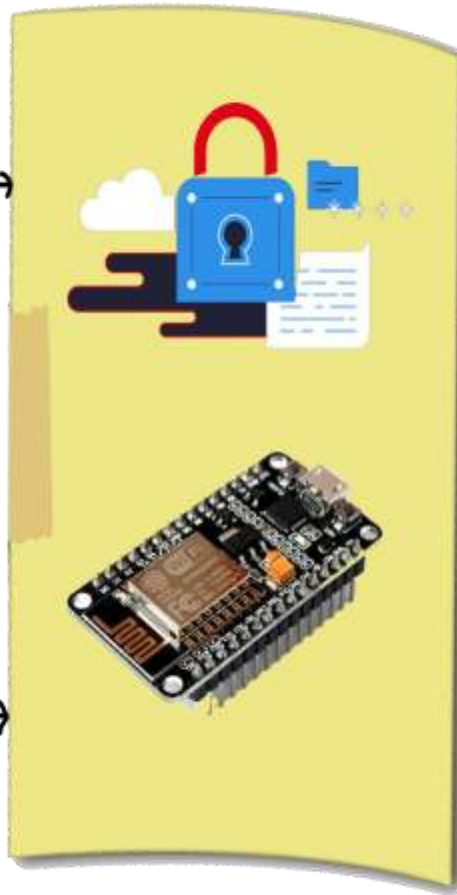


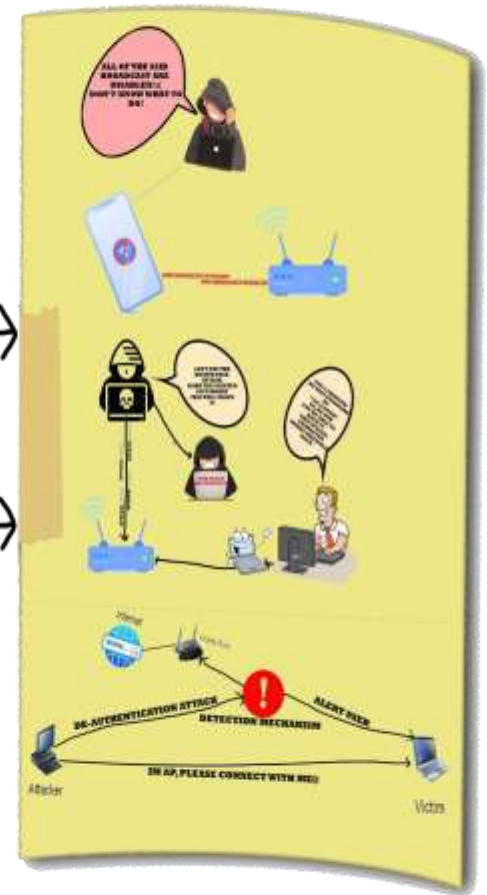
Problem



Proposed Prototype



Solution



Abstract

The critical problem highlighted throughout this project is poor verification as well as authorization deployment in WIFI. There's many specialized problems, for instance the incapacity to create or choose security mechanisms as well as implement them, therefore culminates with in identification as well as installation of susceptible encryption stack, password protection as well as authentication system, end-user measures, and security mechanisms. The creation and access privilege reliability of WIFI have been the important points of this study's emphasis. This work's significant element is the creation of a prototype system that makes it possible to choose or create security protocols adequately and install those for WIFI. This work is significant since no prior research has been done with the goal of creating a prototype system that would allow an application to see the security level that would result from adopting a particular collection of security mechanisms and how they would be configured.

Keywords



Contents

Abstract	6
Keywords	7
Table of Figures	11
Introduction	13
Aim.....	16
Objectives.....	17
Technical Objective.....	18
Business Objective	18
learning Objective	18
Personal Objective.....	19
Scope.....	20
Ethical Questions.....	22
.....	22
Justification	23
Problem Statement	23
Solution	25
Step 1.....	26
Step 2.....	26
Step 3.....	26
Step 4.....	26
Step 5.....	26
Ethical consideration	28
Secondary Literature Review	30
Case Study One: Cisco Meraki.....	30
How it actually provides security?	31
Successful Security Provider Reason	32
▪ Cloud Managed Security	32
▪ Upgraded network	33
▪ Simplified Network Management.....	33
Case Study Two: Webroot WIFI Security.....	33
How it will Benefits Users?.....	34
Successful security provider Reason	34

Case Study Three: Net Gear Armor	34
Primary Research	36
Considered Methodology	36
Waterfall model.....	36
Prototype Model.....	37
Agile Model.....	38
Selected Development methodology	40
Agile methodology	40
Phase of Methodology	40
▪ Concept	40
▪ Inception.....	41
▪ Iteration	41
Survey Result	43
Pre survey result.....	43
Post survey result	43
Tools.....	44
Node MCU	44
▪ Benefits	44
Jumper Wire	45
▪ Benefits	45
TP Link TLW722N WIFI Adapter.....	45
▪ Benefits	45
LED and Bread Board	46
▪ Benefits	46
Technology.....	47
Arduino IDE.....	47
▪ Benefits	47
C Programming	48
▪ Benefits	48
Airmon-NG	48
▪ Benefits	48
Kali Linux	49
▪ Benefits	49

Virtual Machine.....	49
▪ Benefits	49
Techniques for Better Improvement.....	50
Security	50
Availability.....	51
User experience.....	51
Attributes of Technical Quality.....	52
Findings.....	52
Overview	52
Research Question Conclusion.....	53
Question One.....	53
Question Two	53
Question Three	53
Risk Plan	54
Project Plan	55
Future Work	56
Creating a Statistical Model	56
The framework proposed Depends on Information Provided by Users.....	56
Analysis of the Figure's Applicability	56
Challenges	57
Limitation.....	58
Reliability	58
Recommendation.....	58
Conclusion.....	59
Appendix	60
Arduino Installation.....	60
Code Sample	62
System Prototype.....	63
Reference.....	64

Table of Figures

Figure 1: Concept of Evil Twin.....	13
Figure 2: Outcome of SSID Broadcast Enabled.....	14
Figure 3: Factors of Weak WIFI Security	15
Figure 4: De-Authentication Concept.....	15
Figure 5: Objectives	17
Figure 6: Sub Objectives	18
Figure 7: Scope	20
Figure 8: Ethical Questions	22
Figure 9: Project Problem	23
Figure 10: Solution for Problems	25
Figure 11: De-Authentication Solution Steps.....	26
Figure 12: Dashboard of Meraki	31
Figure 13: Successful Security Provider Reason of Meraki.....	32
Figure 14: Considered Methodology.....	36
Figure 15: Waterfall Methodology	37
Figure 16: Prototype Model.....	37
Figure 17: Agile Model	38
Figure 18: Phase of Agile Methodology.....	40
Figure 19: Iteration of Agile Methodology.....	41
Figure 20: Pre Survey Result	43
Figure 21: Post Survey Result.....	43
Figure 22: Tools	44
Figure 23: NODE MCU Benefits.....	44
Figure 24: Jumper Wire Benefits	45
Figure 25: WIFI Adapter Benefits.....	45
Figure 26: Bread Board Benefits.....	46
Figure 27: Technology	47
Figure 28: Benefits of Arduino IDE.....	47
Figure 29: Benefits of C Programing	48
Figure 30: Benefits of Airmon-NG	48
Figure 31: Benefits of Kali Linux	49
Figure 32: Technology for Better Improvement.....	50
Figure 33: Security	50
Figure 34: Technical Quality Attributes	52
Figure 35: Risks Plan	54
Figure 36: Project Plan 1	55
Figure 37: Project Plan 2.....	55
Figure 38: Future Works	56
Figure 39: Challenges.....	57
Figure 40: Arduino Installation 2	60
Figure 41: Arduino Installation 1	60
Figure 42: Arduino Installation 5	61
Figure 43: Arduino Installation 4	61
Figure 44: Arduino Installation 3	61
Figure 45: Code Sample.....	62
Figure 46: De-Auth Demonstrate	63

Figure 47: System Prototype 63

Introduction

Because of the lower cost and mobility of work in recent years the use of Private WIFI Network has been increased and can be found installed in almost all house. The continuously increasing in this network also poses different types of security risks against the data, information of the connected users. This dissertation is mainly focused on the security risks on WIFI Network, how to detect the types of attack against the network and what are the approaches to improve the security. The methods proposed here is mainly focused on protecting the sensitive information and guaranteeing the flow of data and information authentic. If discussing about the recent security approaches, almost all WIFI Network uses the WPA2, results the several outsider attacks which allow hackers to easily eavesdrop over the data that is transmitted over the network. Even the encryption is used in WPA2, hacker can easily crack the password by sending the De Authentication Packet which helps to capture the Handshake that allow hacker to crack and connect to the network by doing Brute Force over the captured Handshake. Problem like eavesdrop which was possible in “WPA2” is now almost impossible on “WPA3” because of it’s more advanced security feature. (james, 2020) But these standards also unable to solve another major problem like “Evil Twin Attack”.

