**Teaching Aid: Understanding Wireless Security and securing home IoT network.**

**Name: Kaushik Mazumder  
UCID#30267154**

**Introduction**

Today’s technology has evolved to an extent where we have a network interface card on every single device, we use in our day to day lives. In this teaching aide I will focus on home Wi-Fi, wireless security protocols, vulnerability study and securing our home network. With the rise in devices connecting to the internet, the attack vectors have also increased significantly. Moreover, these devices are resource sensitive, which limits the type of encryption security policies that can be implemented on them, making these devices more vulnerable to attacks.

The number of current IoT devices has grown from **10 billion**in 2019 to approximately [8] **18.8 billion** at the end of 2024.

Thanks to 5G and other technologies,[8] this figure is expected to more than double to **41.1 billion** total IoT devices by 2030.

#### ****[8]There will be over 40 billion IoT devices within the next 5 years (****[IoT Analytics](https://iot-analytics.com/number-connected-iot-devices/#:~:text=Number%20of%20connected%20IoT%20devices%20to%20grow%2013%25%20by%20end,by%20the%20end%20of%202024.)****)****

Most IoT devices are connected using wireless, for ease of use and hence its important more than ever to understand the wireless network and its security features.

**Wi-Fi Security Protocols**

In WLANs, privacy is attained by the protection of data content through encryption, though it is optional. If WLANs are implemented without encryption, every standard wireless device can intercept and read all network traffic. Over time, three major generations of security protocols have developed to secure WLANs: WEP, or Wired Equivalent Privacy; WPA, or Wi-Fi Protected Access; and WPA2, or Version 2 Wi-Fi Protected Access. Each protocol offers two versions commonly referred to as "personal" and "enterprise" to offer different approaches suitable to different sizes of networks and different approaches to security.

**Wi-Fi Protected Access (WPA)** – WPA improves on the older standard of WEP by offering two modes of access control. The recommended mode for personal use is WPA PSK, where a 256-bit key is used. WPA enterprise uses a 802.1X radius authentication server to authenticate users connecting to Wi-Fi. To secure the integrity of the data, WPA utilizes the Temporal Key Integrity Protocol, better known as TKIP, which dynamically generates a unique 128-bit key for each packet.

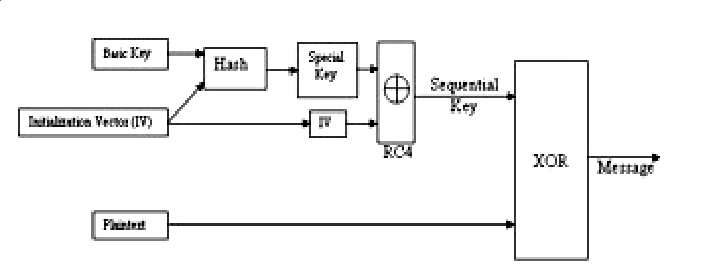


Figure1: WPA Encryptions Algorithm(TKIP)

**Wi-Fi Protected Access (WPA2) -** An improved version of WPA, which is more resistant to attacks. It implements the Advanced Encryption Standard (AES) encryption algorithm very effectively and replaces TKIP with the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).

Before we dive into CCMP process its important to understand what MPDU MAC Protocol Data Unit is, these are frames which contains the MAC header along with a PHY trailer to connect to PHY through radio.

**CCMP Encryption Process**:

* There is an assigned packet number to every MPDU (MAC Protocol Data Unit) that increases with each MPDU.
* MPDU header contains Additional Authentication Data, part of which CCMP uses in deriving integrity.
* PN, MPDU address 2, and Priority field - set to zero, are used in deriving the CCMP nonce; this along with the PN and key identifier forms a 64-bit CCMP header.
* The CCMP nonce, temporal key, AAD and MPDU data produce the cipher and Message Integrity Code.
* MPDU encryption is completed by combining the CCMP header, MPDU header, encrypted data, and MIC from which AAD and nonce values can be read.
* MPDU header is utilized to create the AAD and values such as PN, MPDU address 2 (A2) and Priority fields provide the nonce.
* This would include the combining of AAD, temporal key, MIC, nonce and encrypted MPDU to ensure integrity.

