attacks.pdf>

The web was 1st designed based on the HTTP Protocol. However, because of the session stealing attacks, HTTPS was introduced which is based on HTTP+SSL where SSL provides a secure communication medium. Most of the session stealing attacks happen when instead of HTTPS, users enter sensitive information on HTTP pages which can be accessed by hackers. Hence, browsers should always show a warning when going to sites where security certificate is not trusted!

1. <https://dl.acm.org/doi/pdf/10.1145/2220352.2220353>

This paper proposes using One Time Cookies (OTC) wherein Instead of utilizing a single, static token to authenticate each request, OTC produces a unique token based on a session key for each request generated by the user. Because each OTC token is associated with a specific request through a hash-based message authentication code (HMAC), an attacker cannot utilize OTC tokens to illicitly redirect a session. The main advantage is the need of the single static cookie is eliminated! Gmail uses a related concept where the cookies change every few seconds so it is impossible to compromise it

1. Other common solutions include never using public WiFi.

## 4. Malicious codes

Malicious code is code inserted in a software system or web script intended to cause undesired effects, security breaches, or damage to a system. Taking advantage of common system vulnerabilities, malicious code examples include computer viruses, worms, Trojan horses, logic bombs, spyware, adware, and backdoor programs. Visiting infected websites or clicking on a bad email link or attachment are ways for malicious code to sneak its way into a system.

The most common form of malicious code is the computer virus, which infects a computer by attaching itself to another program and then propagating when that program is executed. Another common form is the worm, which makes copies of itself, spreading through connected systems and consuming resources on affected computers.

Case Study: T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740

### SOLUTIONS:

## 5. Access control

Access control describes the process of regulating who can access or use resources within a computing environment. It’s a security principle used by organizations to minimize risks by limiting access to a resource or place.

Examples of access control include passwords, biometric scanning, and security clearance. Software programs or scripts can also be used to restrict or limit access to files on a computer system.

Access control policies ensure that users are who they claim to be and have the proper access to data.

Access control encompasses a wide range of security features you can implement at your healthcare facility, but electronic access control is more specific. This type of access control uses technology to better protect your facility, patients, staff, and assets.

Health care is under attack. In 2022 alone, over 1000 confirmed attacks on health care took place in emergency-affected countries and fragile settings. These attacks deprive people of urgently needed care, endanger health care providers, and undermine health systems.

WHO's Attacks on Health Care initiative aims to ensure that health workers everywhere are able to provide health care in a safe and protected environment without disruption from acts of violence. The initiative has three main pillars of work including the systematic collection of evidence of attacks, advocacy for the end of such attacks, and the promotion of good practices for protecting health care from attacks.

### SOLUTIONS:

1. . Kamau, C. Boore, E. Maina and S. Njenga, "Blockchain technology: Is this the solution to emr interoperability and security issues in developing countries?", *2018 IST-Africa Week Conference (IST-Africa)*, pp. 1, 2018.

Blockchain was proposed as a secure solution to manage the Electronic Health Records of patients. Its main advantage is it being tamper-proof (hacker needs to demonstrate Proof of Work to add a transaction). However, the 2 major disadvantages include:

1. Not suitable for huge data like X-ray images or CT-Scan videos
2. Access Control mechanisms can still be compromised

2) H. Guo, W. Li, M. Nejad and C. -C. Shen, "Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 44-51, doi: 10.1109/Blockchain.2019.00015.

It proposes a framework that offers a hybrid architecture that uses both blockchain and edge nodes to allow access to Electronic Health Records of patients. The blockchain-based module handles identity and access control regulations and acts as a secure log of access events inside the architecture. Moreover, off-chain edge nodes store EHR data and implement attribute-based access control on EHR data based on the rules of Abbreviated Language For Authorization (ALFA) in combination with blockchain-based access control logs.

## 6. Ransomware attack

Ransomware is a type of malware that infects systems and files, rendering them inaccessible until a ransom is paid. When this occurs in the healthcare industry, critical processes are slowed or become completely inoperable.

Ransomware, in which hackers extort companies and organizations by breaking into and often holding computers and files hostage, has become one of the toughest problems in cybersecurity and a threat to industries around the world. But it can be especially damaging when it hits hospital chains, causing trickle-down damage for patient care across the country.When Kelley Parsi took her 3-year-old son to a hospital in Des Moines, Iowa, after tonsil surgery, she expected doctors to quickly treat him for pain and dehydration and send him home. Instead, she said, the trip became one of the scariest days of her life.

The computer system that automatically calculated medicine doses wasn’t working, the resident doctor informed her, and he mistakenly “gave him five times what was prescribed,” she said. She later learned a cyberattack had taken down some of the hospital’s digital tools.She waited for hours, terrified, while her son’s body processed the overdose. “Because of the cyberattack, my son overdosed on pain medicine,” Parsi said. He made a full recovery, she said.

Some famous ransomware attacks include WannaCry, CryptoLocker, jigsaw and GoldenEye.

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9899708>

The various types of Ransomware attacks include:

1. Locker Ransomware - the users can't access data till ransom is paid
2. Crypto Ransomware - the data is encrypted & ransom is demanded in exchange for the decryption key.
3. Double Extortion Ransomware - the data is encrypted and users are threatened that it will be made public unless ransom is paid.

The hackers use various methods to perform ransomware attack like:

1. Phishing Attack

Phishing is a method of attempting to gain usernames, passwords or medical data, for malicious reasons, using communications such as email or messaging by encouraging recipients to click links to legitimate looking websites running malicious code or to download or install malware.

Cytometry Specialists, known as CSI Laboratories, disclosed a phishing attack that impacted 244,850 individuals. On July 8, CSI discovered that an employee email account had been compromised.

After discovering the incident, CSI said it took steps to isolate the email account and investigate the attack.

“We believe the access to a single employee mailbox occurred not to access patient information, but rather as part of an effort to commit financial fraud on other entities by redirecting CSI customer health care provider payments to an account posing as CSI using a fictitious email address,” CSI stated in a notice to patients.

1. Botnets

Emotet can steal email from victims’ mailboxes, which allows the attackers to craft convincing yet malicious messages to fool recipients. Attackers can also use it to steal SMTP credentials, useful to take over email accounts.

Gamut seems to specialize in spam emails that try to establish a relationship with the victims. This might be in the form of a dating or romance guise. In other campaigns, the actors behind the botnet send out messages hawking pharmaceuticals or job opportunities

Necurs first emerged in 2012 and has spread a variety of threats, ranging from Zeus to ransomware. While its activity has received far more attention in the past, Necurs appears to have faded into the background. However, this botnet is still very much active. In fact, the Necurs botnet is the primary distribution vehicle for a variety of scams, including digital extortion.

### SOLUTION

1. N. Thamer and R. Alubady, "A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research," 2021 1st Babylon International Conference on Information Technology and Science (BICITS), Babil, Iraq, 2021, pp. 210-216, doi: 10.1109/BICITS51482.2021.9509877.

This paper lists the 4 main proposed mechanisms against the ransomware attack:

1. J. K. Rajesh Kumar, Xiaosong Zhang, WenYong Wang and Riaz Ullah Khan, "A Multimodal Malware Detection Technique for Android IoT Devices Using Various Features", pp. 64411-64430, 2019.

Machine Learning + Blockchain: ML is used to analyze & classify the requests and the data is stored in blockchain. However, it doesn’t perform well enough if we use some strategies to hide the malware.

1. A. Almashhadani, M. Kaiiali, S. Sezer and P. O’Kane, "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware", *IEEE Access*, vol. 7, pp. 47053-47067, 2019

This paper proposes an intrusion detection system to identify the malware.

1. M. Wazid, A. K. Das and S. Shetty, "BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare," in IEEE Transactions on Consumer Electronics, 2022, doi: 10.1109/TCE.2022.3208795.

This paper proposes using blockchain enabled security, the main advantages of blockchain are because it is unanimous and, immutable and decentralized, it is impossible to modify or hack into and thus ensures data integrity. Machine Learning Algorithm runs to detect various methods of Ransomware attack while Blockchain is used as a secure backup and data-alteration and data leakage are very difficult.

## 

# IIOT

## 1. Sybil attack

In a sybil attack, an attacker takes control of multiple nodes in the network. Various identifiers are assigned to the same node and operate. No trusted nodes are present in the blockchain network. The attacker is surrounded by the fake nodes and closes all the transactions of the nodes. In sybil attack, an attacker pretends to be so many people at the same time. It may lead to problems for the peer-to-peer network. The network has been manipulated and multiple fake identities take control of the network. An unknown attacker can control the whole network from outside but it looks like multiple attackers are controlling the network. In sybil attack, it is tough to identify the difference between the honest node, sybil node, and our node. Using the fabricated devices the performance of computer devices has been reduced and it creates traffic jams in the network. These kinds of attacks are very destructive as they decrease the overall execution of the devices and it performs the affect network's availability. Sybil attack is one of the computer network-based service attacks.

a Bitcoin Sybil attack can be used to obtain information about the IP address of a user connecting to the network. This compromises the security, privacy and anonymity of web users.

Furthermore, a Sybil Attack can be used to take an entire Blockchain in control and then modify information / reverse transactions etc which can lead to disastrous consequences.

### SOLUTIONS:

Although there is no guaranteed solution to Sybil Attacks, there have been several proposed algorithms.

* They propose a solution using consensus algorithms like Proof of Work (PoW) & Proof of Stake (PoS). These consensus algorithms make it very impractical to carry out Sybil Attack. Eg: Bitcoin uses a set of rules to create a new node of which one of them is that the ability to create a block has to be proportional to the total processing power of my device. Hence, it is infeasible to carry out Sybil attack
* [Airehrour et al., 2019](https://www.sciencedirect.com/science/article/pii/S1084804519303418?casa_token=bMu52Orj0ygAAAAA:70q8gKe-7aj2PNLLb3LIy3qiaNrfD_KHyTVn3ub5G5INE2MCnlnwsjraB9RlvLHht4kOxjHFR28#bib3)

They proposed SecTrust-RPL, a trust-aware RPL routing protocol that employs a trust-based methodology. The SecTrust framework is included within the ContikiRPL, which acts as the central engine for routing choices and identifying malicious nodes. The selection is made exclusively on the basis of node trust, and bad nodes are swiftly segregated from the network. At the time of transfer of packets, each node calculates the Trust score of its neighbors. The nodes with high trust are marked for further routing while nodes with low score are categorized as compromised. Thus, the network segregates bad nodes before they can multiply and overpower the honest nodes. However, the decision of identifying Malicious Nodes still needs more research. Moreover, if the malicious nodes overpower the honest nodes, they can destroy all the honest nodes.

## 2. Sinkhole attack

Sinkholes are nodes that have been hacked. In this attack, as data is traveling from source to destination, when the data reaches the attacked node/sinkhole node, it is redirected to an incorrect destination. The hacked node attracts network traffic in this attack by publishing a fake routing update. Sinkhole attacks can also be used to launch other network attacks such as spoofing attacks and selective forwarding attacks.

Sinkhole attack is a network layer assault in which an attacker attempts to gather a large amount of traffic in order to prevent the base station from getting all sensing data from nodes.

Sinkhole attacks can be used to compromise sensitive information like military networks.

As most of the IoT devices have limited battery and computational power, security aspect is often ignored which makes it an ideal target to attackers to perform sinkhole attack.

C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), Macau, China, 2009, pp. 1-5, doi: 10.1109/ICICS.2009.5397594.

A selective forwarding attack is when the malicious nodes forwards only selective packets and drops other packets. It is an intelligent version of Sinkhole Attack wherein it behaves normally for all other nodes while causing DoS attack on those nodes whose packets are dropped.

### SOLUTIONS

* <https://arxiv.org/ftp/arxiv/papers/1505/1505.01941.pdf>:

This paper reviews in detail various measures to defend against sinkhole attack.

* . Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on (pp. 711-716). IEEE.

They formulated an algorithm that can detect a sinkhole attack based on comparing the CPU Utilization of every node over a period of time. If it exceeds the threshold, it is identified as a malicious node. This approach can also be used by monitoring the network traffic of all nodes and flagging that node which shows a sudden spurt in activity.

* Fessant, F., Papadimitriou, A., Viana, A.,Sengul, C. and Polamar, E. (2011) A sinkhole resilient protocol for wireless sensor network: Performance and security analysis. Computer Communications, 35(2), 234-248.

Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE

They recommended using a key-based approach to isolate sink nodes. There is a set of public key and private keys and using the concept of cryptography, can be used to identify if the message comes from the base station or some other node and to verify the authenticity of the message. The keys were uploaded when the Network was offline so it can't be misused. This way, sinkhole attacks are prevented.

* C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," 2009 7th International Conference on Information, Communications and Signal Processing (ICICS), Macau, China, 2009, pp. 1-5, doi: 10.1109/ICICS.2009.5397594.

They articulated RSSI based Detection Approach wherein at the start where all nodes behave normally, a visual graph map of network traffic is created and then, based on the anomalous network traffic, sinkhole nodes can be isolated.

## 3. Liveness attack

Three phases are presented in this attack preparation phase, transaction denial phase, and blockchain retarder phase. In the first phase, the attacker joins with the honest blockchain node. In the second phase, the malicious node goes for the transaction but it creates a delay in the transaction and blocks all the genuine blocks. In the third phase, the transaction slows down. The third phase is called the blockchain render phase.

## 4. Replay attack

## 5. Worm

## 6. Back door attack

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

Backdoor installation is achieved by taking advantage of vulnerable components in a web application to remotely control the entire website, steal data, modify content or even install malware in the user’s devices. Once installed, detection is difficult as files tend to be highly obfuscated.

For example wordPress was spotted with multiple backdoors in 2014. These backdoors were WordPress plug-ins featuring an obfuscated JavaScript code. This vulnerability is extremely critical, especially for devices that use Deep Neural Networks (DNN). because many deep learning and machine learning models are trained with data from third-party sources, it provides hackers with an opportunity to exploit that source and manipulate training data, thus giving wrong results. Example: it can penetrate into the algorithm of a self-driving car and when it sees the sign: “school ahead”, it may intentionally misclassify causing the trigger and cause to speed up instead of slowing down, thus leading to critical situations.

### SOLUTIONS

1. B. Chen et al., "Detecting backdoor attacks on deep neural networks by activation clustering", *Proc. AAAI Workshop*, 2019

They advocated training neural network on the poisoned dataset and using Activation Clustering (A.C) to classify any malicious activity. Although the classification of both normal and malicious activity is the same, the methodology is different. Using this principle, the last hidden layer’s activations are gathered and segmented according to their class.Clustering involves employing the Independent Component Analysis to reduce the dimensions. Once clustered, they use k-means to seperate the dataset and the majority is normal while minority is the backdoor triggers.

1. B. Hou et al., "Mitigating the Backdoor Attack by Federated Filters for Industrial IoT Applications," in IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3562-3571, May 2022, doi: 10.1109/TII.2021.3112100.
2. <https://www.sciencedirect.com/science/article/pii/S157087052100216X?casa_token=-CdUEpfsr1YAAAAA:tmBNf9mP6uAIi4PFfughKGudmBz2ntjL1fgh7p1ZxEd4WdBNHUQYlCiizrfpDRi0QVK_LaqODFA>

Although Deep Learning is one of the best techniques to identify malicious events, it was too computationally intensive for IIoT Devices. Hence, the authors of this paper came up with a solution to distribute the work to edge servers - CoDefend. They mainly focus on detecting trigger events. Using STRIP-based Detection, they detect Backdoor attacks. If detected, edge servers use CycleGAN to find out all the possible triggers. Moreover, they also implement the model mitigation strategy given by (K. Liu, B. Dolan-Gavitt, S. Garg, Fine-pruning: Defending against backdooring attacks on deep neural networks, in: Proc. of RAID, 2018) by re-modifying / updating the model.

## 7. Eavesdropping

An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, [smartphone](https://www.investopedia.com/terms/s/smartphone.asp), or another connected device.

The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.

Eavesdropping is a deceptively mild term. The attackers are usually after sensitive financial and business information that can be sold for criminal purposes.

### SOLUTIONS

1. J. H. Anajemba, C. Iwendi, I. Razzak, J. A. Ansere and I. M. Okpalaoguchi, "A Counter-Eavesdropping Technique for Optimized Privacy of Wireless Industrial IoT Communications," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6445-6454, Sept. 2022, doi: 10.1109/TII.2021.3140109.

The study delves deeper into the design of optimal jamming parameters by proposing a new model called the "Optimal Counter-Eavesdropping Channel Approximation Technique" (OPCECA) for defending against eavesdropping attacks in IIoT. It is a powerful tool for legitimate nodes to transmit information without giving the eavesdropper precise channel approximations. Thus, OPCECA effectively neutralizes the impact of the eavesdropper's location and preserves privacy by using artificial noise. The authors also examine the eavesdropper's optimal performance and how it influences privacy, and illustrate the performance advantage of OPCECA over existing models.

1. X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu and M. S. Hossain, "Enabling secure authentication in industrial IoT with transfer learning empowered blockchain", *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7725-7733, Nov. 2021.

This article presents a revolutionary Authentication technique based on Transfer Learning enabled Blockchain (ATLB). It balances the best of both: Blockchain and Authentication Techniques to ensure Data privacy and integrity. Blockchains are used in ATLB to provide privacy preservation for industrial applications. Furthermore, the transfer learning-based authentication method is incorporated to ensure that only verified users get access. ATLB, in particular, uses a guiding deep deterministic policy gradient algorithm to train a specific region's user authentication model, which is then transferred locally for foreign user authentication or cross-regionally for another region's user authentication, significantly reducing model training time. The main advantage of this solution is inspite of the use of Blockchain, it gives high throughput and low latency.

1. F. Kohnhäuser, D. Meier, F. Patzer and S. Finster, "On the Security of IIoT Deployments: An Investigation of Secure Provisioning Solutions for OPC UA," in IEEE Access, vol. 9, pp. 99299-99311, 2021, doi: 10.1109/ACCESS.2021.3096062.

OPC UA (Open Platform Communications Unified Architecture) is a communication protocol that is used for industrial automation and the Internet of Things (IoT) like electricity generation and control units, manufacturing plants etc. It is a platform-independent, service-oriented architecture that enables the secure and reliable exchange of data between diverse systems, devices, and applications. However, as the interdependency increases so does the risk of cyber attacks. The authors review the current security standards in the OPC UA and also identify some of the prevailing vulnerabilities. (sir, this was more of a review paper so didnt understand their contribution)

## 8. Tampering

## 9. Routing attack

Routing attack drop, redirect the data packets. Routing attack blocks the messages, propagates the network, and changes them before transferring them to their peers. The attack detection is possible when a receiver receives a different copy of a transaction from another node. In this attack, an attacker divides the network into two or more partitions. The partition parts cannot communicate with each other. Routing attacks come under the network layer attack. In the peer-to-peer network-based attack we already described the DDoS attack.

The rank attacks are the most devastating for RPL protocol since they yield other attacks such as sinkhole, black hole, loops etc. In RPL, the rank is calculated by an objective function in order to locate the position of each node in the DODAG. This rank can be manipulated by a compromised node to intentionally downgrade specific QoS parameters. For instance, by decreasing its rank, a compromised node could be falsely situated close to the root node and could maliciously manipulate a large amount of traffic flowing through it. Conversely, a compromised node may excessively increase its rank and eventually disrupt the network topology, reset the timer trickle, trigger the sending of control messages thus depleting neighboring nodes' resources.

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths.

### SOLUTIONS:

1. C. Li, Y. Liu, J. Xiao and J. Zhou, "MCEAACO-QSRP: A Novel QoS-Secure Routing Protocol for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18760-18777, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3162106.

This article discusses a new QoS-secure routing protocol based on the node trust mechanism. According to the success rate of sending and receiving by nodes, their direct and indirect success score is calculated and accordingly, the nodes are given weight to be followed by routing protocol. However, to ensure that the time complexity of message traveling does not increase, a novel “QoS-secure routing algorithm (MCEAACO-QSRP)” is proposed that follows “multiobjective chaotic elite adaptive ACO ''.

1. L. Wallgren, S. Raza and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things", *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.

They advocate the setting up of border routers that act as an Intrusion Detection System against sinkhole attacks. However, the main limitation is it works only with IPSec which requires a lot of power to run and isn't feasible for IoT devices.

1. K. Chugh, A. Lascbae and J. Loo, "Case study of a black hole attack on 6lowpan-rpl", *SECURWARE 2012: The Sixth International Conference on Emerging Security Information Systems and Technologies*, 2012.

The authors propose a mechanism that measures various parameters of each node like packer delay etc and accordingly, based on threshold, classifies them as malicious or not. A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment and J. Schonwalder, "Addressing dodag inconsistency attacks in rpl networks", *Global Information Infrastructure and Networking Symposium (GIIS) 2014*, pp. 1-8, 2014. Improves the above concept by using adaptive threshold algorithm that also accounts for change in the network conditions to classify nodes as malicious or not. These solutions work on mitigating blackhole attack.

1. G. Glissa, A. Rachedi and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 2016, pp. 1-7, doi: 10.1109/GLOCOM.2016.7841543.

This article advocates the use of Secure RPL based on the Routing Protocol for Low Power and Lossy Networks in 6LoWPAN networks. The primary goal of SRPL is to prevent misbehaving nodes from fraudulently modifying message control parameters like a node's rank, which might disrupt a network by generating a bogus topology. To cope with internal attacks such as sinkhole, black hole, selective forwarding assaults, and so on, they also propose the notion of rank threshold as well as hash chain authentication that controls the rate of increase or decrease of the rank of a node. The node requires authentication based on hash values while repositioning itself in the network which prevents rank manipulation.

1. <https://www.sciencedirect.com/science/article/abs/pii/S1570870521001748>

It uses Deep Learning based GAN network to identify Routing Attack.

10. Malware Attack

Example: Outage of Electricity in Mumbai caused by the insertion of Trojan horses by Chinese Hackers

# Electric vehicle

## 1. False data injection attack

<https://crashtest-security.com/false-data-injection-attack/#:~:text=False%20data%20injection%20attacks%20(FDIA,the%20control%20center's%20computational%20capability>.

False data injection attacks (FDIA) are one form of data attack orchestrated when adversaries can alter/modify the original measurements supplied by these sensors, affecting the control center's computational capability..

**December 2015 Ukraine Blackout**

This is one of the first publicly acknowledged cyber attacks on power system automation software. On 23rd December 2015, attackers were able to hack Ukraine’s power grid system and use spear-phishing techniques to install malware that led to a blackout affecting over 200,000 consumers. The malware bypassed a bad data detection mechanism and remotely connected with employees’ machines to disconnect 30 substations for over three hours. The adversaries also blocked telephone device communication networks that prevented residents from reporting the outage to concerned officials.

**Stuxnet Worm on Iranian Nuclear Power Stations**

[Stuxnet](https://spectrum.ieee.org/the-real-story-of-stuxnet) is a computer worm that targets programmable logic controllers used to automate industrial processes and power systems. The worm has been under development since the mid-2000s and usually targets computers that use Windows OS and run the Siemens Step 7 real-time data transmission software. As part of the planned attack, attackers planted the worm on Iranian critical infrastructure management centers, collecting real-time data from industrial systems. They also caused the uranium gas centrifuges to spin out of control and cause maximum damage to the entire power grid.