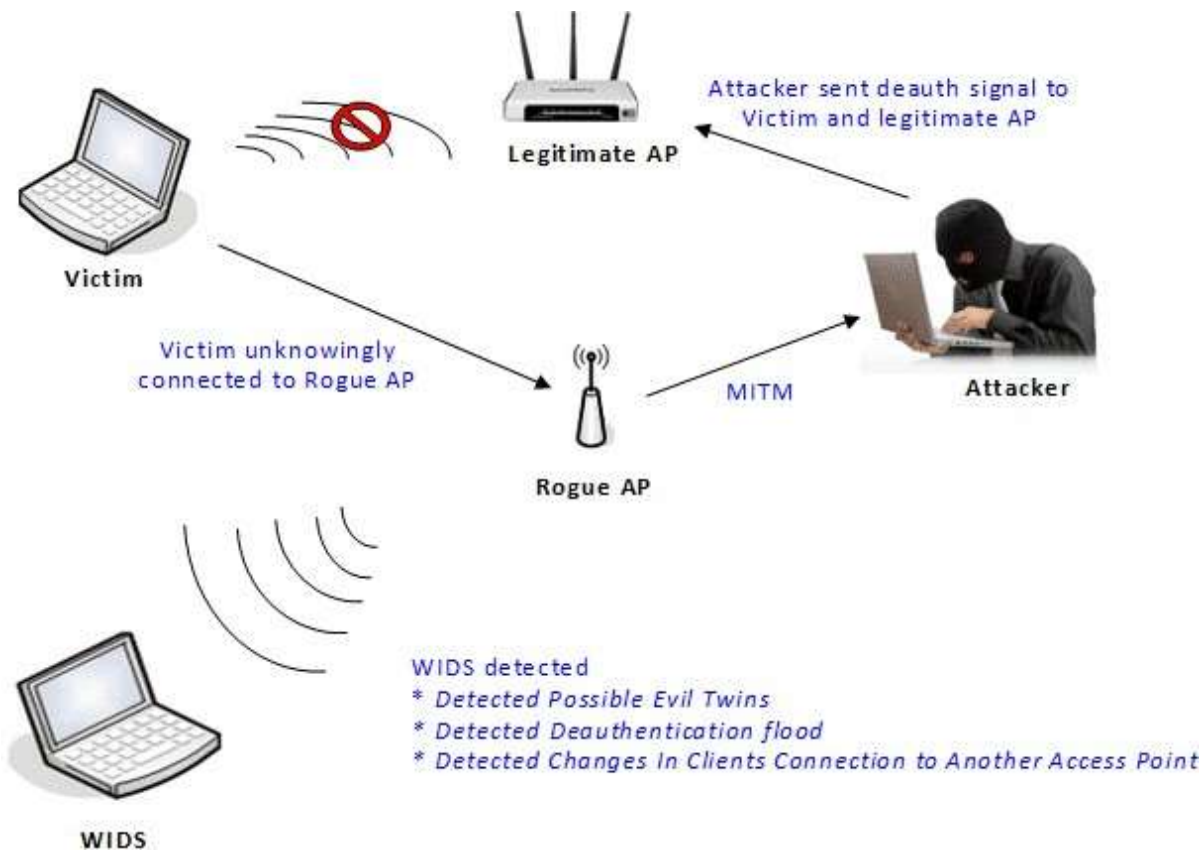


Figure 1: Concept of Evil Twin

Nowadays most of the WLAN's apply the "IEEE 802.11i" standard whose main motive is to provide the maximum level of integrity with confidentiality that can be obtained by allowing access control and encrypting the data which can be transmitted over the network. (Chrtsy, 20012-07-24) But whenever these standards are not well implemented which surely will fail to maintain the integrity and confidentiality of users. Because of the poor implementation of security approaches over the Private WIFI Network there are way too threats which will be received at the WLAN's.

- The wireless AP will broadcast the SSID Name, MAC addresses and many more within it's signal coverage to the mobile devices which benefits hacker to connect to the network by detecting and cracking it. (Winder & Davey, 2018)



Figure 2: Outcome of SSID Broadcast Enabled

- Whenever the poor encryption standards are used then, the attacker can easily sniff the data frame by using different tools like Wireshark to know what they are surfing or to capture the credentials. Even the encryption standards are used then in some cases the hacker will use the different cracker to crack it. (ED REFORM, 2011)

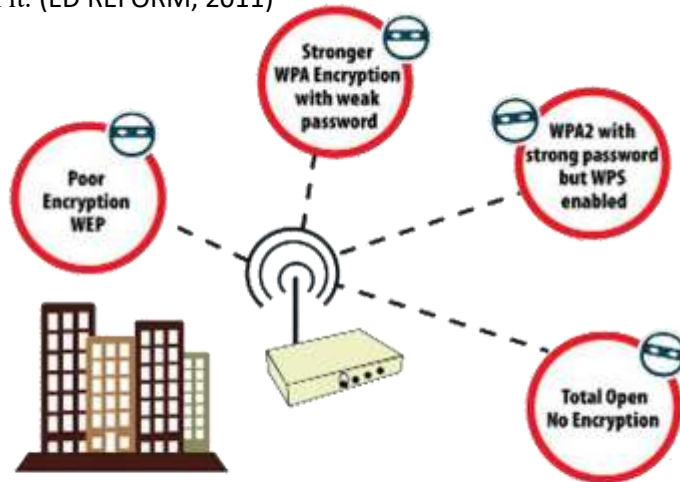


Figure 3: Factors of Weak WIFI Security

The use of unencrypted frames for De Authentication and negligence in authentication in “802.11” standards, the attacker can easily inspect the MAC Address of the connected users which can be used to allow De Auth attack. So, to confirm the authenticate De Auth Frame, the source of these packets must need to be verified.

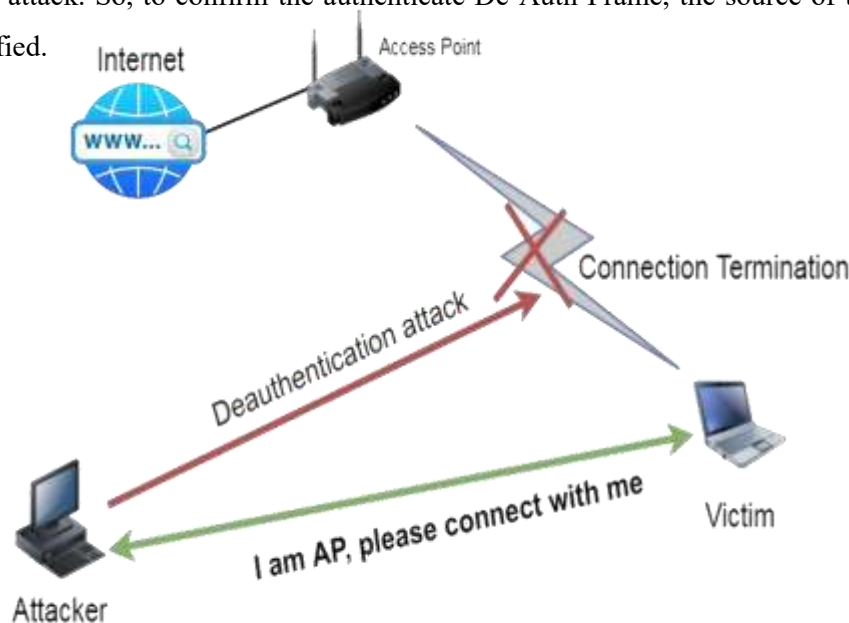


Figure 4: De-Authentication Concept

In this paper, security issues over WIFI Network along with the detection technology for De Authentication Attacks and verification of the root of these De Auth Frame which is transmitted over the “802.11” network standard, and defending solution for different security issues is proposed in order to make the Private WIFI Network more secure and safe. (stantzouris, 2020)

Aim

The main aim of this report is to make Private WIFI Network more secure and reliable by subjecting it's different security issues, development of De Authentication detection device, verification of the source of De Authentication Packets and solution for different attacks which will compromise the integrity and confidentiality of the data of users.

Objectives

The main objective of this thesis is to develop the detection technology by studying its different security issues and to make the WLAN more authenticate, to implement the access control security system. Some of the primary objectives are mentioned below:



Figure 5: Objectives

- Proper investigation of the “IEEE 802.11” network standard implementation to dig out the particular vulnerability which will play the lead role to contribute the weak WLAN authentication as well as access control of the Private WIFI. (Chrity, 20012-07-24)
- To explore the different security measure that is furnished by the WLAN cipher suites, user authentication, different tactics for access control and software that is used in the system of server which is implemented on the WLAN authentication
- To build up the physical device that is used to detect the De Authentication attack. For this a hardware component called “Node MCU” will be used which will indicate using the signal as soon as the WLAN receive the De Auth Packets from the hacker which helps to make the user aware about that. (KODY, 2018)
- To develop the perfect architectural component which then is used to build up the prototype that is rich in security features along with the WLAN authentication and access control in Private WIFI
- To use the different approaches to make the Private WIFI Network more secure. Different technology like De Auth source finder, Detecting Technology and preventive measure for attack like “Evil Twin” which is almost impossible to prevent in WPA3 security standard. (Jomilė Nakutavičiūtė, 2020)

The objectives of this thesis is further more divided in to different subobjectives. These subobjectives and their motive are listed below.