Finally, MAC header and MPDU plaintext are combined to get the original MPDU plaintext.

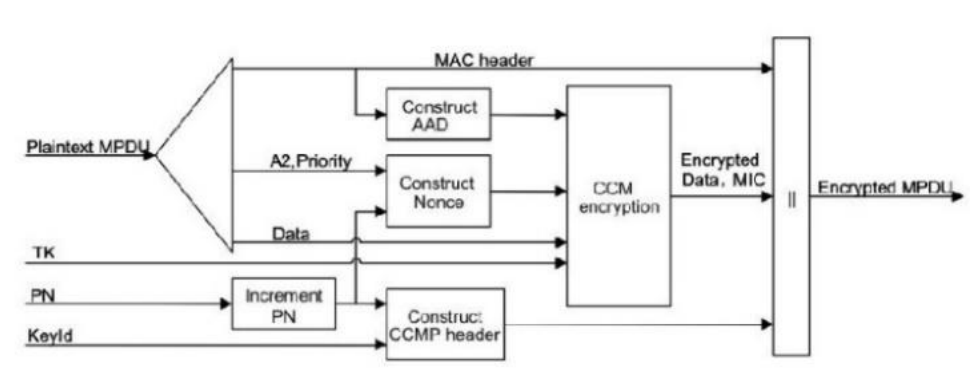


Figure 2 : CCMP Encryptions Process

**WPA 2 Vulnerbalities:**

1. the reinstallation of the PTK-TK, GTK and IGTK during a four-way handshake,
2. the reinstallation of the GTK and the IGTK during a group key handshake and
3. the re-transmission of an FT Re-association Request with the subsequent reinstatement of the PTK-TK.
4. Installation of the STK in the Peer Key handshake or of the TPK in the TDLS handshake. When a WNM Sleep Mode Response frame is processed installation of the Group Transient Key and Integrity Group Key.

**WPA3 (Wi-Fi Protected Access 3)** In June 2018, the Wi-Fi Alliance released [9] Wi-Fi Protected Access 3 (WPA3), and in July 2020, WPA3 became mandatory for all Wi-Fi-certified implementations. Considering all the hype created during the release date, many anticipated a very fast adoption rate. Statistics surprisingly proved otherwise, though. The clear motivation for developing WPA3 was to fix some security shortcomings in the WPA2-PSK handshake. Since the development process was secret, independent researchers were unable to study the features of WPA3.

Wi-Fi union impelled WPA3 the cutting-edge remote security standard that can dispose of every current deficiency in wireless. [10] The key highlights of WPA3 are Protection against brute force attacks, WPA3 Secrecy, Protecting Open/Public Networks. WPA3 utilizes SAE (Simultaneous Authentication of Equals) handshake to offer Forward Secrecy, which keeps the offender from decoding old caught traffic. Gives individualized data encryption a component that encodes remote traffic to alleviate the danger of Man in-the-Middle-Attacks. Provides 192 -bit encryption to Wi-Fi communications.

Like WPA2,[10] WPA3 has two modes: WPA3-Personal and WPA3-Enterprise. WPA3 has turned on a transition mode for backward compatibility when both WPA2 and WPA3 are made available. WPA3-Personal leverages SAE, a secure key exchange protocol used for authentication between peers. This would include a mutual password between the parties in the handshake, creating a high-entropy PMK to seed the 4-way handshake that will eventually produce a PTK. In an additional security measure, WPA3-SAE implements MFP(Management Frame Protection) to protect against reauthentication attacks, which otherwise could make users drop their connection to the AP. Since not all the existing 802.11 hardware supports MFP and/or SAE, WPA3 certification also includes a transition mode. In the transition mode, WPA2 APs connect using a 4-way handshake without MFP, while WPA3 APs connect using SAE with MFP.

