# Smart Home

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

## 1. Data and 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 does anything that could be unlawful, and all the blame will be on yours.

In the smart home segment, the data generated by unprotected wearables and smart appliances is the prime target, which has an ample amount of targeted personal information that 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, which offers a password-free authentication technique. The FIDO protocol is the first out of two 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 changes the victim's identity to match the attacker's authenticator instead of having the victim's authenticator checked by the UAF protocol service. This lets the attacker get around the UAF protocol's local authentication process and steal the user's identity.

2) 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.

3) Intrusion Detection Systems that use various Mac

4) 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)

2) 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.

3) 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[1]

### 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.

2) 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.

3) 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[2]

<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.

2) 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.

3) <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.

2) 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.

3) 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

4) 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.

5) 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.

6) 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!

7) 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]

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.

4) 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.

3) 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.[4] ”

## 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[5]

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.