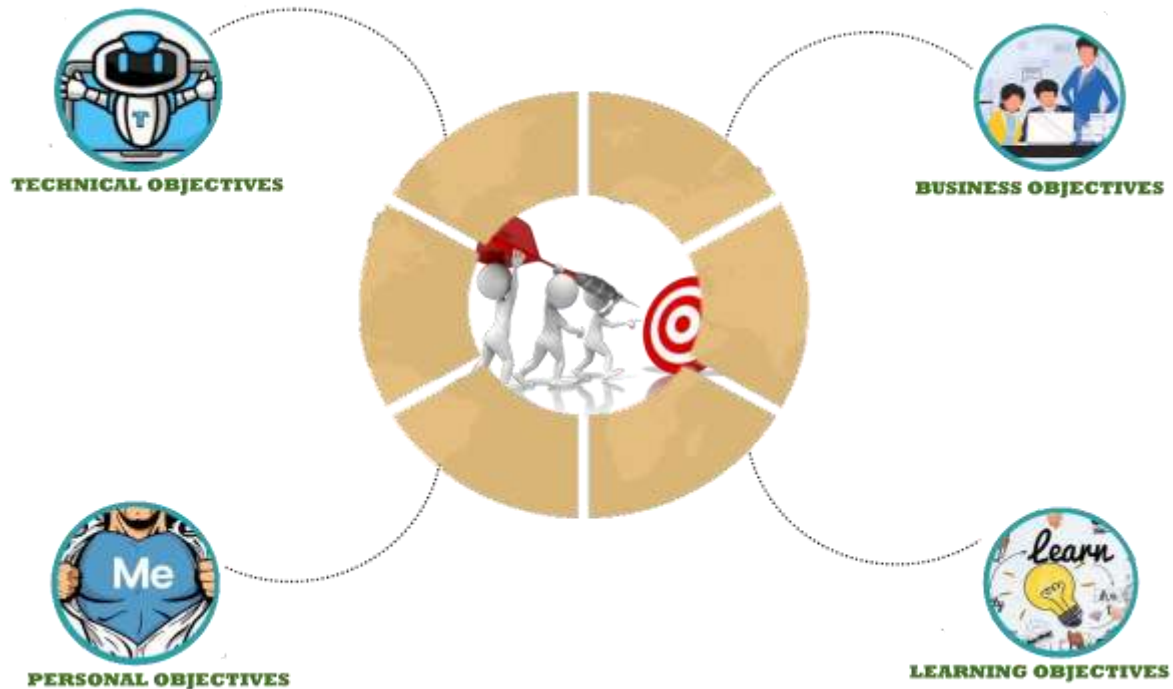


Figure 6: Sub Objectives

Technical Objective

- ✓ Perform the De Authentication Attack to the targeted Private WIFI Network to list and examine it's vulnerability by using the Network Adapter which helps to improve the security of the Network later.
- ✓ Build up the De Authentication Detecting device that will give signal as soon as it receives the De Authentication Packets from the intruders
- ✓ Apply different preventive measures to defend different possible attacks like “Evil Twin Attack” which is almost impossible to defend on itself using WPA3 security standard.

Business Objective

- ✓ Design and develop the tools for detecting the common attacking technique called “De Auth” which will play lead role in making the user aware and take action as soon as the network receive the attack.

learning Objective

- ✓ Understands and explain the different ways to protect the WIFI Network against the different attacks like “Eaves Drop”, “Evil Twin”, “De Auth” by studying the network standards and security standards

- ✓ Understand the necessity and scope for the implementation of the security measures for the Private WIFI Network in order to protect the integrity and confidentiality of the connected users.

Personal Objective

- ✓ Implement and develop the security measure for the sake of the users privacy
- ✓ Study and analysis the same alike project on the basics of it's article and methodology that will aid up making this project even more efficient and good.

Scope

This report is basically developed with the scope to address the different security issues of the Private WIFI Network and methodology to solve them. A simple WIFI Adapter can be used to destroy the entire WIFI Network in minutes. Because of this the information of the connected devices like mobile, laptops can be known easily to the attacker, what they are serving in the internet everything which can challenge the privacy. (Gowri Shankar & Nagesha, 2016)



Figure 7: Scope

So, this report is designed to helps to solve the different security risks on Private WIFI Network. Here different approaches will be mentioned which will helps to defend against the different attacks. The another scope is also to develop the De Authentication Detection Technology which will signal as soon as it receive

the de auth packet. Which means that, it can aware the user that it is under the security risks which alert them to implement more advanced security features. Now a days people still use the standards like “WPA” which is vulnerable to eaves drop because of it’s weak cryptographic algorithm but with the origin of “WPA2” the problem of eaves drop is solved but not the problem of Evil Twin. Implementation of the authentication and access control over the network, use of the strong cryptographic algorithm and to behave as the impetus as well as the catalyst for the upcoming study and research about the WIFI Security is the main scope of this thesis. (Gowri Shankar & Nagesha, 2016)

Ethical Questions

QUESTION:1

WHICH STRUCTURAL FACTORS SHOULD BE TAKEN INTO ACCOUNT WHILE CREATING A PROTOTYPE SYSTEM FOR CHOOSING OR DESIGNING SECURITY MEASURES FOR WLAN?

WHAT LEVEL OF VULNERABILITY IN THE WLAN ENCRYPTION SUITE, AUTHENTICITY AS WELL AS SECURITY SYSTEMS, AND PROGRAM THAT IMPLEMENTS AUTHENTICITY AND SECURITY SYSTEMS IN A WIFI IS EXPOSED BY COMMON THREATS?

QUESTION:2

QUESTION:3

WHAT ARE THE EXECUTION FLAWS WHICH MIGHT IMPEDE THE EXECUTION OF WLAN AUTHORIZATION AND ACCESS CONTROL ASSURANCE IN A PARTICULAR WLAN?

Figure 8: Ethical Questions

Problem Statement

There have been a variety of factors contributing to this recent spike in attack vectors, but the main one is that a WIFI network's essence of incredibly simple end-user access also outcomes in a larger threat landscape. A WIFI technology only needs the intruder to be adjacent, as opposed to a WIFI router in which accessibility to a subnetwork is considered necessary (and even this is relative). Additionally, there's a widespread ignorance and unawareness of WIFI communication. Weak enactment of the authentication and access control as well as the solution for the different security risks of Private WIFI are the main subject which is going to addressed in this report. Poor implementation of security approach more has two different sub-components which covers the following:

- The scarcity of the exact model which helps to entitle design as well as the designation of the security approaches along with their configuration for WIFI authentication.
- Configuration and designation of the control mechanism, different security features like: MAC Filtering, Disabling SSID Broadcast etc.