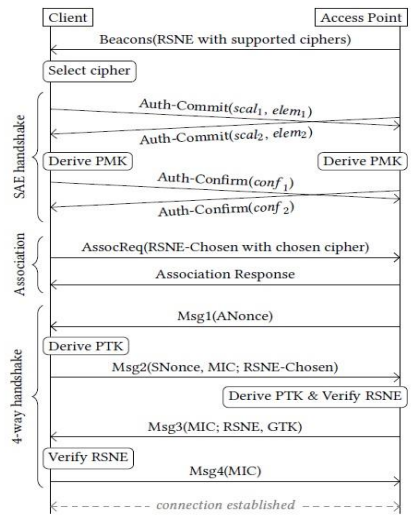


Figure 3: WPA 3 SAE 4-way Handshake

WPA3 underlying structure is similar to its predecessors but it employs enhanced security feature to prevent penetration. At the protocol level, WPA3 introduces an optional 192-bit security mode based on a 256-bit Galois/Counter Mode Protocol called GCMP-256 for authenticated encryption.

SAE[9] is a protocol supported by the Wi-Fi Alliance, whose cryptographic core is a Dragonfly handshake. Researchers either use the terms Dragonfly and SAE interchangeably or consider Dragonfly as part of the SAE protocol. In the IEEE 802.11 standard, SAE is treated as a variant of a zero-knowledge proof-based password-authenticated key exchange known as Dragonfly. Dragonfly is a symmetric peer-to-peer protocol whereby both peers can initiate the handshake with symmetric equal rights using an insecure channel with a secure symmetric key derived from a low-entropy shared secret. It derives underpinning from discrete logarithmic cryptography and elliptic curve cryptography, ECC or FFC. The basic protocol consists of two message exchanges: the commit exchange and the confirm exchange. The committing exchange reveals password guesses of participants. It is followed by the confirm exchange, where each participant confirms that their password is correct. After successful confirmation from both participants, the handshake will have been completed.

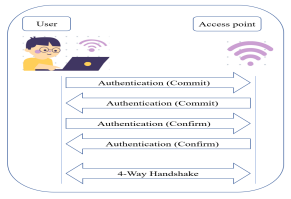


Figure 3: WPA3 Authentication: Dragonfly protocol

The IEEE 802.11w amendment, which was later integrated into the IEEE 802.11 base standard in 2012, was the first to introduce MFP. MFP provides origin authenticity, confidentiality, integrity, and replay protection of management frames. Because an attacker could use this functionality to forcibly disconnect users from a network, the Wi-Fi Alliance mandated the usage of MFP in WPA3. Due to the transition mode, WPA3 APs can advertise MFP as optional; this ensures that WPA2 users can remain connected to them.

**WPA 3 Improvements**:

Compared to TKIP and WEP, the encryption algorithm of WPA extends four necessary enhancements in WEP:

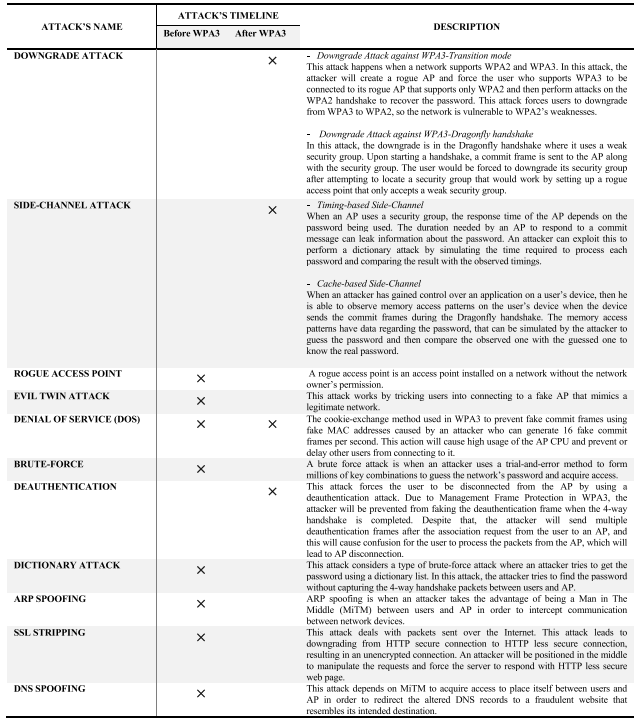
* Added a cryptographic Message Integrity Code, MIC, to prevent message forgeries.
* It should implement a new sequencing discipline on Initialization Vectors that would avoid the replay attack.
* A built-in per-packet key mixing function which removes the correlation between the public IV and a weak key, further enhancing the security. This would be reduced if a rekeying mechanism to derive fresh keys for encryption and integrity had been set up.

**Vulnerabilities to Home Internet**

In general, an IoT network in a home is a collection of multiple, heterogeneous, and autonomous computing devices offering various services to the users. In a common setting, devices in a home IoT network may include a smart thermostat, smart TV systems like Roku, music players, smart lighting, climate control systems, appliances that include dishwashers and washing machines, printers, and entertainment control devices. Many of these gadgets interact amongst themselves, sharing data in order to govern operating conditions such as temperature or pressure. However, due to the open architecture nature of such gadgets, one can't be certain that data is used only and exclusively for legitimate purposes. Aggressive monitoring can expose messages of a control plane, leaving IoT devices vulnerable to unauthorized access, remote control, or even full network disruption.

The DDoS attack in September 2016 has shown how IoT networks can become exposed to network-level attacks and how comparatively easy it can be to conduct a large-scale disruption. While this involved enterprise IoT networks, this incident certainly underlines potential threats to home IoT environments, which do not have the same robust security protections as enterprise settings. However, even in non-malicious scenarios, IoT network stability can be interfered with due to misconfigured devices or network intermediaries like switches or middleboxes. An example of this would be a wrongly configured device that keeps on broadcasting unwanted signals, leading to disruption in the network. Due to these risks, home IoT networks introduce a complex security landscape that requires strict access control, along with handling device communication and configuration.

**Attack analysis in Wireless Networks**

****

**Source:** A. Halbouni et al.: Wireless Security Protocols WPA3: A Systematic Literature Review**https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10274082**

**Challenges in the Home IoT Environment [10]**

Challenge 1: Inability on the Part of Users

One of the key challenges in using IoT in smart homes is that ordinary users are unaware of the security vulnerabilities and mechanisms of protection. ABAC will be highly applicable due to the flexibility of the model wherein policies under ABAC are generalizable and reusable across multiple environments; thus, a policy working in one IoT setting may potentially apply across other networks. These policies can be tested in controlled environments and then deployed in real-world settings. Thirdly, the ABAC policies may depend on environmental attributes. This allows for adaptable security policies which can respond to different home configurations without the need to consider details of individual devices. In this paper, we will provide some samples of pre-configured policies that may improve security within the home IoT networks.

Challenge 2: Onboarding New Devices in the IoT Ecosystem

The second challenge is that devices are usually added in an ad hoc manner to a home IoT network. This, in turn requires policies that are device-agnostic in order to secure the network with no dependency on device-specific configurations. ABAC policies allow easy integration of new devices by avoiding continuous reconfiguration of the policy each time a new device joins the network. This retains the plug-and-play nature of IoT networks.

Challenge 3: Preserving Quality of Experience

For instance, home users need uninterrupted interaction with their devices; this calls for strong access control and non-interference protocols. Consider, for example, devices like Roku TV or a network-connected music player that is usually controlled via mobile apps. Ideally, no more than one app should be accessing any of these devices at any given time to avoid accidental or intentional interference. ABAC can ensure that only one app interacts with a device at any instant in time and thus reduce response latency and user frustration.