### SOLUTIONS: [As the demand for EV Increases, the uncertainty in charging causes extra power losses and undesirable voltage variations, which may overburden the existing electrical infrastructure as emergence of EV increases. A "smart grid" system that allows EVs to connect with an EV aggregator module should be implemented as a feasible option.] However, as EV’s are directly connected with the power grid, they are also vulnerable during the charging period.

1. <https://www.sciencedirect.com/science/article/pii/S2352146521000715>
2. T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740.
3. <https://www.sciencedirect.com/science/article/pii/S0167404821003643>

## 2. GPS deception

<https://www.okta.com/identity-101/gps-spoofing/#:~:text=GPS%20spoofing%20involves%20a%20radio,and%20information%20to%20the%20receiver>.

GPS spoofing involves a radio transmitter near a target that interferes with the actual GPS signals being transmitted. GPS signals are often weak and transmitted through satellites. A stronger radio transmitter can be used to override the weaker signal and send illegitimate coordinates and information to the receiver.

<https://www.missionsecure.com/blog/the-cyber-attack-on-garmin-exposing-gps-vulnerabilities>

In 2016, Iran captured two U.S. Navy command boats who strayed into Iranian waters. The sailors claimed their GPS showed they were in international waters.

The Black Sea GPS spoofing incident in June 2017 is well-publicized where over 20 vessels in the Black Sea region showed their locations many miles in-land.

In March 2019, the Center for Advanced Defense Studies (C4ADS) published a report on GPS spoofing incidents, noting “9,883 GNSS spoofing instances affecting 1,311 vessels across ten locations in Russia, Crimea, and Syria between February 2016 and November 2018.”

Earlier this year, the U.S. government received inquiries regarding GPS circle spoofing in Iran. Coincidentally, the Iranian GPS circle spoofing analysis highlights how Strava data also had anomalies for users. (Strava is a strategic Garmin partner and area of service outage with Garmin devices unable to upload to Strava.)

## 3. Unauthorized Access

### Solutions:

1. T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740

## 4. DOS

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

**Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

**ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

**SYN flood** – sends a request to connect to a server, but never completes the [**handshake**](https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan). Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

For example, Black Friday sales, when thousands of users are clamouring for a bargain, often cause a denial of service. But they can also be malicious. In this case, an attacker purposefully tries to exhaust the site's resources, denying legitimate users access.

## 4. Modification attack

<https://www.sciencedirect.com/topics/computer-science/modification-attack#:~:text=Modification%20attacks%20involve%20tampering%20with,data%20contained%20in%20the%20file>.

Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.

<https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks>

Modifying the contents of messages in the network.

Changing information stored in data files.

Altering programs so they perform differently.

Reconfiguring system hardware or network topologies.

T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740.

## 5. Sybil attack

<https://www.geeksforgeeks.org/sybil-attack/>

Sybil Attack is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal(with respect to rules and laws set in the network) actions in the system. A single entity(a computer) has the capability to create and operate multiple identities(user accounts, IP address based accounts). To outside observers, these multiple fake identities appear to be real unique identities.

## 6. Wormhole attack

<https://www.sciencedirect.com/topics/computer-science/wormhole-attack#:~:text=Wormhole%20attack%20is%20a%20severe,these%20data%20packets%20are%20broadcasted>.

Wormhole attack is a severe and popular attack in VANETs and other ad-hoc networks. This attack involves two or more than two malicious nodes and the data packet from one end of the malicious node is tunneled to the other spiteful/malicious node at the other point, and these data packets are broadcasted.

## 7. Reply attack

<https://www.kaspersky.com/resource-center/definitions/replay-attack>

A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants. The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network. The attack could be successful simply by resending the whole thing.

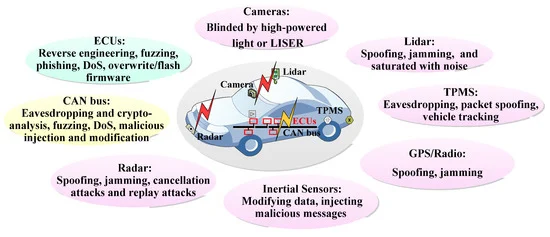
8. RSU spoofing

9. Jamming attack

All reference for autonomous vehicle from the below link

<https://research-management.mq.edu.au/ws/portalfiles/portal/140649743/140591961.pdf>

# Autonomous vehicle:

[https://ieeexplore.ieee.org/abstract/document/9447840](https://ieeexplore.ieee.org/abstract/document/9447840?casa_token=xEDy-TkeTYIAAAAA:lFt-pBx0sTU2ynKSYneP_ScL89J5Yn29hMgirqrj8VdHrp5IVRpoeWGWOb3TcYN04YSgPvt2oyw)

1. Malware attack

The On-Board Diagnostics (OBD) is one of the most vulnerable parts of self-driving cars to have malware attacks. The authors in [89] showed that an attacker could use the malware-infected diagnostic tool to insert malware to ECU via OBD. These malware codes can tune and reprogram the codes of ECUs. An ECU infected by the malware may fail to respond to communicate with the other OBU components (e.g., Lidar, Camera, Radar), compromising the safety of the self-driving cars. The first remote intrusion of a vehicle leading to cyberphysical controls against Chevy Malibu was introduced in 2011 by Checkoway et al. [45]. The attacker manipulated the radio of the vehicle using a Bluetooth stack weakness and inserted the malware codes by syncing their mobile phones with the radio. After the radio was hacked, a gateway system disconnected the intruder from the high-speed CAN network. However, they could repurpose this gateway from their open low-speed CAN network. Afterward, the inserted code could send messages to the ECU of the vehicle that could lock the brakes.

2. MITM attack

Self-driving cars use wireless communication methods with other vehicles and roadside infrastructures. These self-driving cars also use wired or wireless communication methods to communicate with OBUs. In a man-in-the-middle attack, an attacker can manipulate the communication messages between the two entities (e.g., two cars of a VANET in V2V, vehicle, and RSU in V2I), while both entities believe that they are in direct communications with each other. An attacker can take control of OBU or RSU and actively eavesdrops, replays, and modifies the messages transmitted between two entities [90]. As alluded in Figure 4, the authors [91] conducted a similar assault on a Jeep Cherokee in 2015. By using the Internet-accessible weakness in Jeep Cherokee’s communication method, the hackers performed a man-in-the middle attack, and they intercepted the communication messages between ECUs and the braking system. Hackers were able to reconfigure the firmware on the central processing unit of the vehicle with CAN network access for another processor. Then they sent CAN messages that regulate the steering, brakes, and vehicle acceleration. The central processing unit was unable to detect that the instructions (to slow down or turn right) came from an external device that was manipulating the communication message between ECUs and OBUs.

SOLUTIONS:

1. G. R. Andreica, L. Bozga, D. Zinca and V. Dobrota, "Denial of Service and Man-in-the-Middle Attacks Against IoT Devices in a GPS-Based Monitoring Software for Intelligent Transportation Systems," 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 2020, pp. 1-4, doi: 10.1109/RoEduNet51892.2020.9324865.
2. J. Cui, L. Shen, Liew, G. Sabaliauskaite and F. Zhou, "A review on safety failures security attacks and available countermeasures for autonomous vehicles", *Ad Hoc Networks*, vol. 90, pp. 101823, July 2019.
3. <https://www.sciencedirect.com/science/article/pii/S235286481930197X>
4. <https://www.sciencedirect.com/science/article/pii/S1877050919310610>

## 3. DOS attack

X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6240-6259, July 2022, doi: 10.1109/TITS.2021.3085297.

### DoS attacks [36] happen when the adversary blocks the whole communication channel with interference signals. The adversary inserts useless messages or creates some issues on the network nodes. Hence, authentic users cannot access network services. Correct messages cannot reach their destinations. DoS attacks can cause delay and interfere the receiver’s response. In the environment of CAVs, some delay may affect the driving security of the vehicle. Even one second can cause or avoid an accident. In addition, the request for response time is comparatively high [37]. DoS attacks are dangerous and fatal for CAVs.

### SOLUTIONS:

1. Sliding Mode and Adaptive Estimation
2. Bandwidth and Entropy
3. Similarity of Sliding Windows

DoS attacks are difficult to be corrected even though they can be detected. Early detection will be helpful to thwart the attacks or alert the driver to take some efficient measures. To resist DoS attacks, there are some strategies, including sliding mode and adaptive estimation [84], bandwidth and entropy [85], and similarity of sliding windows [86].

A real-time mechanism [84], which includes a set of observers that are designed by the usage of sliding mode and adaptive estimation theory, can be used to detect the occurrence of DoS attacks, and estimate the effect of these attacks on the connected vehicle system. Inspired by the port-hopping mechanism, Jie *et al.* [126] designed a simple but effective defense mechanism, which has the advantage that the detection and filtering out of malicious packets can be implemented without any change in the existing protocol. Based on the usage of bandwidth and entropy, Kumar and Mann [85] proposed an algorithm for the detection of DoS attacks in vehicular networks. Then, the authors proposed a packet detection algorithm that can be used for preventing DoS attacks. Based on the similarity of sliding windows, an improved DoS attacks detection strategy [86] is designed to detect each type of DoS attacks.

4. Ransomware attack –

5. Sybil –

## 6. Attack on IMU (Inertial Measurement Unit), LIDAR (Sensors)

Along with GPS, Inertial Measurement Unit (IMU) is used for vehicle navigation (e.g., positioning, motion tracking). To this end, Zhao [102] showed how the advancement of telemetric systems could introduce an integrated and connected community and thus enhance the capability of a vehicle contributing to safe driving through ITSs and on-board entertainment. This is because automotive technology is rapidly advancing towards V2V and V2I connectivity. Such advancement and integration expose cars to potential threats. Early research by Wolf et al. [103] identified such threats when the ECUs were being interfaced with systems like Bluetooth, GSM, and GPS modules to receive updates.

For discovering the vulnerabilities in the IMU and wireless connectivity, attackers demonstrated how they took control of a Cherokee Jeep. In July 2015, two scientists, Charlie Miller and Chris Valasek, hacked into the Cherokee from Miller’s basement when the car itself was ten miles off the highway [91]. They were able to remotely control car functions via a simple 3G connection that exploited a loophole in the Uconnect system. Uconnect is an Internet-connected software that controls the navigation and entertainment system of the vehicle. They also rewrote the adjacent chip firmware into the car’s head unit through Uconnect’s cellular connectivity loopholes and creating an entry point. Consequently, they were able to send instructions to suppress the brakes and gain control via the IMU. The driver of the car had no power over either the steering wheel or the pedals.

Lidar technology is used to generate 3D maps of a vehicle environment for localization, obstacle avoidance, and navigation. Lidar measures the distance by measuring the flight time of a laser beam projecting vertically to the ground. This flight time is used to determine the presence of an object and its distance from the car. Self-driving cars are highly dependent on Lidar systems. As shown in Table 4, the Lidar of a Tesla’s vehicle was under attack by hackers and unable to detect a van in front of that autonomous vehicle. As a consequence, this Tesla vehicle hit the van [128].

Stottelaart et al. [129] showed by a lab experiment the likelihood of congestion because of an attack on Lidars by leading the emanating light posterior to the scanner component, which has the same rate of recurrence as a laser replicating from the object [129]. Petit and Shladover [111] ethically hacked a self-driving car using a raspberry pi and thereby breached automatic, and net linked vehicles using their created cyber-attacks. They were capable of interfering with the Lidar structure to coax it into not sensing any highway obstructions like debris, people, cars, buildings, etc. This interference can lead an automatic or self-driving car when moving at maximum speed to stopover, and thereby inactivating the vehicle. For example, because of the car sensors receiving jamming signals from raspberry pi, a Lidar unit failed to notice any highway debris or people or obstructions during its right turn. Consequently, the car hit the obstacles and immediately stopped after traveling around a hundred meters.