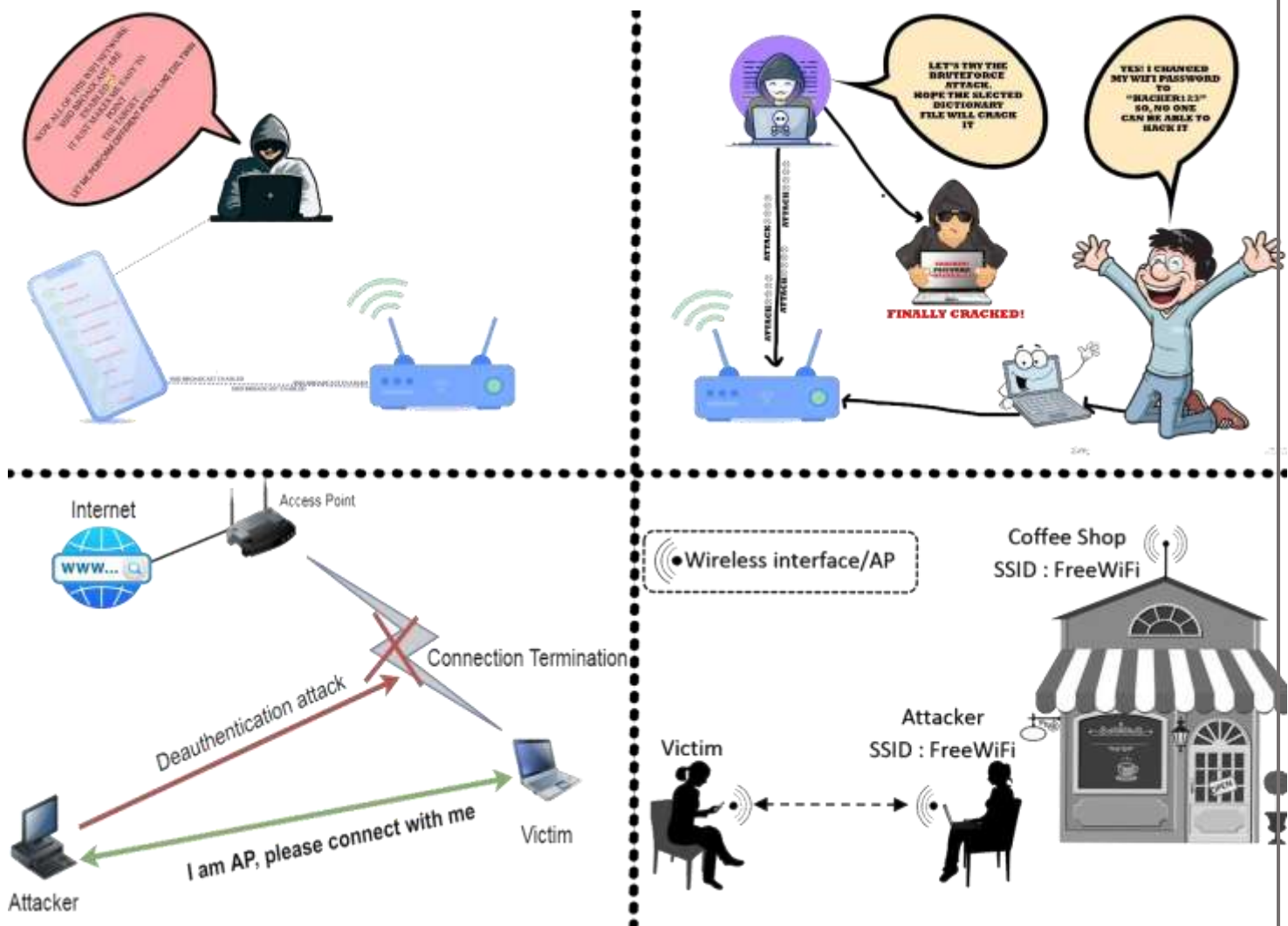


Figure 9: Project Problem

Furthermore, there are a lot of problems with Private WIFI Networks. The most common problem is configuration issues which is one of the biggest negligence that leads to different security issues on WIFI Networks. Issues like misconfiguration, incomplete configuration, default passwords of SSID and Admin Panel, Enabling the SSID Broadcast, inappropriate use of MAC Filtering and URL Blocking as well as the Signal range are some issues which need to be configured wisely. Enabling the SSID Broadcast allows a hacker to target the network easily as it can be visible directly over mobile devices. (Bradley Mitchell, 2020) Similarly, the use of wider signal range even on a small area leads a hacker to target the Network even from a distance. So, the configuration needs to be configured wisely. Similarly, another problem that compromises the WIFI security is De Authentication Attack which lies under the genre of management frame. As the user wants to disconnect from WIFI, then it will send the De Auth Frame which helps the client to disconnect from the network. Similar technology is used by the hacker to disconnect the other user from the network by using the simple WIFI Adapter which supports the Packet Injection. The hacker first inspects the target MAC Address and then sends the frame which plays a role to loosen the connection of the victim that helps to capture the handshake which is an actual password of the WIFI that the hacker gets while the user is trying to reconnect to the AP. Likewise the above mentioned problem there is another term called “Evil Twin Attack” which is one of the major issues where an attacker lures the Access Point with a strong signal which actually is the duplicate SSID of the legit Access Point. Because of this the regular user will try to connect to the fake AP thinking it's the real one. As soon as the victim connects to the fake AP distributed by the attacker, now the hacker can see what he is surfing, credential details etc. (Kody, 2019)

Solution

The methods suggested here are primarily concerned with safeguarding sensitive data and ensuring the integrity of data and information flow. Different strategies, such as disabling SSID Broadcast, help to conceal the AP name, which makes it more difficult for attackers to target the network; using lower signal helps to provide signal in a lower coverage area, which forces attackers to send packets with higher latency, which makes it even harder; using MAC Filtering aids in the blocking of specific suspected MAC Addresses; and using URL blocking aids in the blocking of suspected sites that are hosted to steal credentials. (Ruri Ranbe, 2018)

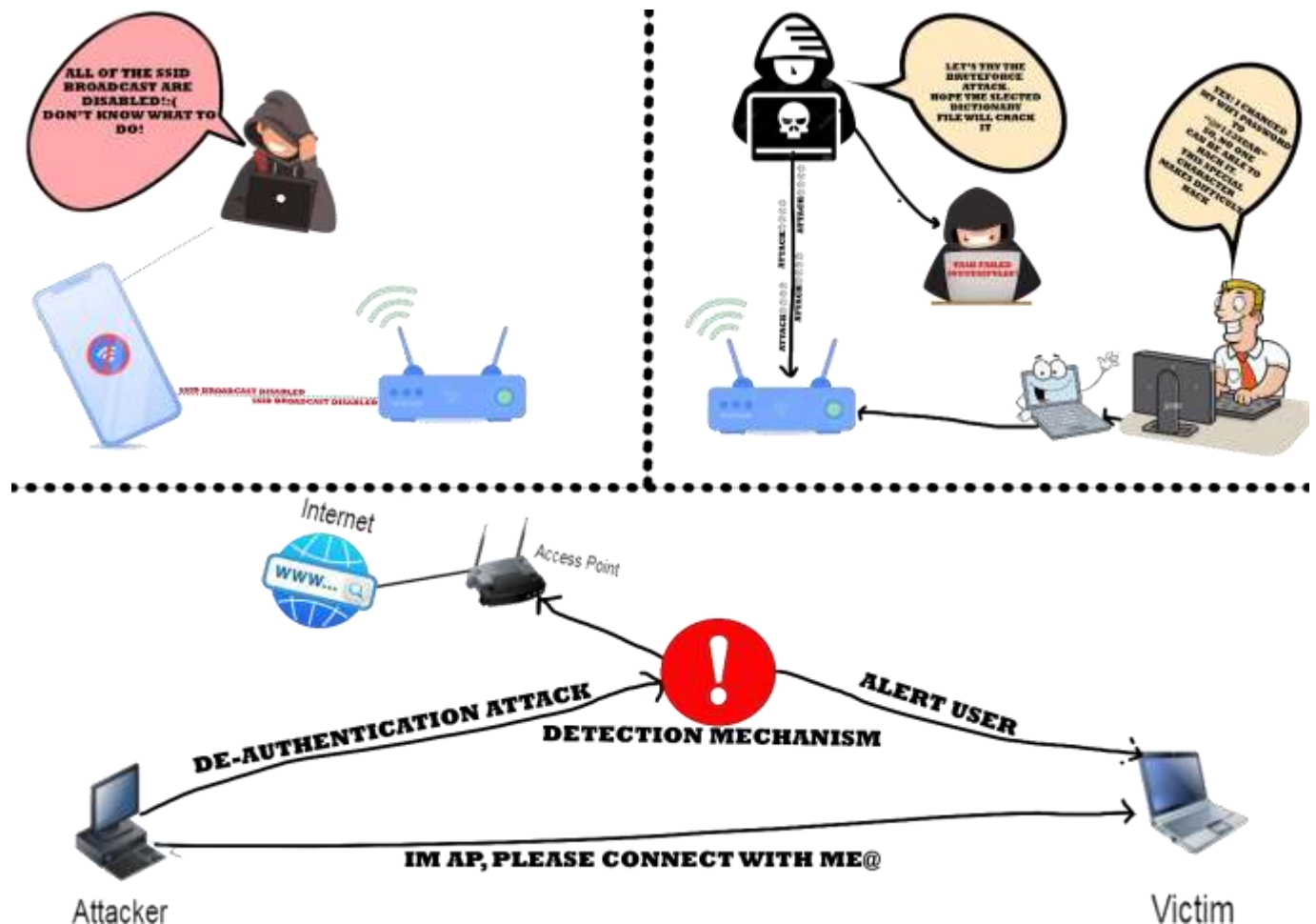


Figure 10: Solution for Problems

Similarly, to fight for the De Authentication attack a simple device will help to play a lead role in detecting the De Authentication attack which makes person to take more preventive measures and to take the action as soon as possible. For this an IOT device called “NODE MCU” will be used which is injected with the code to detect the frame. Similarly, the use of SHA algorithm will solve the issues of the De Authentication Attack which helps to hash a Unique ID during the process of connection and verify for the unique ID as soon as the packet of the De Authentication is being dispatched. Another solution i.e. “MAC SDP Dos

Algorithm” can be used by modifying it for the detection and prevention of the De Authentication attack which can be initiated by spoofing the connected users MAC Address. The proposed solution is explained in the following steps:

Step 1

In this step the devices of both hacker and legitimate user need to be connected to same network

Step 2

The Access Point now will develop 8-bit key which now will be forwarded to the targeted victim by encrypting firstly with the algorithm called RSA

Step 3

Now, the victim uses RSA to decrypt the key which then is safely deposited by both sender and receiver.

Step 4

As soon as the De Authentication Attack start happening, it can be detected by AP machine by verifying threshold value which is determined as 5. It is chosen at as it helps the AP to start De Authentication Attack.

Step 5

Now, the AP will terminate the flow of TCP packet to the victim. Now, the victim will pass the key to the AP which is in encrypted form. The AP now will match the key received from victim by decrypting it with the available key. By this a De Authentication Attack can be prevented.

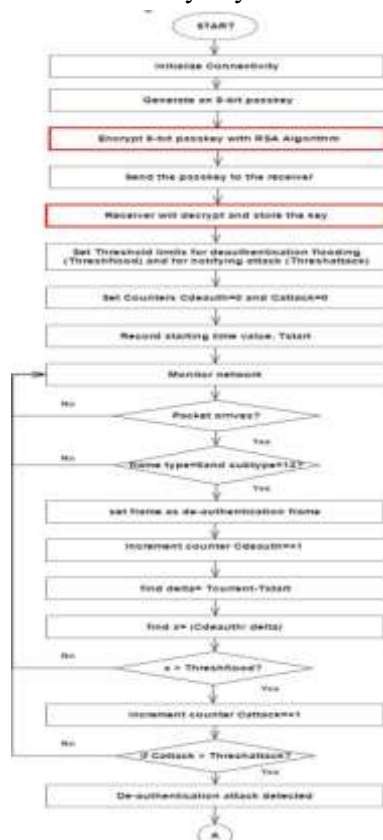


Figure 11: De-Authentication Solution Steps

One of the biggest problems of WIFI Network was Eaves Drop Attack where attacker can easily capture the frame and decrypt it with the encryption cracker tools which allow them to see the sensitive information. This attack was only possible on the “WPA” network standard. But the “WPA2” network standard solve this issue. The issue of “Evil Twin Attack” is not solved by the “WPA2” standards. So, to solve this, approaches like Certificate, Trust on First Use and Static Network Name will be used.

Ethical consideration

This dissertation will explain why carrying out a risk evaluation is crucial when drafting a safety strategy. The primary goal of a cyber policy is to enhance encourage the group of security by outlining who is responsible for what components of network protection. Another reason is to specify how data must be safeguarded when being transferred over a WIFI router. As an illustration, the IEEE standard protocol (WEP), that might not be the optimal encryption method, could be used. It is crucial for businesses handling confidential material to be cognizant of current privacy issues and take precautions against them. As soon as it comes to the WIFI Network that supports the internet connectivity to surf on internet the use of VPN, GPS devices to protect privacy of users are not illegal until the topic of attacking or bleaching of data comes in. Similar to this, it is unlawful to expose or disclose the hacker's location or MAC address by performing node scanning or using any other way as it compromises privacy such as location privacy and information privacy. Given the potential employment of networking, a variety of ethical issues have been raised, especially some who pertain to just using WLAN technology's possibilities for statistics harvesting and implementing technology that all other firms can use of their own resources and materials. Those ethical implications have primarily been explored, and in numerous instances, it corresponds with the ones that have been addressed by literature and legislation.