Challenge 4: DDoS Attack Mitigation in Home IoT Networks

Flooding attacks initiated by rogue devices can pose a severe threat in home IoT networks by consuming network resources with unnecessary traffic. Detection and isolation of these devices remain challenging as home networks neither have any monitoring system nor IDS. ABAC allows capturing and constraining network-level behavior, hence isolate the misbehaving devices, and mitigate the disruption.

Challenge 5: Mitigating Malicious Behaviour from Co-located Devices.

This final challenge addresses the mitigation strategies for malicious code co-located within IoT devices and third-party applications. Most IoT devices rely on third-party applications to carry out useful functions; hence, there is a chance of infection by malware that would lead to exposing device control to remote attackers. ABAC enforces access controls in order to assure that the third-party apps are compliant with the security protocols and only dispatch valid commands to IoT devices. Besides, logical control in ABAC may prevent suspicious inter-device communications, hence limiting malicious or unintended interactions.

**Securing Home Internet**

We are admins of our home and home network. We should be diligent and be aware of which devices are connected to our home network. We should be privy to all changes to our home network including new devices joining and to any device which got disconnected from the wireless network. As more and more wireless IoT devices gets connected it can be overwhelming to keep a track of home Wi-Fi networks as they can get complicated as they add up quick.

Considering an average home with regular devices for a family of 2 members,

Device list:  
2 Laptops  
2 cellphones  
2 smart watches  
One smart TV  
One door bell camera  
One door lock  
One Smart assistant (Google/ Amazon/ Apple)  
One thermostat  
Smart Washer  
Smart Dryer  
Couple of smart switches

So, from above list we already have 14 devices, now if we add a child in the family or visitors the number can quickly add up.

Now, staying on top of these device list at our home can be overwhelming and is also crucial to keep our home network safe.

**Steps to Secure Home Network**

Ensure router supports WPA3 and is enabled to communicate using WPA3, is not its time to switch the router. Also ensure that the router firmware is updated.

Changing router default settings after installation is crucial. Routers of certain manufacturers tend to have same default admin username and password combinations and can be found online and if not changed this is a major vulnerability to the network.

Two important passwords to change:

1. The Wi-Fi network password: this is the password you use to connect to the wireless network.
2. The router admin password: this is the admin password you use to log in to the router to make changes to the router admin configurations.

Some router features can be handy but pose greater risk to the network, such as “remote management”, its critical to turn off the feature as this allows to log into the router remotely through the internet.

Another feature such as WPS which is a primitive wireless technology can be found of some newer routers, which allow a router to pair connectivity to a device which doesn’t support WPA3/2 hence can be connected without password.

Lastly UpnP which is a feature that allows devices on the network to talk to each other, this feature can be handy but can make the wireless network vulnerable to attacks.