### SOLUTIONS:

1. Authentication
2. Consistency Check
3. Sensor Fusion
4. Spatio-Temporal Challenge Response

In order to improve the security of ultrasonic sensors, Xu *et al.* [62] proposed two defense strategies, namely single sensor-based physical shift authentication which is used for verifying signals on the physical level, and multiple sensor consistency check that multiple sensors are employed to verify signals on the system level. In order to defend sensor spoofing attacks, Matsumura *et al.* [63] proposed a solution that authentication fingerprint is superimposed onto light wave itself. In order to counter sensor interference [116], sensor fusion and backup cameras [64] are used to verify the legality and precision of ultrasonic sensor measurements. Kapoor *et al.* [66] used the technique of spatio-temporal challenge-response to detect and stop sensor spoofing attacks by verifying physical signals in the analog domain. In 2019, Miura *et al.* [117] used random-chirp modulation to defend a low-cost distance-spoofing attack on a mmWave Frequency Modulated Continuous Wave radar. In [65], the sensor fusion technique, which intelligently combines data from various sensors to improve performance, is used to defend lidar spoofing attacks. The influence of remote sensor attacks can be reduced by modifying the internal sensing structure of the lidar.

## 7. Attack on GPS

GPS spoofing is a rather complicated process involving the generation of incorrect GPS signals to confuse GPS receptors. An attack by spoofing can, for example, start with the transmission of fake signals synchronized with the correct signals found at the target recipient. The attack increases the strength of the phishing signals, which progressively divert the position from the target. This sounds relatively straightforward in principle; however, the hardware required to generate realistic signals is a complicated operation. As hackers see increasingly potential benefits of GPS spoofing, the generation of simplified plugs and play controls will become a reality in the future. The public domain already holds a complete theory on how to spoof GPS attacks. For example, the literature on successful attacks on GPS has been published [136].

There are two main spoofing modes: generating false message information and increasing signal propagation delay, which correspond to two spoofing modes: generating mode and forwarding mode.

CASE STUDY: A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing", *J. Field Robot.*, vol. 31, no. 4, pp. 617-636, 2014.

### SOLUTIONS:

1. Using Machine Learning based approach:

S. Semanjski, A. Muls, I. Semanjski and W. De Wilde, "Use and Validation of Supervised Machine Learning Approach for Detection of GNSS Signal Spoofing," 2019 International Conference on Localization and GNSS (ICL-GNSS), Nuremberg, Germany, 2019, pp. 1-6, doi: 10.1109/ICL-GNSS.2019.8752775.

The paper discusses monitoring the inter-correlation of numerous GNSS observables and measurements from instruments which are taken as an input for a supervised machine learning-based technique to detect potentially fake GNSS signals. C-Support Vector Machines are used as the model because of their better accuracy, faster computation time, can accommodate more training data and also accounts for misclassified points. The Principal Component Analysis (PCA) is also implemented which is a useful supplemental technique for better understanding the relationships between the selected variables.

1. W. Zhou, Z. Lv, X. Deng and Y. Ke, "A New Induced GNSS Spoofing Detection Method Based on Weighted Second-Order Central Moment," in IEEE Sensors Journal, vol. 22, no. 12, pp. 12064-12078, 15 June15, 2022, doi: 10.1109/JSEN.2022.3174019.

SQM - Signal Quality Monitoring: it uses the output signals and detects any distortions or abnormalities . based on this principle, the authors use the Weighted Second Order Central Moment (WSCM) that basically tracks the signals and identifies GPS Spoofing if it finds distortion in symmetry of the receiver by correlating the time-domain signals. The main advantage of this method is that the alert time is shortened which is of paramount importance to prevent an emergency situation. Moreover, it is extremely accurate.

1. L. Xiao, X. Li and G. Wang, "GNSS Spoofing Detection Using Pseudo-range Double Differences between Two Receivers," 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2019, pp. 498-502, doi: 10.1109/ICCSNT47585.2019.8962453.

This paper advocates using 2 receivers and analyzes differences in measurements of the Position, Velocity and Time Services of GNSS and the estimated predictions. Accordingly, the Spoofing is detected. This model is very accurate and if the baseline is 10m long and false alarm rate = 0.001, the detection probability reaches 99.99%. Moreover, it also incorporates the case where spoofing signals are sent from multiple sources and not only a single source.

1. J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing", *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45-57, 2015.

They suggested using phase-delay measurement in the many antennas installed. Based on the quality received at each antenna, they are then compared.

1. S. Malik, P. Bandi and W. Sun, "An Experimental Study of Denial of Service Attack Against Platoon of Smart Vehicles," 2021 Fourth International Conference on Connected and Autonomous Driving (MetroCAD), Detroit, MI, USA, 2021, pp. 23-30, doi: 10.1109/MetroCAD51599.2021.00013.
2. <https://www.sciencedirect.com/science/article/pii/S1570870518309260>
3. S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang and W. Shi, "Edge Computing for Autonomous Driving: Opportunities and Challenges," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1697-1716, Aug. 2019, doi: 10.1109/JPROC.2019.2915983.
4. <https://ieeexplore.ieee.org/abstract/document/9625017>
5. \Bias Estimation Range Check
6. Velocities Consistency Check
7. Statistical Test
8. Global Navigation Satellite System Augmentation
9. Least absolute shrinkage and selection operator

## 8. (Electronic Control Unit) ECU’s Software Flashing Attacks

X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6240-6259, July 2022, doi: 10.1109/TITS.2021.3085297.

ECUs are the embedded systems, which can control gear shift, servosteering, ignition system, electronic window lift, climate controls, etc. In addition, ECUs are reprogrammable, which is helpful for correcting bugs and integrating new functionalities without replacing ECUs. ECU software flashing includes the development, delivery, and installation of software. However, possible attacks on ECU software flashing [31] include reverse engineering, code modification, fuzzing attacks [32], and phlashing attacks [33]. Reverse engineering may disclose information. Code modification may corrupt information and degrade hardware performance. Fuzzing attacks can find vulnerabilities in the embedded systems. Phlashing attacks can trick a remote device into allowing you to flash its firmware. Hence, the machine can never be rebooted. It must be pulled out and replaced. Phlashing attacks may use unpatched vulnerabilities in the embedded systems to gain access.

### SOLUTIONS:

1. M. S. U. Alam, S. Iqbal, M. Zulkernine and C. Liem, "Securing Vehicle ECU Communications and Stored Data," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8762043.

Encryption

They advocate the utilization of “symmetric key cryptography and elliptic curve-based Public Key Encryption (PKE)” to provide confidentiality, and that digital signatures be used to ensure integrity and authenticity. Furthermore, they also use a Blockchain inspired approach to secure the data held in ECU's and prevent it from getting modified, because as we know, Blockchain is immutable, secure and safe. Thus, the cryptography algorithm ensures data is encrypted while the blockchain solution ensures that data is stored safely and correctly.

1. Authentication
2. Integrity Check

In order to defend ECUs software flashing attacks, there are some strategies, including encryption [80], authentication [81], and integrity check.

Reverse engineering may destroy the confidentiality of ECU data, ECU data should be encrypted [80]. Therefore, the adversary cannot read them. Authentication [81] can identify the origin of the software correctly. Integrity [125] is important for preventing software modification by unauthorized users. Hence, every ECU should check the integrity. Nonrepudiation is helpful for tracking the software version that has been installed, installation time, and who installed the software. Then, the adversary is difficult to implement malicious software flashing.

## 9. Location Trailing Attacks

X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6240-6259, July 2022, doi: 10.1109/TITS.2021.3085297.

In location trailing attacks, the adversary can obtain drivers’ private information through locating and tracking their vehicles. With the help of location information, the adversary can discover behaviors and activities of vehicles, even obtain the profile of the driver and match to personal privacy in the real world. These attacks may damage to the transportation-based cyber-physical systems, for example, the increasing number of congested roads.

In order to protect the privacy, messages are anonymously transmitted. In addition, pseudonyms are changed frequently. However, it has been proved that a single pseudonym is not sufficient to resist location trailing attacks [25]. Specifically, pseudonymous position samples can be collected and combined into pseudonymous location profiles. Then, an adversary can easily relate them to specific vehicles. For example, profiles, which include the same starting/ending location on weekday mornings, may reveal home and work addresses

### SOLUTIONS:

1. S. Jeong, M. Kim and J. Lee, "CUSUM-based GNSS spoofing detection method for users of GNSS augmentation system", *Int. J. Aeronaut. Space Sci.*, vol. 21, no. 2, pp. 513-523, Jun. 2020.

K-anonymity - it provides data privacy by generalizing and hiding attributes. The user’s location is hidden in k-1 locations and thus, it increases privacy but decreases the speed of response time. The major advantage of this approach is that because of the private blockchain nodes, the Location Service Provider can now no longer directly access the user’s location and hence, it ensures privacy. Hence, now no 3rd-party trusted servers are also required. Thus, the user gets best, accurate features based on his/her location without compromising privacy.

1. Mix-zone

Y. Zhou and D. Zhang, "Double mix-zone for location privacy in VANET", *Proc. 7th Int. Conf. Inf. Technol. IoT Smart City*, pp. 322-327, Dec. 2019.

<https://dl.acm.org.elibrary.nirmauni.ac.in/doi/pdf/10.1145/3377170.3377250>

The correlation of the vehicles entry and exit points in VANET along with the vehicle speed may result in identification of the vehicle’s location. Thus, the paper designed an algorithm - DMix that adds noise to location information and modifies the vehicles’ speed to secure the users’ location. The main disadvantage of this method is that it may cause the phenomenon of overspeeding while readjusting and recalibrating the speed.

1. Software Defined Networks

A. Boualouache, R. Soua and T. Engel, "VPGA: An SDN-based location privacy zones placement scheme for vehicular networks", *Proc. IEEE 38th Int. Perform. Comput. Commun. Conf. (IPCCC)*, pp. 1-8, Oct. 2019.

This paper analyzes optimal “Vehicular Location Privacy Zones” (VLPZ) placement which is an NP-Hard problem and presents a genetic-based approach in a software-defined vehicular network to assure minimal trajectory cost of engaged cars and therefore less use of their pseudonyms. Basically, the Software Defined Networks manage the network dynamically.

1. Perturbation-hidden

X. Li et al., "Perturbation-Hidden: Enhancement of Vehicular Privacy for Location-Based Services in Internet of Vehicles," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 3, pp. 2073-2086, 1 July-Sept. 2021, doi: 10.1109/TNSE.2020.3011607.

This algorithm is more stricter than Geo-Ind wherein if the users’ differential behavior is organized, then the data is leaked.

[BRIJ SOJITRA](mailto:20bce035@nirmauni.ac.in)aa paper ma khabar pade che perturbed etle su?

10. Attack on warning messages

It is essential to make sure that the safety of Vehicle to Vehicle messages, particularly data legitimacy and dependability due to the messages’ nature exchanges in V2V communication (for example, acceleration, velocity, and position) because they are safety-critical. To ensure that the data content’s legality is ambiguous and it is not possible to do it traditionally, although source authenticity message veracity can be guarded by cryptographic means. Harsh effects will include undermining the advantages of V2V communications if false data is received from another car. A dangerous circumstance can occur. For example, crashing accidents from the rear end can occur if, for instance, recent studies [140], [141] prove that in a CACC setting, feeding false data to a wireless conduit can cause a malevolent car to increase or reduce the speed of other vehicles incorrectly. It is imperative to make sure that cars sense and filter data from other motor vehicles, given that a linked car’s decision-making process much depends on the received V2V messages. When drafting a trust framework for secure V2V data authentication, many challenges are present. Cars should be able to detect false messages and approximate the true states in real-time as the attackers may feed incorrect data from another car at any given time. Detection of untruthful data should be done in a manner that is confined and decentralized as a substitute for depending on national infrastructures to gather universal information such as the trusted roadside components. With the number of surrounding vehicles being small and the possibility of collusion, we cannot presuppose a candid, more significant part of the one-hop area of a car.