Unaccredited disclosure poses ethical considerations, like when that there is no legislation that prosecute someone else who signs on to the next user's computer on a private network. When using another's network means that significant access could no mores use the maximum throughput that is assigned for him, this would also be deemed thieving. In computer networks, one of most moral choices are reached when evaluating an user's right to confidentiality against the objectives of a bigger organization. Monitoring a person's history, location, packets, and frames, for instance, and how they access the internet. Figuring out what an user's expectation of security also is indeed an essential thing in discovering a remedy for this issue. Tapping another connection or service without consent is labelled snatching.

The sensitive information is indeed the topic of something like the confidentiality. Confidentiality is a private affair. Whatever confidentiality is to multiple individuals, the amount of solitude people are willing to forfeit either expediency or comfort, fluctuates. Similar to this, the issue of authenticity is raised and examines who really is answerable again for content's dependability, correctness, and legitimacy. The provenance of a content and the individual who is responsible of authentication mechanism should be accounted for whenever executing network penetration testing. The issue of what types of statistics an individual is entitled access acquire. In this scenario, this even forecasts recognizing necessary precautions against every unpredictable circumstances. Gamers who subscribe for private connectivity are doing it because gaming uses additional broadband compared to any other activity. Many persons will do almost

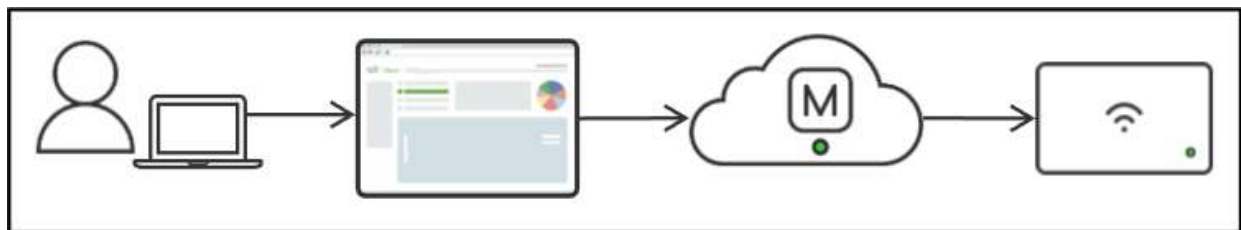
anything to get onto the network. Individuals become more conscious of the difficulties of wireless connections every day.

The main intention of this article is to strengthen the safety as well as dependability of a Private WIFI Network by acknowledging its threats, developing a De Authentication detection device, verifying the source of De Authentication Packets, and developing solutions to a variety attack that might jeopardize the privacy and consistency of user data. This article will not cause any harm to the individual as it helps to ensure the protection of WIFI networks and safeguarding confidentiality is just a hard process since doing so meant sacrificing against menaces from wireless broadband devices that are connected around each other in addition to single innovative trends. Consequently, utilizing appropriate risk evaluation and planning, security system is indeed a good approach to safeguard clients since this level of protection requisite for Private Network is completely different.

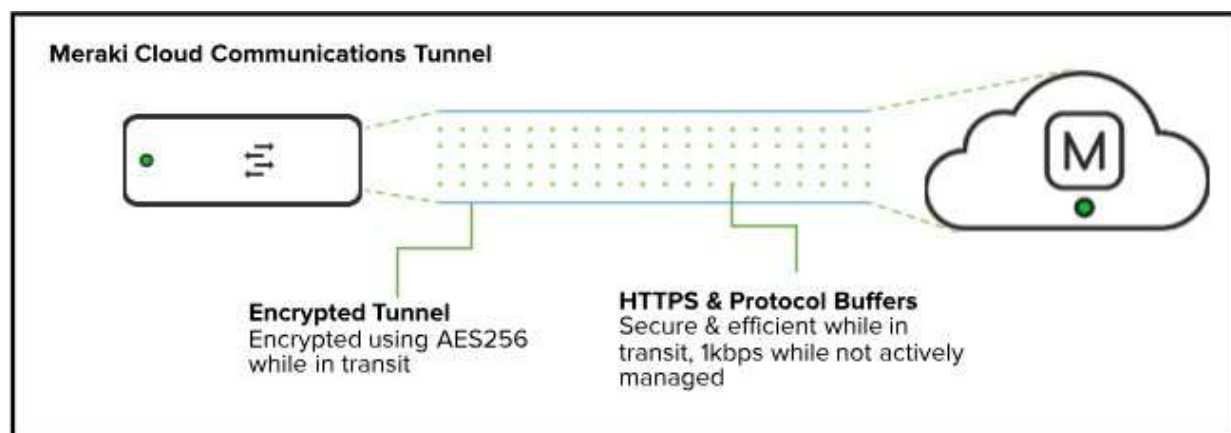
Secondary Literature Review

Case Study One: Cisco Meraki

Cloud-managed Cisco Meraki gives better insights that guarantees firm's competitiveness plus exceptionally easy maintenance. Cisco Meraki access points were particularly powerful as well as adapt to something like an user-friendly experience because of improved connectivity capabilities, growing customer capacity, as well as detailed analysis. These were manufactured with greatest possible materials. They allow unequalled transparency enabling intelligent network management and arm security analysts including in network knowledge. (Jiri Brejcha, 2020) The comprehensive and user-friendly Meraki Dashboard gives you complete transparency into your network's clients, the equipment individuals are employing to connect to it, in addition to the activities that are executing upon these gadgets. Additionally, it enables you establish user activity controls to boost both network security as well as the user engagement. Meraki actually is a service provided by Cisco for management of the networking devices like router, switches by providing them a secure platform.



Meraki employs its own compact encrypted connection featuring AES256 encryption to interconnect devices to the internet enabling administrative packet forwarding. Meraki exploits HTTPS as well as protocols buffering on the inside of the tunnel for just a reliable and safe alternative, restricting data transfer speeds to 1 kilobits per second for every devices although the device isn't being continuously maintained.



The Meraki backend maintains devices parameters as more than just a receptacle. The containers gets modified and afterwards delivered towards the related device through a secured network whenever a device specification is amended by an accounts administrator through the use of the portal or Apis. The container simultaneously refreshes the Meraki clouds with its backup as well as redundant modifications. Whenever some fault or vulnerability regarding outdated firmware or software found, it calls the devices the update the latest configuration so that it will make the firmware and software of WIFI more secure which helps to protect against different threats. (Lawrence, 2016)

Meraki's web server as well as computers share information with one another and with the dashboard and used an occurrence remote method call RPC. When calls are transmitted to Meraki hardware components enabling information gathering and setup rollout, such devices utilize as even the client or recipient upon behalf of the Meraki cloud. Settings can always be carried out in the internet first before endpoints are indeed operational or perhaps even installed geographically because the software system acts as originator. (Cisco, 2020)

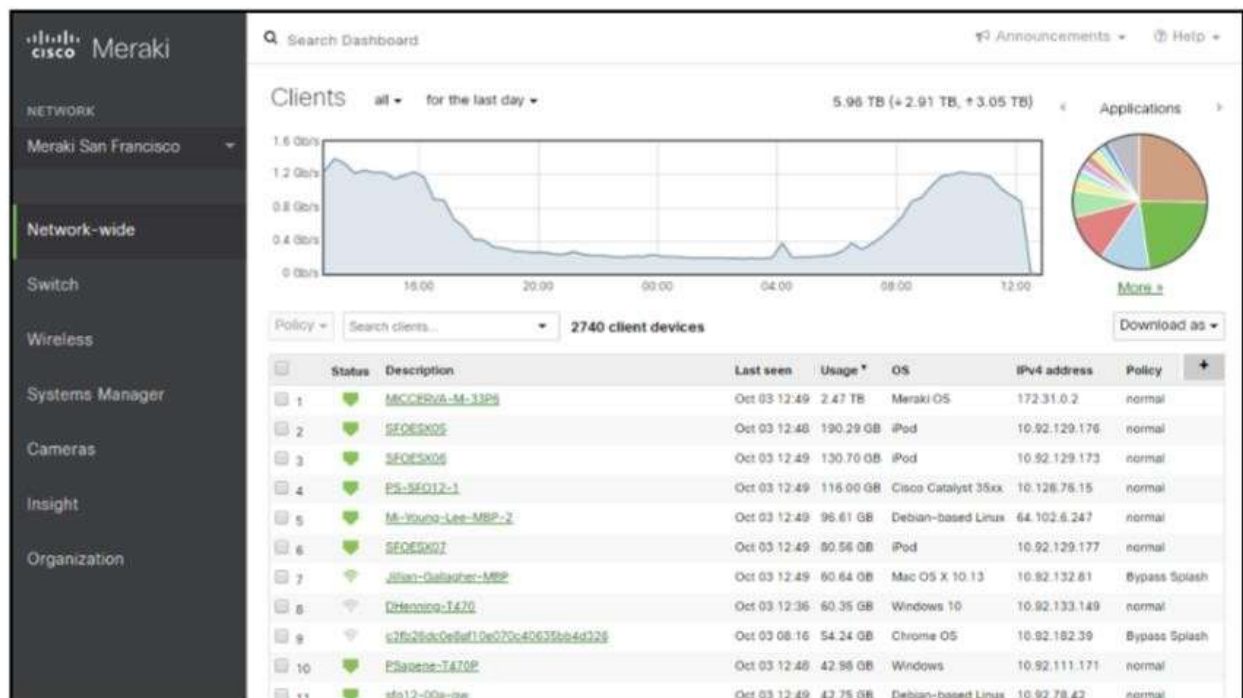


Figure 12: Dashboard of Meraki

How it actually provides security?