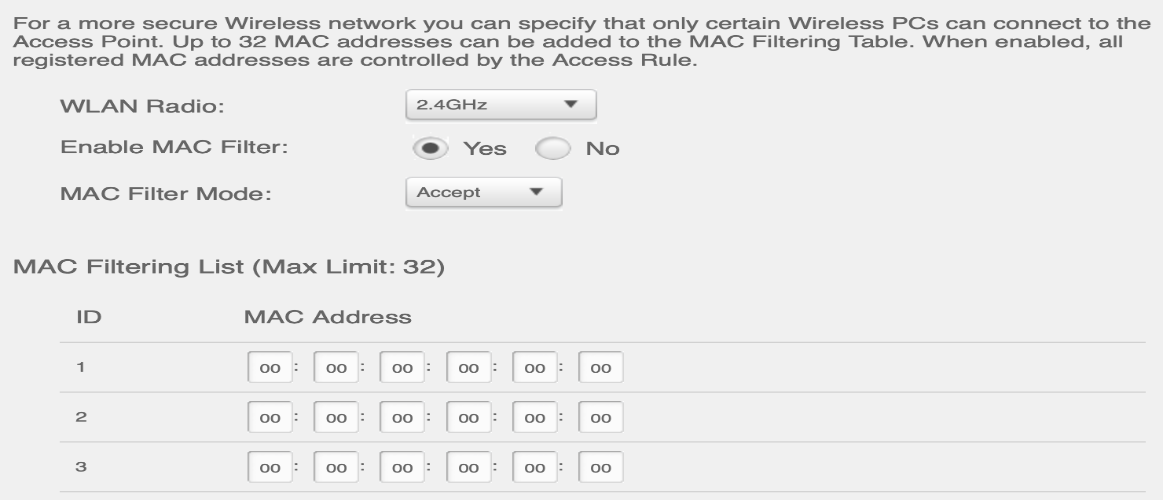
Its important to set up Guest Network on the Wi-Fi network, this ensures that the home Wi-Fi network to which all home devices are connected aren’t used by visitors and fewer people are aware of the home Wi-Fi password.

Ensure router firewall is turned on and its also important to add knowledgeable rules to the firewall ensuring its applied to the proper interface, as we all know just the firewall rules won’t do anything unless applied to any interface.

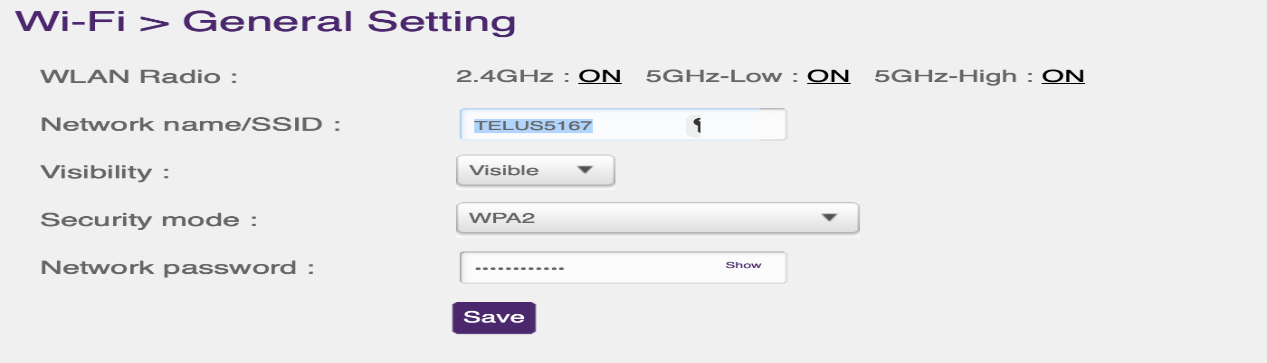
Protecting devices and ensuring device OS’s are updated regularly along with proper authentication mechanisms in place. Just like an organization its every member at home’s responsibility to ensure their devices are secured, emails are properly vetted and not clicking on any links which may look suspicious or from unknown senders.

There are few other important steps that can be performed and should be done to secure the home wireless network,

* Set up MAC filtering for devices that can connect to the main Wi-Fi network while you have a Guest Network where visitors can connect. At the same time, one will need to add any new device to the MAC filter before connecting.



* Hide the main home Wi-Fi network SSID, only the owner can connect to the wireless network by typing the SSID and password, in this way nobody will be able to even try to brute force the network as they won’t know the SSID of the network.



These steps will not only ensure the IoT devices are safe in the home Wireless network but also ensure the wireless network is safe from any localized attacks.