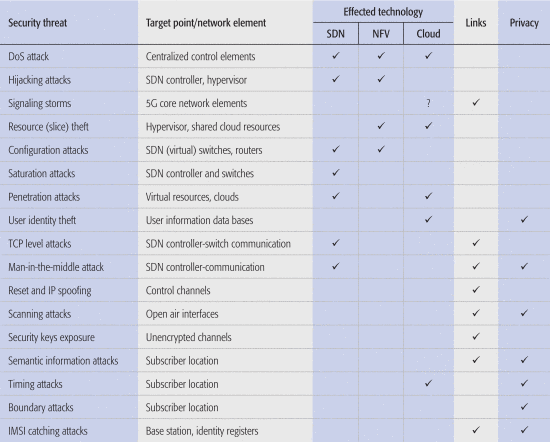
A Mitsubishi Outlander PHEV was hacked, and the investigators of safety at Pentest Partners executed a man in the middle attack to know the one responsible between the PHEV’s cell phone application and the Plug-in Hybrid Electric Vehicle (HEC) Wi-Fi application [118]. They were able to find out the binary protocol that was used for messaging after repeating the different messages from the mobile app. The attackers were able to switch on and off the lights, immobilize the entire burglary alarm system, thus making the car at risk of more attacks.

11. Attack on AU

12. Attack on thruster monitoring unit

A self-driving car’s thrusters, a type of propelling unit acting as actuators, are responsible for the faults or failures associated with different types of motions. The status of thrusters is monitored by a special unit called the Thruster Monitoring Unit (TMU). If this unit is attacked in a self-driving car, it can result in disturbances in the vehicle’s fault control. The attack eventually takes control of the motion of the car. A selfdriving vehicle will hardly have enough time to notify the driver to control the car in the event of such an attack. Very little research has been conducted on such attacks.

# Telecom sector



## 1. Network jamming attack ( a particular type of DoS attacks)

Paper :- Aggressive jamming attack in IOT networks

An IoT architecture is subject several potential cyber-attacks, one of which is Jamming attacks, where threats can affect performance and hence cause a critical problem for IoT devices. This paper presents several scenarios of a smart jamming attack (coalition attack) mechanism, where the attackers are originally legitimate nodes and form part of a network before they leave it and return as a compromised nodes. In order to intensify the attack, the compromised nodes re-group smartly, share the memorized network information, assign the role of a jammer for each node and subsequently achieve an aggregate jamming effect. Furthermore, the mechanism allows the compromised nodes to select the correct transmission rates for attacking according to an attacking-probability table which is kept updated during the coalition life cycle and contains the most probable link-transmission rate among the network nodes. Simulation results of the presented scenarios using NS3 show that attacks which rely on this mechanism can adversely affect the performance of the network.

According to [W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in Mobile Ad Hoc Networking and Computing, ACM, 2005.], there are 4 main types of Jamming attacks:

1. Constant
2. Reactive
3. Random
4. Intermittent

### SOLUTIONS:

IoT device insecurity can open up a gateway for the entire network to be compromised. Moreover, With its versatility of jamming intervals, the attacker can create network latency and reduce network throughput, resulting in a considerable reduction in network performance. Hence, it is necessary to secure IoT devices from Network Jamming Attacks.

1. Z. Liu, H. Liu, W. Xu and Y. Chen, "Exploiting jamming-caused neighbor changes for jammer localization", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 547-555, 2012.

The authors present a method that uses a least squares-based localization technique to find the jammed device by detecting changes in the hearing range of the nearest nodes. However, they necessitate more signal power, resulting in higher overhead.

1. G. Thamilarasu and R. Sridhar, "Game theoretic modeling of jamming attacks in ad hoc networks", *Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1-6, 2009.

The authors introduced a game theoretic framework for detecting jamming assaults in wireless ad hoc networks in this research. To evaluate the interaction between the attacker and the network monitoring nodes, they represented jamming as a two-player, non-cooperative game and developed hybrid detection algorithms for attack detection at the monitor node by incorporating cross-layer characteristics. However, the main disadvantage of this approach is when the attacker communicates at high power and high bandwidth, then the proposed model fails to mitigate Jamming.

1. Handling the jamming attacks has 2 main phases: “Detection” and “Mitigation”. Automatic Detection involves using Machine learning and Deep-Learning techniques to train the IoT device by itself on identifying possible attacks. One such approach is “Detecting and Mitigating Jamming Attacks in IoT Networks Using Self-Adaptation”

The authors propose DeMiJA, - “Detection and Mitigation of Jamming Attacks in IoT” as a potential solution. It follows the “MAPE-K” model and is simulated on the Delta-IoT System. They trained 2 models, namely Deep AnT and ARIMA that uses Computer Vision and Auto regression respectively to predict the next value based on historical data. Next, they normalize the score and if it exceeds the threshold, it is marked as suspicious and appropriate mitigation steps are followed. 1 major requirement includes that there has to be historical data available for the model to train on. However, the main disadvantage of this approach is it excludes the jamming attacks that target the gateway.

1. H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” IEEE Communications Surveys & Tutorials, 2022.

It gives a comprehensive survey of the Jamming attacks and explores the various solutions proposed. It covers each sector, namely: WLAN’s, Cellular Networks, Cognitive Radio Networks (CRN’s), Zigbee networks, RFID, GPS System and Vehicular Networks, specifically the UAVs and VANET’s.

1. B. Upadhyaya, S. Sun and B. Sikdar, "Machine Learning-based Jamming Detection in Wireless IoT Networks," 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Singapore, 2019, pp. 1-5, doi: 10.1109/VTS-APWCS.2019.8851633.

A similar approach is used by the authors of this paper. The only overhead expense involved is placing the anchor nodes inside the network that measures the transmitting signals’ power at regular intervals and based on the historical data, if any suspicious entry is identified, it is flagged and appropriate mitigation strategies are adopted. It gives a relatively high accuracy of 89.7% on real data!

1. M. R. Manesh, M. S. Velashani, E. Ghribi and N. Kaabouch, "Performance Comparison of Machine Learning Algorithms in Detecting Jamming Attacks on ADS-B Devices," 2019 IEEE International Conference on Electro Information Technology (EIT), Brookings, SD, USA, 2019, pp. 200-206, doi: 10.1109/EIT.2019.8833789.

The authors of this paper experiment with all different Machine Learning and Neural Network algorithms specifically to prevent Jamming attacks in Aircraft Communication Systems. A 2 layer Neural Network with 15 neurons each performs the best.

1. O. Punal, I. Aktas¸, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, ˜ “Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation,” in International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2014.

## 2. Interception attack

<https://www.firstpoint-mg.com/blog/top-10-cyber-threats-to-private-5g-lte-networks/>

An interception attack in the telecom sector using IoT refers to a situation where an attacker gains unauthorized access to the communications of IoT devices connected to a telecommunications network. This can be done by intercepting and decoding the signals sent between the devices and the network, or by compromising the devices themselves. The attacker can then use this access to gain sensitive information, disrupt communication, or even take control of the devices. To prevent such attacks, it is important to use strong encryption and authentication methods, as well as regularly update the software and firmware on IoT devices to address any vulnerabilities.

**When these networks are the only point of contact with the outside world, there is considerable risk in the possibility of hackers intercepting and misdirecting communications**. One possible attack vector is service downgrading, forcing devices to connect using slower, less secure communication protocols, thus allowing for easier capture and decryption of data.

The 2 main characteristics of this attack are:

1. Measurable delay
2. Unusual Travel time

### SOLUTIONS:

1. S. Gong, H. Ochiai and H. Esaki, "Scan-Based Self Anomaly Detection: Client-Side Mitigation of Channel-Based Man-in-the-Middle Attacks Against Wi-Fi," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 1498-1503, doi: 10.1109/COMPSAC48688.2020.00-43.

The authors propose a “Scan based Self Anomaly Detection (SSAD)” whose main purpose is to mitigate against channel based Man in the Middle Attacks. While the IoT Devices connect to the Access point to use the WiFi services, there is usually no warning if it is malicious. However, they focus on the concept that no 2 Access points have the same MAC Address and if they find so, they warn the user. The main advantage being this process is computationally light and doesn't require the support of Access Points and thus, can be implemented in the IoT Devices. It gives an excellent accuracy of 99% when the attacker is in the same room as Access point. A future research topic would be to work on finding the location of rogue access points and reporting it.

1. <https://pdfs.semanticscholar.org/03ad/76245da522cf0becd585c1dbe3be2a001da7.pdf>

They suggest using Cryptographic Techniques for Encryption: both Asymmetric and Symmetric Techniques to ensure that the attacker can’t read and understand the message.

M. S. Mehmood, M. R. Shahid, A. Jamil, R. Ashraf, T. Mahmood and A. Mehmood, "A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment," 2019 8th International Conference on Information and Communication Technologies (ICICT), Karachi, Pakistan, 2019, pp. 54-59, doi: 10.1109/ICICT47744.2019.9001945.

However, these authors survey and find that Encryption Algorithms like RSA, advanced encryption standard (AES), data encryption standard (DES) etc are too computationally expensive and have higher complexity hence they are difficult to implement in IoT. Hence, it summarizes light-weight encryption-decryption techniques to improve IoT Security.

1. J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua and P. Haskell-Dowland, "Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks," 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), Auckland, New Zealand, 2019, pp. 1-6, doi: 10.1109/ITNAC46935.2019.9077977.

The paper refers to a hybrid routing protocol wherein secure nodes are introduced to securely route packets between IoT Devices. Being dedicated to security, they are more capable in handling security issues. They find the most secure routes within the network and avoid malicious nodes, which is based on a trust-based ranking algorithm. It works on the delayed time difference in transmission between source and destination and accordingly, classifies routes and nodes as suspicious or safe.

1. C. Li, Z. Qin, E. Novak and Q. Li, "Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1156-1164, Oct. 2017, doi: 10.1109/JIOT.2017.2685596.

Analyzing the vulnerability in the OpenFlow channel, the authors propose a bloom filter. It confirms the existence of an element and thus, when each intermediate node passes the bloom filter, we can identify the node that has different parameters. However, this approach won't work if all the nodes are compromised because then, the attacker can manipulate the filters also.

## 3. Session attack

A session attack in the telecommunications sector using IoT devices refers to a type of cyber attack where an attacker gains unauthorized access to an IoT device and uses it to initiate a session, such as a phone call or data session, on a telecommunications network. This can be done by exploiting vulnerabilities in the IoT device's software or by stealing login credentials. The attacker can then use the compromised device to make calls or send data, potentially incurring charges on the device's owner's account or using the device to launch further attacks on the network. To prevent session attacks, it is important to ensure that IoT devices are properly secured and that vulnerabilities are patched promptly. Additionally, using strong authentication methods, such as two-factor authentication, can help prevent unauthorized access to IoT devices.

### SOLUTION:

1. <https://www.researchgate.net/profile/Arnob-Paul-2/publication/324448404_Survey_of_the_Protection_Mechanisms_to_the_SSL-based_Session_Hijacking_Attacks/links/6022f588299bf1cc26b5462d/Survey-of-the-Protection-Mechanisms-to-the-SSL-based-Session-Hijacking-Attacks.pdf>

The web was 1st designed based on the HTTP Protocol. However, because of the session stealing attacks, HTTPS was introduced which is based on HTTP+SSL where SSL provides a secure communication medium. Most of the session stealing attacks happen when instead of HTTPS, users enter sensitive information on HTTP pages which can be accessed by hackers. Hence, browsers should always show a warning when going to sites where security certificate is not trusted!