User privacy is Meraki's top priority. With elements including two-factor verification for panel accessibility and then out cloud- based structure, significant expenditures have been made in systems, methods, and innovations to keeping both clients and corporate connections secured. Meraki collaborates from outside

entities that add supplementary protection on upper edge of the existing security companies that it and Cisco have. The Meraki security package offers measures like regular third-party vulnerability assessments, test automation, and infrastructure screening. In order to maintain the architecture and users secure, Meraki also launched a vulnerabilities incentive programs including both software and hardware. This initiative incentivizes outside research to work with their security department. Meraki's intelligent monitoring architecture gets rid of the issues associated with regular administration, test execution, and governance complexity that result in weaknesses. System administrators will embrace the user-friendly and economical security mechanisms, whereas chief data officers would value the robust and perfectly alright administrative tools, identity safeguards, inspections, and program management. The time it necessitates to identify infrastructure issues can be significantly decreased with the aid of the advanced analytics Meraki Insight provides. Because of lightning-fast debugging, the IT staff is able to proceed directly to the settlement step. As a consequence, users can guarantee that they will be happy with the results. Additionally, Meraki Insight provides information on program trends as well as helps to anticipate potential issues. (Inc, 2021)

Successful Security Provider Reason



Figure 13: Successful Security Provider Reason of Meraki

- **Cloud Managed Security**

Switching, wireless Local area network, and strong firewall defense are now all characteristics of the Meraki. The systems effectively defend remote places, network infrastructure, and decentralized domains through the use of Unified Threat Management. With the aid of a

straightforward Cisco Meraki dashboard, together all appliances may be easily integrated and monitored from whatever the place is.

- **Upgraded network**

The Cisco Meraki WIFI networks don't require any special software solutions and controller equipment to be deployed at your various physical places. Meraki base stations offer an incredibly wide network coverage and unmatched efficiency since they are designed with improved CPUs as well as a professional security radio. Automated deployment of firmware and security updates engage actively while making the consumers informed.

- **Simplified Network Management**

It only takes a couple of minutes to connect in, established, and operate Cisco Meraki routers. All that is required to setup the routers is a website. These were expandable anywhere at time and provide a reliable functionality for networks including all dimensions. In addition, especially theoretically for the secure links, the routers are completely interchangeable. The network managers' precious information is liberated owing to a simple remote monitoring, allowing them to focus more on projects with a greater significance.

Case Study Two: Webroot WIFI Security

The newest VPN for users is Webroot WIFI Security which without restricting users or their equipment, keeps the user online safety at homes as well as on public Wi-Fi networks. Webroot WIFI Security shields the connections against cyber attackers, internet provider, focused adverts, and several others who seek to eavesdrop, analyze, or collect private information, regardless the users is doing online shopping, maintaining banking or social media profiles, or posting pics among family and acquaintances. The very first activities that typically do while stepping into a hotel would be to access to the WIFI connectivity. Despite the fact that it appears like a good deal, it is not a smart option to sign into a internet even without Webroot WIFI Security app. The hacking collective, who attempts to attack users computers after they have linked towards the house's WIFI, was claimed to be have returned in July by ZDNet. As soon as the WIFI has been compromised, a hacker organization can use a variety of spoofing and psychological manipulation strategies to attack specified PCs. Everyone can use a Webroot WIFI Security to assist keep safe and prevent prospective assaults, and travelling and accommodation are just two examples. Utilizing a WiFi can conceivably expose the information you're transmitting over through the internet at jeopardy, either you're browsing your corporate data when freelancing, looking at Facebook from unknown WIFI, or using an unsecured WIFI at your neighborhood. (Max Eddy, 2020)

Web blocking is another feature offered by Webroot. Although it may appear to be a remote management option, isn't. The Brightcloud Threat Intelligence system, that filters out harmful websites, will be utilized by the VPN when it becomes active. That really is helpful, notwithstanding the fact that modern internet platforms come with created monitoring, that makes it somewhat unnecessary. While employing a VPN,

users wish to be confident that it is effective and is not exposing DNS or IP address details. While using Webroot, DNS queries are routed to multiple hosts, as well as the IP address is adjusted.

How it will Benefits Users?

- ✓ It provides the more secure connectivity without slowing down the users internet experience
- ✓ It really is very effortless to setup, activate and to use for monitoring
- ✓ It helps to keep the users safe online by using the technique called Advanced Web Filtering technique which will aware to access the malicious sites and even from spying.
- ✓ It helps to hide the IP Addresses of the users
- ✓ It provides advanced protection within network like WIFI by enabling the secure browsing in order to preserve the user identity and privacy simultaneously.

Successful security provider Reason

Finest protection is provided by architecture, yet Webroot WIFI Security would still be simple for using. Only with single touch, security mechanisms are instantly enabled without even any complication or missing procedures. Users of Android, Mac, and Windows devices can utilize the distinctive "killswitch" function of Webroot WIFI Security for enhanced protection. The kill switch restricts transfer of information and data across an unsecured network whenever the VPN connection has been lost until you're back linked to the VPN. By hiding the geolocation, Webroot WIFI Security additionally contributes to the protection of user privacy. The exact location can be determined by sites, who then employ this information to monitor user surfing patterns. Webroot WIFI Security could give the appearance that you are in any of the and over 30 countries wherever the VPN locations are positioned. Internet Blocking enabled by Bright Cloud Threat Intelligence is another feature of Webroot WIFI Security. The financial data, credentials, and private documents are protected from becoming misused by this function, which adds an additional degree of security. With protecting users against accessing harmful or dangerous URLS suspected to be connected with ransomware, fraud, keystroke logger adware, and malware attacks, Webroot extends far beyond competing VPNs. A function which the user could activate or deactivate is web filtering. Some of the most innovative and safe VPN services that are available today is Webroot WIFI Security, due to the strength of finest threat intelligence as well as the confidence of customers. Webroot does have a longstanding experience of preserving the confidentiality of its users, and are pleased to demonstrate this commitment in the Virtual private network market. (Cathie, 2022)

Case Study Three: Net Gear Armor

The NETGEAR routers network already has NETGEAR Armor supported by Bitdefender™ preloaded. Just tap once to turn it on in the Intruder or Client devices app. Armor dynamically adjusts and assists in preventing hackers from targeting not just to PCs and yet also cellphones, tvs, central locking, and

surveillance cameras. When NETGEAR Armor discovers any perceived risks, it promptly warns users. Users can quickly ban shady devices from connecting to the network, assess your degree of protection, evaluate the security score, as well as receive guidance on how to keep the gadgets as well as necessary details safe. This aids in ensuring that the internet traffic is kept secret. Employ NETGEAR Armor to enable it and increase the user's sense of security and tranquility. Users won't need to be concerned about the internet privacy when using Bitdefender VPN. VPNs secure all data traffic in order to safeguard the confidential internet behavior. When connecting to a Wireless router, safeguard the identities, download files, especially confidential banking details against cybercriminals. Every smart phones including linked PCs in the house are secured by NETGEAR Armor. The enormous quantity of IOT systems, including thermostat, video surveillance, alarm systems, lighting controls, and much more, are going to be accessible in along with mobile handsets and desktop pcs. Inside a dedicated app, it make easier to control sensitive information, suggestions, and warns from hackers. Evaluate the private security rating, check which pages as well as Addresses is blocked for unusual activity reason etc. An IoT device can be compromised by an attacker, giving them reach to the personal information. For instance, a compromised baby monitor enables strangers to eavesdrop on the users as well as, unsecured printers might reveal the confidential files, and vulnerable surveillance cameras permit intruders to look about the house. All of your PCs, cellphones, including Connected devices are routinely scanned for any known vulnerabilities by NETGEAR Armor. Armor locates weaknesses including default settings, short and delicate passwords, recognized software issues, and network connections. Prevent network assaults on the wifi network by putting a halt to them. All of your devices connected are scanned by NETGEAR Armor for security weaknesses of WIFI network like possible vulnerabilities, inadequate passwords, and unencrypted or insecure interactions. All outgoing data transmission is screened for risky or insecure websites using our Address blocklist to guarantee secure navigation, that including banning any scamming or counterfeit domains. As a result, you can be confident that you will be secure on any page. Get immediate notifications when devices that are not detected by the connection are barred from connecting. You can keep track of what's occurring on your wifi network with NETGEAR Armor. You'll get prompt updates if dangerous risks are found or stopped, enabling users to conduct appropriate immediate measures. (MARK B, 2022)

Primary Research

Considered Methodology

Three distinct software strategies in altogether are vital to the completion of my research on WiFi security. Our proposed research will implement a different methodology, which will undoubtedly be determined by the objectives of the thesis. Before choosing a particular topic, the researcher must decide what it is that he genuinely wants to learn. Should we conduct a questionnaire in order to collect statistics? Is the representative sample for our investigation exceptionally large? There are different intentions and explication over using Agile Methodology