**Reference**

1. Author: H Valchanov Title: OP Conference Series: Materials Science and EngineeringLink: <https://iopscience.iop.org/article/10.1088/1757-899X/618/1/012031/pdf>
2. Author: [Kindervag, John](https://www.proquest.com/openview/d5ec426f44daae5c8889b1791dda8767/1?pq-origsite=gscholar&cbl=52433) Title: The Five Myths of Wireless Security Link: <https://www.proquest.com/openview/d5ec426f44daae5c8889b1791dda8767/1?pq-origsite=gscholar&cbl=52433>
3. Author: T. M. Hoang, A. Vahid, D. C. Sicker and A. Sabharwal, "Physical-Layer Spoofing in WiFi 6 to Steer the Beam Toward the Attacker," ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 2024, pp. 4006-4011, doi: 10.1109/ICC51166.2024.10622744.  
   keywords: {Wireless communication;Protocols;IEEE 802.11ax Standard;Physical layer;Encryption;Security;Jamming;802.11ax;WiFi 6;physical layer security},
4. M. Trnka, J. Svacina, T. Cerny, E. Song, J. Hong and M. Bures, "Securing Internet of Things Devices Using The Network Context," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4017-4027, June 2020, doi: 10.1109/TII.2019.2954100. keywords: {Authentication;Wireless fidelity;Internet of Things;Sensors;Context-aware services;Servers;Context-awareness;anomaly detection;authentication;Internet of Things (IoT);security},
5. Author: Bruhadeshwar Bezawada Computer Science Department Colorado State University Fort Collins, Colorado, USA Bru.Bezawada@colostate.edu Kyle Haefner Computer Science Department Colorado State University Fort Collins, Colorado, USA Kyle.Haefner@colostate.edu Indrakshi Ray Computer Science Department Colorado State University Fort Collins, Colorado, USA Indrakshi.Ray@colostate.eduTitle: Securing Home IoT Environments with Attribute-Based Access Control Link: https://dl.acm.org/doi/pdf/10.1145/3180457.3180464
6. Author: Debora Estrada, Lo'ai A. Tawalbeh, Robert Vinaja Title: How Secure Having IoT Devices in Our Homes? Link: <https://digitalcommons.tamusa.edu/cgi/viewcontent.cgi?article=1023&context=computer_faculty>
7. Author: RNAR PÉTURSSON Title: Ethical Hacking of a Ring Doorbell Link: <https://www.diva-portal.org/smash/get/diva2:1751192/FULLTEXT01.pdf>
8. Author: Fabio Duarte Title: **60+ Amazing IoT Statistics (2024-2030)** Link: <https://explodingtopics.com/blog/iot-stats>
9. Author: ASMAA HALBOUNI, (Graduate Student Member, IEEE), LEE-YENG ONG , (Senior Member, IEEE), Title: Wireless Security Protocols WPA3: A Systematic Link: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10274082>
10. E. Baray and N. Kumar Ojha, "‘WLAN Security Protocols and WPA3 Security Approach Measurement Through Aircrack-ng Technique’," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2021, pp. 23-30, doi: 10.1109/ICCMC51019.2021.9418230. keywords: {Protocols;Computer hacking;Atmospheric modeling;Linux;Wireless networks;Standards organizations;Security;Aircrack-ng;Crack;Airodump-ng;Kali Linux},
11. Author: Kim, HyunHo Title: Analysis of IoT Security in Wi-Fi 6 Link: <https://koreascience.kr/article/JAKO202120941712294.page>
12. Arash Habibi Lashkari, Mir Mohammad Seyed Danesh and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," 2009 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, China, 2009, pp. 48-52, doi: 10.1109/ICCSIT.2009.5234856. keywords: {Communication system security;Wireless application protocol;Cryptography;Data security;Protection;Access protocols;Media Access Protocol;Knowledge management;Data privacy;Wireless LAN;Wireless Security;WEP;WPA;WPA2;802.11i;802.11X},
13. Author: Federal Trade Commission Consumer Advice Title: How To Secure Your Home Wi-Fi Network Link: https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network