1. <https://dl.acm.org/doi/pdf/10.1145/2220352.2220353>

This paper proposes using One Time Cookies (OTC) wherein Instead of utilizing a single, static token to authenticate each request, OTC produces a unique token based on a session key for each request generated by the user. Because each OTC token is associated with a specific request through a hash-based message authentication code (HMAC), an attacker cannot utilize OTC tokens to illicitly redirect a session. The main advantage is the need of the single static cookie is eliminated! Gmail uses a related concept where the cookies change every few seconds so it is impossible to compromise it

1. Other common solutions include never using public WiFi.

## 4. DNS spoofing

<https://www.firstpoint-mg.com/blog/top-10-cyber-threats-to-private-5g-lte-networks/>

DNS spoofing is a type of cyber attack in which an attacker redirects traffic intended for a legitimate domain to a malicious one. In the telecom sector, this could be done by compromising an Internet of Things (IoT) device, such as a smart router, and using it to intercept and redirect DNS requests. This could allow the attacker to redirect traffic intended for a legitimate telecom provider to a malicious site, potentially stealing sensitive information or spreading malware. To prevent this type of attack, it is important to keep IoT devices updated with the latest security patches, and to use a DNS security solution that can detect and block malicious DNS requests.

A hacker that has gained access to a private network via IMSI impersonation (or some other method) can launch DNS spoofing attacks on that network. MiTM (Man-in-the-Middle) based, this attack can allow bad actors to **change the IP address of the requested DNS server**. **Said bad actors can then redirect domain requests to resolve malicious sites under their own control**.

One example where this type of attack could be incredibly harmful is in [school districts](https://www.fiercewireless.com/private-wireless/cbrs-private-network-put-to-test-by-utah-school-district) where private networks are used for remote learning. **Cybercriminals could use DNS spoofing to display unwanted content to students by redirecting the traffic from educational portals and virtual classroom links**.

A common tool to perform DNS Spoofing attack is Ettercap.

SOLUTION:

1. A. Dua, V. Tyagi, N. Patel and B. Mehtre, "IISR: A Secure Router for IoT Networks," 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2019, pp. 636-643, doi: 10.1109/ISCON47742.2019.9036313.

They suggest using data exchange techniques that are encrypted. End-to-end encryption with SSL/TLS ensures secure communication and reduces the likelihood that a website or its visitors may be compromised by DNS spoofing. It enables users to determine if the server's digital certificate is legitimate and belongs to the anticipated owner of the website. Users can also use Domain Name System Security Extensions (DNSSEC) to assist evaluate data authenticity by using digitally signed DNS entries.

1. R. Nagai, W. Kurihara, S. Higuchi and T. Hirotsu, "Design and implementation of an openflow-based tcp syn flood mitigation", *2018 6th IEEE International Conference on Mobile Cloud Computing Services and Engineering (MobileCloud)*, pp. 37-42, March 2018.

One of the main techniques of attacking through DDoS is multiple TCP syn requests. This paper advocates sending wrong SYN+ACK reply to the client. Either the client will reply to the wrong message or ignore it, in both ways, keeping the load on the server safe.

1. H. Mohammadnia and S. B. Slimane, "IoT-NETZ: Practical Spoofing Attack Mitigation Approach in SDWN Network," 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 2020, pp. 5-13, doi: 10.1109/SDS49854.2020.9143903.

IoT-NETZ - was built by the authors on the concept of Floodshield. It helps in flow control by using the DHCP protocol. It uses a spoofing detection algorithm to identify the origin of the incoming packets. Accordingly, the flow can be controlled, malicious network traffic can also be identified and removed. It also involves source validity.

1. <https://arxiv.org/pdf/2008.09339.pdf>

This paper has a detailed survey on the various Anomaly based and Signature based DoS attacks mitigation and highlights the noteworthy features and vulnerabilities too.

## 5. Battery drain

<https://www.firstpoint-mg.com/blog/top-10-cyber-threats-to-private-5g-lte-networks/>

A battery drain attack in the telecom sector using IoT devices involves an attacker finding a way to exploit vulnerabilities in these devices to cause them to consume more power than they normally would. This can be done by causing the device to continuously perform resource-intensive tasks, such as running a large number of processes or sending a large amount of data.

In the context of the telecom sector, this type of attack could be used to disrupt the network by causing a large number of IoT devices to run out of battery power. This could cause a cascade effect where other devices in the network are also affected, leading to a wider disruption of service.

To prevent this type of attack, it is important to keep IoT devices updated with the latest security patches and to use strong authentication mechanisms to prevent unauthorized access to the devices. Additionally, it is important to monitor the power usage of IoT devices to detect any abnormal behavior.

Also, it is important to have a robust infrastructure in place that can detect and respond to such an attack quickly.

Another type of [man-in-the-middle attack](https://www.firstpoint-mg.com/blog/how-to-prevent-man-in-the-middle-attacks/) can **send signals that cause device batteries to drain rapidly**. These attacks can have **serious, even life-threatening consequences when used against networks that are used to maintain critical IoT devices**.

One such example is a private cellular network used by the [mining company Newcrest](https://enterpriseiotinsights.com/20190704/channels/news/telstra-turns-on-private-lte-for-newcrest) to make their equipment operate more safely and efficiently. In that scenario, it could be dangerous for a **remote sensor to lose battery power unexpectedly, as replacing the battery could be a hazardous and complex operation in itself**.

### SOLUTIONS:

1. Lee, Il-Gu, Kyungmin Go, and Jung Hoon Lee. "Battery draining attack and defense against power saving wireless LAN devices." *Sensors* 20.7 (2020): 2043.

The authors propose an Intrusion Detection System that has 2 main components, 1) IDS Routers whose main function is efficient routing and managing the firewall, and 2) IDS detectors - who monitor the communications to and from the network. Characteristics of nodes like packet sending rate, packet dropping rate, interval between 2 packets are used to help classify malicious nodes during detection.

1. C. Gehrmann, M. Tiloca and R. Höglund, "SMACK: Short message authentication check against battery exhaustion in the Internet of Things," 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Seattle, WA, USA, 2015, pp. 274-282, doi: 10.1109/SAHCN.2015.7338326.

The authors came up with SMACK - “Short and lightweight Message Authentication Code“ that analyzes each received message and eliminates the invalid messages, particularly sent during DoS attacks which also drain the battery. Thus, as the packet itself is eliminated, future effort is saved and saves battery life. The authors claim that it is efficient and suitable for IoT applications and has good computational power, consumes less energy etc.

1. Z. Guo, I. G. Harris, Yutong Jiang and L. -f. Tsaur, "An efficient approach to prevent Battery Exhaustion Attack on BLE-based mesh networks," 2017 International Conference on Computing, Networking and Communications (ICNC), Silicon Valley, CA, USA, 2017, pp. 1-5, doi: 10.1109/ICCNC.2017.7876092.

Bluetooth Low Energy (BLE) is an energy efficient version of bluetooth used for IoT devices for communication. Their solution is very effective in controlling the effect because they work on 2 aspects:

* If a suspicious activity is detected, the nodes are blacklisted and not allowed to enter the network. However, in case a malicious node is not detected, still the power consumption will be distributed across the network.
* It also uses a mechanism like token ring (Wherein each sender gets to send a packet when he/she has the token and then, has to wait till next time token comes), a priority list of the requests of all the nodes is maintained and once the request is fulfilled, the priority is lowered. Moreover, the request is fulfilled only if the requests rate is below the threshold.

6. Mobile identity capture → sub-part of MNMap

It’s not difficult for hackers to intercept cellular signals and infer the identities of the devices sending and receiving them. This process of capturing identities can be the starting point for MNmapping and other attacks, but it can be a big enough problem in itself in certain contexts.

When [health and social welfare systems](https://liverpool5g.org.uk/wp-content/uploads/2020/04/how_can_5G_support_transformation_health_social_care_services.pdf) are using private 5G networks to provide services, **mobile identity capture can endanger the privacy and safety of patients**.

7. MNmap

Wireless data-sniffing devices can use identifying data sent over cellular signals to determine what types of devices are connected to the network. This is known as an [MNmap attack or device fingerprinting](https://threatpost.com/5g-security-flaw-mitm-targeted-attacks/147073/). It can **give bad actors access to sensitive information about the devices within a private network and their capabilities**.

At [the port of Antwerp](https://enterpriseiotinsights.com/20200207/5g/proximus-deploy-private-5g-network-belgium-port-antwerpen), private 5G networks are used to streamline communications between tugboats, inspectors, and security services. In such a scenario it would be essential to eliminate any gaps in mobile networking mapping protocols that could be exploited by bad actors looking to conceal physical crimes committed. For example, **illegal trafficking operations that wish to evade detection would want to discover where cellular security cameras are located around the port**.

## 8. Deauthentication Attack

<https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9036313>

H. Xu, D. Sgandurra, K. Mayes, P. Li and R. Wang, "Analysing the resilience of the internet of things against physical and proximity attacks", *International Conference on Security Privacy and Anonymity in Computation Communication and Storage*, pp. 291-301, 2017.

It is a very basic attack wherein the attacker can disconnect the user from the Wireless Access Point.

### SOLUTION:

The authors of <https://ieeexplore.ieee.org.elibrary.nirmauni.ac.in/document/9036313> identify Deauthentication attack with a packet sniffer, which was built by configuring an ESP8266 Wifi Module in monitor mode with the Arduino IDE. They are able to successfully detect and stop both the Deauthentication and Fake Authentication attacks.

Aa rehva deje delete nai karto

Autonomous vehicle

1. Malware attack -

2. MITM attack

3. DOS attack -

4. Ransomware attack -

5. Sybil -

6. Spoofing attack

7. Attack on IMU(inertial measurement unit)

8. Attack on LIDAR

9. Attack on GPS

10. Attack on warning messages

11. Attack on AU

12. Attack on thruster monitoring unit

Telecom sector

1. Network jamming attack

2. Interception attack

3. Session attack

Smart Home

1. Data & identity theft

Data theft means when someone steals data or your personal information and identity theft means using your identity and your personal data the hacker do anything which could be unlawful and all the blame will be on yours.

In smart home segment the data generated by unprotected wearables and smart appliances are the prime target which are having ample amount of targeted personal information, which can be exploited for identity theft.

2. Device hijacking

When a device is hijacked for the purpose of carrying out fraud. This is called device hijacking.

In this the attacker does not change the basic functionality the main motive is to infect all smart devices in the home, because of which it is very difficult to detect.

Through this attack the attacker can remotely access the entire network of your home and can for example remotely unlock your door or can change the PIN code for entry, change attack your smart appliance which could damage its battery and many other things could be done.

3. Eavesdropping attack

Eavesdropping is a type of sniffing or snooping attack, in which the theft of information is transmitted over a network by a computer. The hacker takes advantage of unsecured network communications to access data as it is being sent or received by its user.

By launching this attack hacker can able to see all the messages sent or received by the user. In the smart home domain for example if the person enters the home by entering the password PIN then the hacker can see that password if the network is hacked.

4. DDOS

<https://securityboulevard.com/2022/08/prevent-ddos-attacks-with-proper-cybersecurity/>

In a DDOS or distributed denial of service attack, the hacker tries to flood the server with a lot of traffic so that it could not respond to the request at a time. Thus, this makes a site slow or even crash so that authentic users won’t be able to access that website.

The majority of the DDOS attack has been with botnets, this are the group of computers which all together will try to access website which would increase the load on the server and can be bring it down.

The DDOS attack can be done on the any of the smart appliance in house and make them damage permanent or can use the smart appliance as the botnet to attack others.

For example, the hacker can make multiple requests to the smart bulb to turn on and off at the same time because of which bulb might get damaged.