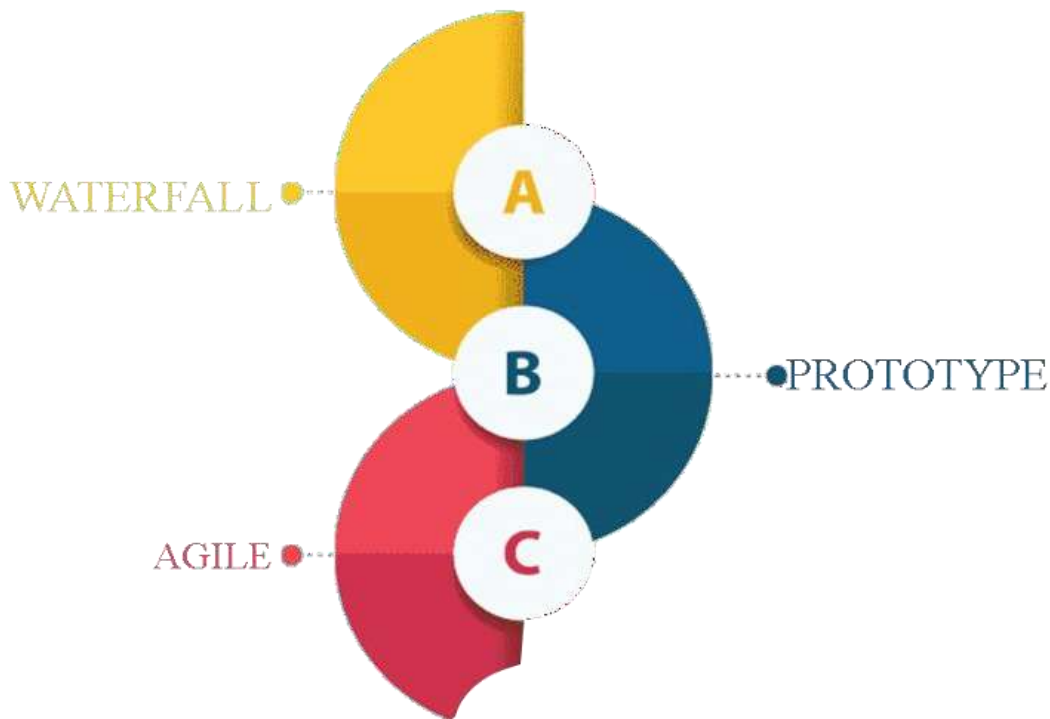


Figure 14: Considered Methodology

Waterfall model

For the comprehensible as well as reasonable approaches to project management waterfall model must need to be used. A progressive creative procedure is the foundation of the waterfall model, a product development strategy. The waterfall approach, which was conceived as a framework for the software development process, is excellent for small initiatives where criteria can indeed be accurately outlined up advance. In order to jump into the next step, the previous one must need to finished. A evaluation is carried out at the conclusion from every stage of project to assess if indeed the project is proceeding as planned and if it should be carried or aborted. (GeeksforGeeks, 2018)

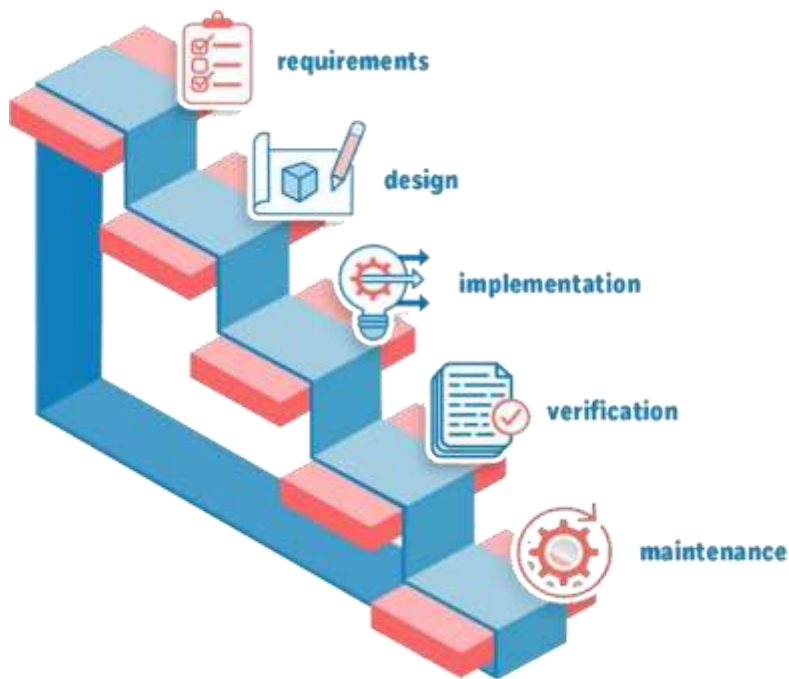


Figure 15: Waterfall Methodology

Prototype Model

The fundamental concept behind the concept paradigm is to create a throwaway sample is created better comprehend the specifications instead than limiting them even before concept or scripting could be accomplished. In accordance with the requirements that have been generally listed, this prototype was designed. Considering sophisticated as well as enormous processes outside of an existing framework or operational approach that effectively determine specific specifications, prototyping is an appealing choice.

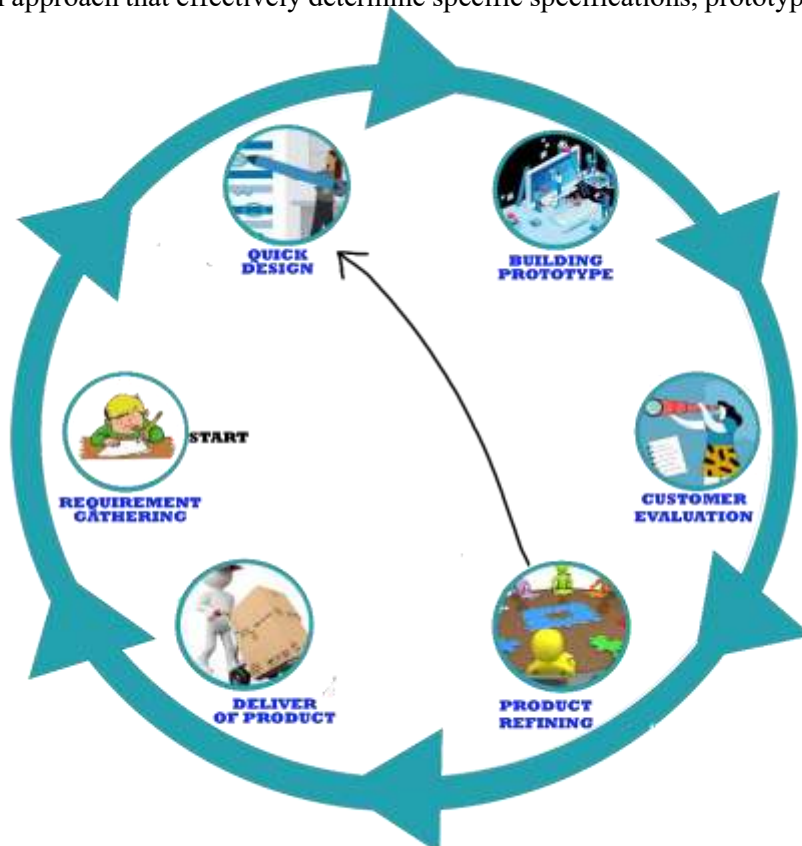


Figure 16: Prototype Model

For the solution of the proposed problem, the prototype model can be used which is composed of different effective steps. First step is to Identify the proposal's primary objective. Alongside, the researcher need to start commence the early sketching. Users may also be conscious of the issues with the layout and desire to seek into alternatives. So, it begins out whilst reducing the functionality to keep it simple. The account is taken into the consideration that this iteration will be enhanced as the project goes on. Now the next step is to develop the arrangement on article. When communicating with relevant teacher, explanation on enhancements is notified. Regarding input, any administrator academics is mentioned. After talking with teacher, the design is revised. form paper to machine for development. For the prototype different resources are used like Node MCU, Bread Board, Jumper wire which later will be used for development of the engineered product. A model of a final version is initially developed, validated, and propelled forward during response to client feedback till a best end sample is developed, that functions as fuel for the actual device's advancement. (Sarah Lewis, 2018)

Agile Model

Implementing the agile paradigm is quite versatile. It primarily comprised five sections. Utilizing a shared platform, individuals from all around the globe are now using ideation to collect the elements that should be incorporated into the program in their specific needs.



Figure 17: Agile Model

Finally, the fundamental concept as well as the pertinent paperwork are created and stored on. Those kind of are administered by the supervision of a community and made accessible to any determined programmer from around the globe upon application. The authors give their edition and system software after certain

modifications. Others provide valuable opinions or file bug reports. After being repeatedly verified, the source codes then adjusted as necessary and combined with both the actual source code. More than a specific amount of time, the program gradually then well developed. (Kate Brush & Valerie Silverthorne, 2017)

Selected Development methodology

Agile methodology

At last, the Agile Methodology is selected for the development of this project after the deeper analysis of the different advanced technology. Multidisciplinary, cross-functional, personality teams functioning around agile approaches are meant to produce the appropriate products while permitting for superior client input as well as reassessments when necessary. Agile methodologies typically endeavored to abbreviate deliver products in order to guarantee the fewer component portions of the product make it to field, letting customers to submit comments close to the start and guarantee that solution they actually receive satisfies its requirements. Crews should indeed produce end-to-end operational systems, interfaces, as well as other outputs that will have an effect on users—not just about the technological components—because agile emphasizes groups on providing software quality. On what they have creating, who is responsible for what, as well as how the program will be built, the colleagues should be in agreement.