5. Mirai botnets (more optimization needed)

<https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>

<https://www.coursehero.com/file/185088874/21040604-Asmita-KCAssignment-1pdf/>

<https://www.chegg.com/homework-help/questions-and-answers/essay-help-research-high-profile-ddos-attacks-carried-using-mirai-botnet-major-focus-dyn-d-q95824534>

<https://www.govtechleaders.com/2019/05/07/regulatory-proposal-on-mandatory-iot-security-label/>

<https://heimdalsecurity.com/blog/smart-home-vulnerable-hacking/>

Mirai botnet is a type of botnet attack where it hijack large number of IOT devices and spread further using that infected node. Mirai infects smart devices which runs on ARC processors, turning them into a network of bots or zombies. Mirai targets IOT devices that run on ARC processor because this processor works on stripped down version of the LINUX OS, so if default username and password is not changed then mirai can infect that device. This network of bots is called botnet and is often used for the DOS attack.

Here are some of the latest examples of mirai botnet attack. In February 2017 when smart toy manufactured by spiral toys were hacked leaving personal information get exposed using voice recording. More than 8,00,000 users data was comprimised

After a computer got infected with Mirai, it continuously searched the internet for vulnerable IoT devices and used default usernames and passwords to log in, infecting them with malware. In the October 2016 attack, it was estimated that 100,000 endpoints were affected. This information was available over online database which could be easily access by anyone.

Another such incidence took place in 2019, when a homeowner reported that is smart cameras and thermostat has been hacked.

6. Jamming (more optimization needed)

<https://www.thesecuritybuddy.com/wireless-network-and-security/what-is-jamming-attack-and-how-to-prevent-it/>

<https://quizlet.com/709992188/14-given-a-scenario-analyze-potential-indicators-associated-with-network-attacks-flash-cards/>

<https://mmupcz.matcars.de/page/imdt>

In this attack the hacker transmit inference signal over the wireless networks intentionally because of which user won’t be able to the device to the network. This interference signal keeps the medium busy as device sense medium is busy it stops communicating.

Because of this signal to noise ratio gets at reciver gets lower which leads to disruption in existing wireless communication.

For example in this attack, the hacker does the jamming attack so that you can’t control your smart home appliances remotely because your actual signal is not able to reach the appliance because of this attack.

<https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>

<https://www.oracle.com/in/internet-of-things/what-is-iot/>

<https://www.analyticssteps.com/blogs/9-applications-iot-home-automation>

<https://ordr.net/article/iot-healthcare-examples/#:~:text=IoT%20devices%20can%20automatically%20collect,patients%20to%20collect%20it%20themselves>.

Background

In this paper we are going to talk about IOT and its applications. IOT stands for internet of things. The IOT technology consist of physical devices which are connected over the network, which means that the physical objects like light, fans, etc are embedded with the software, sensor or other technologies for the purpose of exchanging data or connecting with the other devices without any human to human or human to computer interactions. IOT has been popular nowadays just because of its access to low cost, low power sensor technology, machine learning and analytics, cloud computing platforms and connectivity. From past few years IOT has made the human life much more simple for example just by speaking the about the things alexa does all the things get done like light turn on & off, to search songs on speaker, etc.

The Internet of Things (IoT) ecosystem is made up of internet smart devices that incorporate embedded systems, like processors, sensors, and communication gear, to gather, send, and act on the data they get from their surroundings. By connecting to an IoT gateway or other edge device, which either sends data to the cloud for analysis or analyses it locally, IoT devices exchange the sensor data they collect. These gadgets converse with other similar devices on occasion, acting on the data they exchange. Although individuals can engage with the devices to start them up, give them instructions, or retrieve the data, the gadgets accomplish the majority of the job without their help.

IOT is usefull in day to day life and also usefull for the big MNC’s as well. Businesses may automate procedures and save money on labour thanks to IoT. Additionally, it reduces waste, enhances service delivery, lowers the cost of manufacturing and delivering items, and provides transparency into customer transactions.

There several protocols different from the normal protocols different from the normal protocols in the IOT ecosystem network. This protocols are :-

1. Zigbee

<https://www.techtarget.com/iotagenda/definition/ZigBee#:~:text=Zigbee%20is%20a%20standards%2Dbased,and%20is%20an%20open%20standard>.

Zigbee protocol is built for sensor and control networks for WPANs on the IEEE 802.15.4 wireless standard. This protocol is used for the low data rate, low power applications and is an open standards. Theoretically, this permits the mixing of implementations from many manufacturers, but in practise, Zigbee products have undergone vendor extensions and customizations that cause interoperability problems. Zigbee networks accept far lower data rates and use a mesh networking protocol to avoid hub devices and produce a self-healing architecture, in contrast to Wi-Fi networks, which are used to connect endpoints to high-speed networks.

2. LiteOS

<https://iotbyhvm.ooo/what-is-liteos/>

LiteOS is an IOT middleware and operating system. It acts like an operating system for IOT smart terminals. IoT terminals can swiftly connect to the network thanks to LiteOS. It will simplify the creation of intelligent hardware. thus hastening the understanding of everything's interconnectedness. It offers a consistent open-source API that may be applied to a variety of IoT applications, including smart homes, Internet of Vehicles(IOV),intelligent manufacturing wearable technology, and . It makes it possible for an open Iot infrastructure, assisting partners in hastening the creation of IoT goods.

3. OneM2M

<https://www.onem2m.org/using-onem2m/what-is-onem2m#:~:text=oneM2M%20brings%20together%20all%20components,communications%20networks%20and%20IoT%20applications>.

OneM2M is used to increase the reusability of existing technology components and standards. OneM2M’s structure acts as a middleware technology in a horizontal layer between IOT applications and devices and communication networks. Links between connected devices, gateways, communications networks, and cloud infrastructure are standardised as a result, d evelopers can combine and match modules from various vendors. OneM2M is a universal standard that may be used across all business sectors. This guarantees a high rate of reuse. Vertical applications can now communicate with one another, which is another benefit. Working beyond application silos fosters creativity and delivers tremendous value.

4. AMQP

<https://iotboys.com/what-is-amqp-how-amqp-works-for-internet-of-things>

Full form of AMQP is Advance Message Queuing Protocol. AMQP is an open protocol for asynchronous message queuing that has undergone extensive development and maturation. AMQP is a binary application layer protocol with open standards and was created for message oriented middleware. Let's look at how AMQP interacts with publishers and customers. The message is created by the publishers, and the consumer takes it in and processes it. Making sure that messages from publishers reach the appropriate recipients is the responsibility of the message broker (like RabbitMQ).

The broker needs two essential elements to accomplish that:

1.Exchanges

2.Queues.

5. CoAP

<https://www.wallarm.com/what/coap-protocol-definition#:~:text=CoAP%20a%20customary%20client%2Dserver,interact%20over%20through%20CoAP%20only>.

CoAP protocol client-server customizable protocol. It helps the device nodes in the IOT ecosystem to interact over through CoAP only. A common client-server IoT protocol is CoAP. It enables customers to submit requests for online transfers as needed. However, it also enabled assisting servers to reply to incoming requests. In conclusion, the IoT ecosystem's device nodes can only communicate via CoAP. HTTP and CoAP both operate in the same way. However, asynchronous transactions allow CoAP to function (using UDP). The GET, POST, DELETE and PUT calls are used. Because CoAP is an PSK and RPK-certified protocol, API security is enhanced while CoAP is active for this reason.

6. LoRaWAN

<https://docs.aws.amazon.com/iot/latest/developerguide/connect-iot-lorawan-what-is-lorawan.html>

The LoRaWAN protocol works on the LoRa. LoRa is a wireless radio frequency technology that works on license free radio frequency spectrum. The LoRaWAN protocol is a low power wide area networking communication protocol. LoRa is a physical layer technology that provides long-distance communication at the expense of a small bandwidth. It uses spread spectrum modulation. It is resistant to interference since it sends data using a narrow band waveform with a core frequency.

SMART HOME

<https://www.constellation.com/energy-101/what-is-a-smart-home.html#:~:text=A%20smart%20home%20means%20your,and%20is%20typically%20remotely%20controlled>.

Smart home means your home has a system that connects with your devices to access them remotely and automate specific task remotely. IOT can be used to control various mechanism which are utilizing various control system approaches to regulate electrical and electronic equipment in the house like light, fans, fire alarms, etc.

The applications of the smart homes are :-

1. Lighting

The lights might be programmed to dim automatically as people start viewing a movie so they don't get distracted from the plot. The system might automatically turn down the lights when you leave your home to conserve energy so that you don't have to.

2. Gardens

For those who desire to grow their own vegetables, fruit, and herbs at home, sensors may be quite helpful. Users may check the app to determine the proper temperature, whether the plant is getting enough water, and whether it is getting enough sunlight.

3. Security systems

These devices can lock the door, close the shutters, turn off the electronics, and make sure your home is secure from both human and animal intruders when you leave.

4. Kitchen

Using AI technologies, IoT devices can make cooking safer and simpler. To make sure everything is in working condition, smart sensors can keep an eye out for smoke and carbon monoxide as well as the temperature and humidity levels in your kitchen. Special built-in programmes monitor the user's food supply in the refrigerator (and restock it if necessary), provide recipe recommendations, and evaluate the nutritional value of meals. For instance, intelligent spoons encourage users to eat slowly.

HEALTHCARE

IOT enable devices has created an revolution in the healthcare sector. It has made the doctors help to monitor their patients and unleashing the potential to keep patients safe and healthy.

The applications of healthcare are :-

<https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/#:~:text=IoT%20has%20applications%20in%20healthcare,rate%20monitoring%20cuffs%2C%20glucometer%20etc>.

1. Remote patient monitoring

IoT devices can automatically gather health data from patients who are not physically present in a healthcare institution, removing the need for patients to travel to the providers or for patients to collect it themselves. These metrics include heart rate, blood pressure, temperature, and more.

2. Tracking hospital equipments

There are numerous other applications for IoT devices in hospitals besides patient health monitoring. The real-time position of medical equipment like nebulizers, wheelchairs, defibrillators, oxygen pumps, and other monitoring equipment is tracked using IoT devices tagged with sensors. Real-time analysis can also be done of the placement of medical personnel at various sites.

3. Health insurance companies

With IoT-connected intelligent devices, health insurers have a lot of options. Health monitoring device data can be used by insurance companies' underwriting and claims departments. They will be able to identify candidates for underwriting and discover fraud claims thanks to this data. In the underwriting, pricing, claims-handling, and risk assessment procedures, IoT devices increase transparency between insurance companies and their clients.

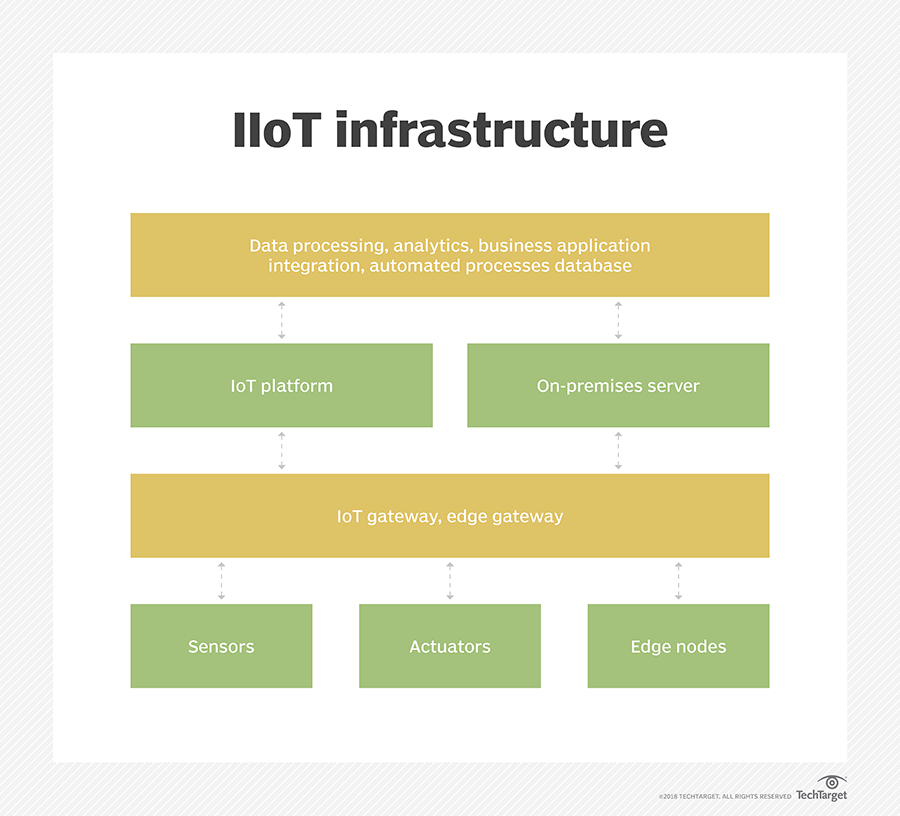
[BRIJ SOJITRA](mailto:20bce035@nirmauni.ac.in)→ all examples reference

5 applications for each sector

Protocols → about 6 lines each

IIoT stands for the Industrial Internet of Things. Initially, the IoT devices were made for the convenience and ease of the end consumers. However, the use of IoT devices in Industries brought about the Industrial Revolution 4.0 and completely revolutionized the Industries. Using IoT devices to enhance manufacturing and industrial processes was very advantageous:

1. Regularly track and monitor the performance
2. Improved productivity because of automation
3. Digitized process thus reducing human error
4. Predictive maintenance based on the Machine’s performance
5. Make better decisions by analyzing data
6. Improved asset tracking



the infrastructure of IIoT [<https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT>]

Few applications where it is used include

1. Smart Waste Collection and Management - There are IoT devices across the city attached to the dustbin and they send an alarm when they are full, and the trash collection van can thus optimize the route to use the least fuel. [<https://iopscience.iop.org/article/10.1088/1757-899X/590/1/012020/pdf>]

2. Process Automation - in industries, the IoT devices are used to monitor the production process and they are capable of adjusting the parameters to improve the efficiency. This is specifically used by robots to tune the machine to its best efficiency. Airbus has incorporated IoT sensors into machines and tools in the factory and the employees wear industrial smart glasses that help in cutting down on errors and enhance work space safety. [<https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT>]

3. Predictive Maintenance - The question of when to service a machine is very important considering the industrial perspective wherein we want to maximize our output. If we service too early, we are wasting resources, if we service too late, the efficiency decreases. Using IoT sensors in machines solves the problem by continuously collecting data and using Data Analytics and Machine Learning to accurately predict when the machine will need maintenance. [<https://terralogic.com/iot-and-how-iiot-became-so-important>]

4. Supply Chains - IoT devices are used in fleet management and supply chain to efficiently track the movement of goods and vehicles and optimize it. Moreover, the IoT sensors in storerooms automatically adjust the weather conditions inside to ensure the stored goods don't degrade.

5. Energy and Grid Optimization - it is useful for the energy companies to monitor daily usage and accordingly track and analyze metrics to ensure energy optimization and load balancing. It can also be used by the industries to monitor their own power load and energy utilization to optimize it. [<https://www.businessofapps.com/insights/sensibly-optimizing-energy-consumption-with-iiot-in-2022> ]

The challenges faced by the IIoT sector includes:

1. Security - in spite of many advantages of IoT devices to be used in Industries, if not secured properly, they can lead to unwanted consequences. It is easier for attackers to hack into IoT devices and if they manage to change the inter-communication between IoT devices and sensors, it can even damage the machine. 2 main challenges include that no encryption techniques are being used and thus, the data is available as plaintext to attackers. Moreover, the industries tend to keep simpler passwords and don't regularly update these devices, thus making it an easy target.

2. Latency and Data Throughput - It is an important factor to consider because even a small delay can lead to disastrous consequences and losses in millions. However, with the advent of 5G Technology, this challenge has decreased.

3. Data Management - with the amount of data being generated daily, it is imperative to make efficient data management systems to ensure proper functioning and optimization of the machines.

4. Interoperability - there are several devices that make IIoT - IoT, sensors, actuators, machines, gateways, cloud. WiFi etc. Integration between these different devices and sensors is complex because they are made by different vendors and there is no standardization. [<https://www.sciencedirect.com/science/article/pii/S0045790618329550>]

The commonly used protocols of IIoT:

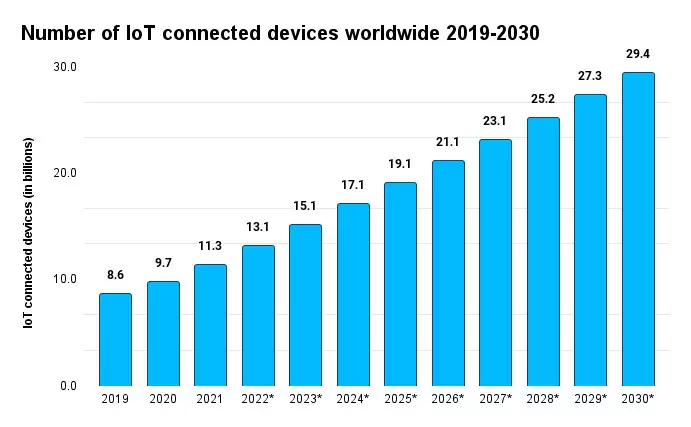
MQTT (Message Queue Telemetry Transport): This is a lightweight, publish/subscribe protocol that is widely used in IoT applications due to its simplicity and efficiency. It is ideal for applications that require low-bandwidth, low-latency communication and is commonly used in IIoT for machine-to-machine (M2M) communication.

CoAP (Constrained Application Protocol): This is a lightweight protocol designed for IoT applications that have limited resources such as memory and processing power. It is designed for efficient use of network bandwidth and is commonly used in IIoT for sensor networks.

DDS (Data Distribution Service): This is a publish/subscribe protocol designed for real-time, high-performance systems such as control and automation systems. It is widely used in IIoT for industrial control and automation applications.

Modbus: This is a simple and widely-used industrial communication protocol that allows industrial devices to communicate with each other. It is commonly used in IIoT for process control and monitoring applications.

OPC UA (Open Platform Communications Unified Architecture): This is an industrial communication protocol that provides a unified and secure way for devices to communicate with each other. It is commonly used in IIoT for industrial automation and control applications.



TELECOM SECTOR: <https://www.datasciencecentral.com/iot-in-telecommunications-challenges-opportunities-benefits-amp/>

Telecommunications sector is in a symbiotic relationship with the IoT devices. The concept of smart devices that could monitor and automate tasks brought about a huge growth in the telecommunication sector, especially with the launch of 5G communication and research on 6G going on. 5G technology was launched specifically keeping the huge rise of IoT devices in mind - it required low latency and high speed, high bandwidth networks. Also, IoT devices have also contributed to the growth of the Telecom Sector. Some of the use-cases include:

1. Asset Management - Telecom sector provides dashboard services for organizations using IoT that helps in smart management and utilization of resources. Based on the current scenario, there are lucrative opportunities available for Telcos to connect with Government in building Smart Cities, and to collaborate with Individuals to offer a Smart Home Environment.

2. Network Management and Customer Satisfaction: Telcos are using IoT devices and sensors to monitor network performance and usage in real-time, providing valuable insights that can be used to optimize the network and improve service quality. Based on their insights, if congestion is detected, the smart IoT devices can dynamically adjust the network to manage the traffic flow, reduce downtime and latency and provide perfect connectivity to all the customers. Moreover, the insights are also used to optimize the network and optimize resource utilization.

3. Saving Energy - According to the writer of this blog [<https://www.helpwire.app/blog/iot-in-telecom/>], AT&T, a mobile-network based company saved almost 9M KWh in 2017 by IoT sensors enabled smart building management and energy optimization. This resulted in savings of almost 1 million USD.

4. Predictive Maintenance - IoT devices help identify issues such as leaky valves or lowered efficiency of the equipment, and are able to forecast when maintenance will be needed thus removing the need of unnecessary maintenance while ensuring to not compromise on performance.

Challenges include:

<https://www.sdxcentral.com/5g/iot/definitions/telecom-using-iot/>

Autonomous Vehicles - Autonomous Vehicles are the cars that are capable of driving itself without the need of human intervention. It has taken the world by storm, especially with the significant usecases like:

1. Traffic Management and Control - with the Vehicle to Infrastructure Communication(V2I), the cars can automatically communicate with the traffic signals and based on the density of vehicles, the traffic signal is operated dynamically to ensure that least fuel is consumed and traffic is managed appropriately. This concept is also known as ecological driving. Moreover, the IoT sensors of Autonomous Vehicles can also be used for Smart Parking - thus it solves 2 major problems of Smart Cities - Parking and Traffic!

2. Improved Safety & Accident Prevention and Response - with the smart IoT sensors along with Vehicle to Vehicle (V2V) Communication, the sensors can sense the speed of vehicles ahead of it and can immediately apply brakes if the car ahead applies brakes. This prevents human error in driving. Moreover, it also ensures the safety of pedestrians and according to a survey by KPMG,, the implementation of Autonomous Vehicles will reduce accidents by 2500 between 2014 and 2030, thus saving several lives..

3. Navigation and Routing - the IoT devices are capable of dynamically re-routing themselves to ensure that the car reaches the destination in the least time. Thus, if there is more traffic at a particular junction, the car will change its route.

4. Predictive Maintenance - The IoT sensors continuously monitor and track the health of the device and it can correctly identify which part of the vehicle needs maintenance and accordingly, money and time can be saved.

5. Infotainment - Here, the IoT devices play an important role with data analytics involved. Based on the user’s preferences and similar users experiences, accordingly new entertainment is recommended to them.

A real life example involves Tesla Autopilot Car which saved its owner by auto-driving straight to the hospital when the owner suffered a blood clot. [<https://www.techrepublic.com/article/how-tesla-autopilot-drove-a-man-with-a-blood-clot-to-the-hospital-and-expanded-the-autonomous-car/>]

Figure showing →. World market forecast for registered vehicles with IoT applications (Source: ABI Research)

Challenges include:

1. Security Issues - it is very challenging and difficult to ensure security and would be very catastrophic. In case of network jamming, the communication between various IoT devices won’t synchronize and thus due to non-integrated readings, the vehicle won’t be capable of driving. Moreover, if communication is hacked, the sensor's data can be modified which may lead to accidents.
2. Latency in Communication - it is critical to ensure that all messages are delivered within the minimum time. In case of huge network traffic, critical messages may not reach timely, thus risking the lives of passengers.
3. Integration with Traditional Cars - it is still unclear how essential communication can be done between autonomous vehicles and the traditional cars.
4. Correctly identifying vehicles - In 2016, a Tesla Autonomous Car couldn’t detect a white trailer crossing the highway on a bright, sunny day which led to a casualty. [<https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk>]. Another case involves wherein an Uber Autonomous Car crashed into and killed a woman who was crossing the street (not at a pedestrian crossing) in Arizona. Although it wasn’t only the vehicle’s fault, it is imperative for the IoT driven AV to take into account all such possibilities.

<https://reader.elsevier.com/reader/sd/pii/S2405896316325162?token=DBA630E331FAB06748D0DB67782BE37E7FD1AAF05C1BB3EE457730382467E1AF3FAFB404C00E0B1E4B826CC9AAB8A9FC&originRegion=eu-west-1&originCreation=20230213030121>

<https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=iot+in+autonomous+vehicles+advantages&btnG=>

<https://ieeexplore.ieee.org/abstract/document/7523574>

<https://erticonetwork.com/self-driving-vehicles-and-iot-services-take-the-stage-in-versailles/#:~:text=IoT%20can%20connect%20all%20types,sensors%2C%20parking%20detectors%2C%20etc>.

<https://www.iotforall.com/iot-and-autonomous-vehicles>

<https://www.naukri.com/learning/articles/application-of-iot-in-teslas-self-driving-cars/>