Phase of Methodology

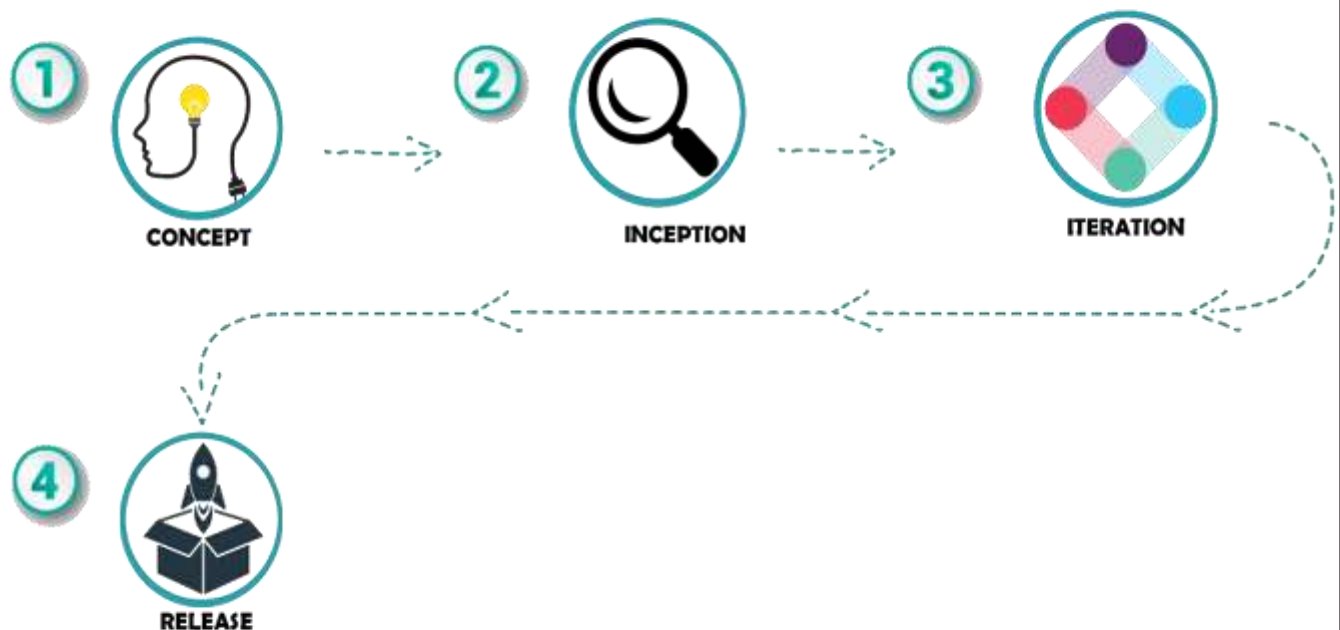


Figure 18: Phase of Agile Methodology

- **Concept**
The initial step of this methodology is conceptual designing by scoping out the process prioritizing the project. Here, total time as well as the time in order to complete the project is prioritized. Later on, this step also helps to regulate which project is appropriate for research as well as effective and problem solving.

- **Inception**

In this step, how to complete the project by selecting right tools, approaches is figured out. Requirements of the customer is noted here. Different responsibilities and roles is illustrated by extending each tasks which needs to be completed.

- **Iteration**

Now, after defining the project layout, a workflow is developed from start to finished which consists of the different step which is explained below:

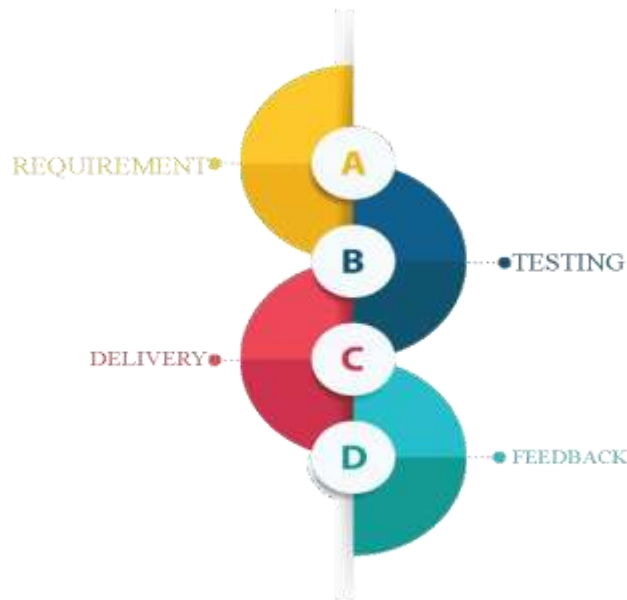


Figure 19: Iteration of Agile Methodology

- **Requirement**

To satisfy the requirements of the user by analyzing their demands the prototype of the product is well documented. Here, a effective research will be done on the development of the de auth detector including the dependability and extent of the project.

- **Development**

Now, according to the requirements set by the users and well as the problem, here the product is developed

- **Testing**

This project consists of different features and services. So this features must need to be tested to test it's effectiveness. So in this step, QA testing is done to verify the different features and services.

➤ **Delivery**

From requirement phase to testing phase now finally it's time to produce the ready to go product. Here, the product is delivered by developing the fully functional product

➤ **Feedback**

This is the last and most important step, where different feedback are collected so that the product will be refined next time in coming iteration.

➤ **Release**

Here, the product is gradually released after doing product iteration. Here, product final testing is carried out so, that it will be easier to note out any bug or vulnerability in source code or the problem in the product. After testing the product, finally the product is released and ready to serve its services on fields.

Survey Result

Pre survey result

The result obtained from the pre survey illustrates that, the De Authentication Detector would be so much admired by the people because of its actual work and power to detect the De Auth Attack on WIFI Network which would be used to aware the owner about it. The below pie chart shows that more than 70% of people don't know about the de auth detector due to the lack of knowledge of the technology and unavailability of the internet access to the individual. But there are also some people who do support the concept of de auth detector as reveals by the below pool.

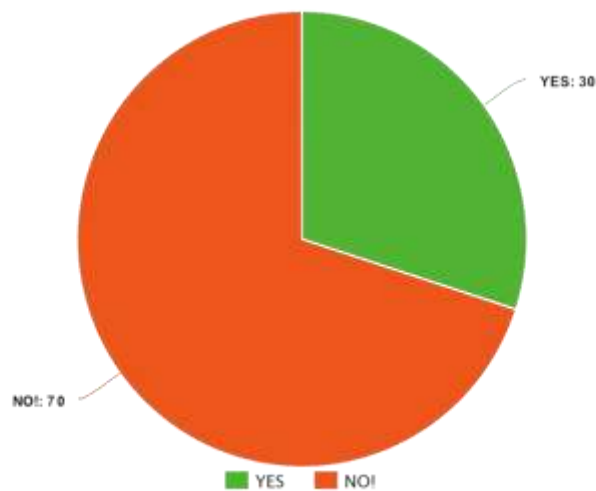


Figure 20: Pre Survey Result

Post survey result

The below figure illustrates the extensive consequences and also the respond to the post survey. Most of the people in the de auth detector acknowledged optimistically to the post survey finding of the initial prototype which is successfully carried out within some of the people.

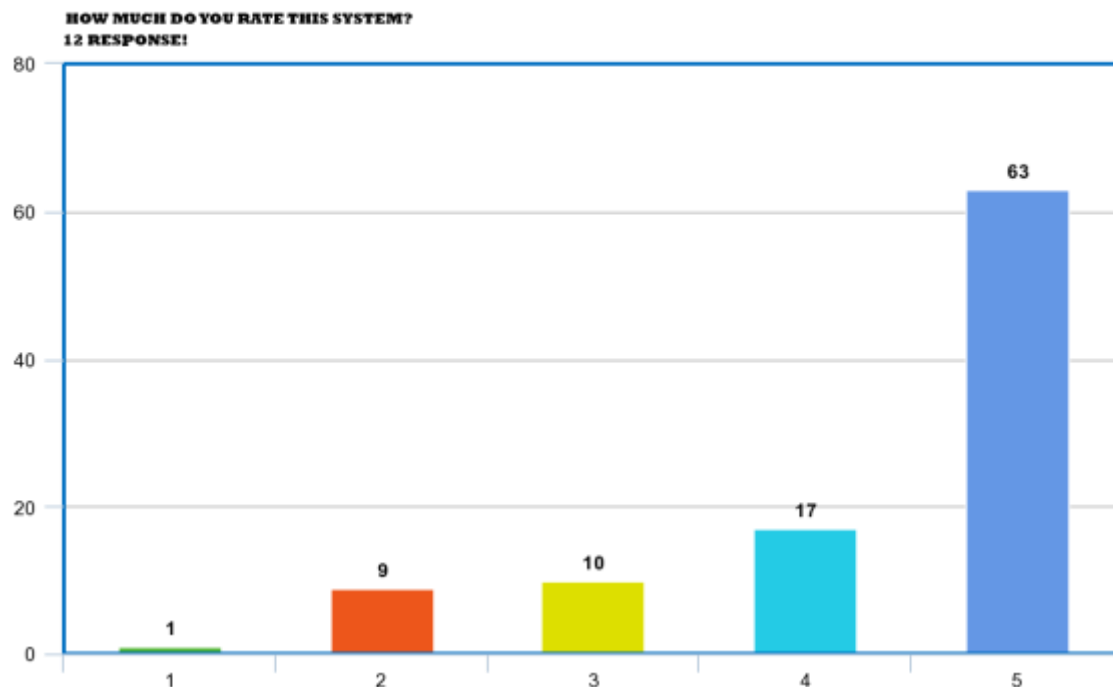


Figure 21: Post Survey Result

Tools

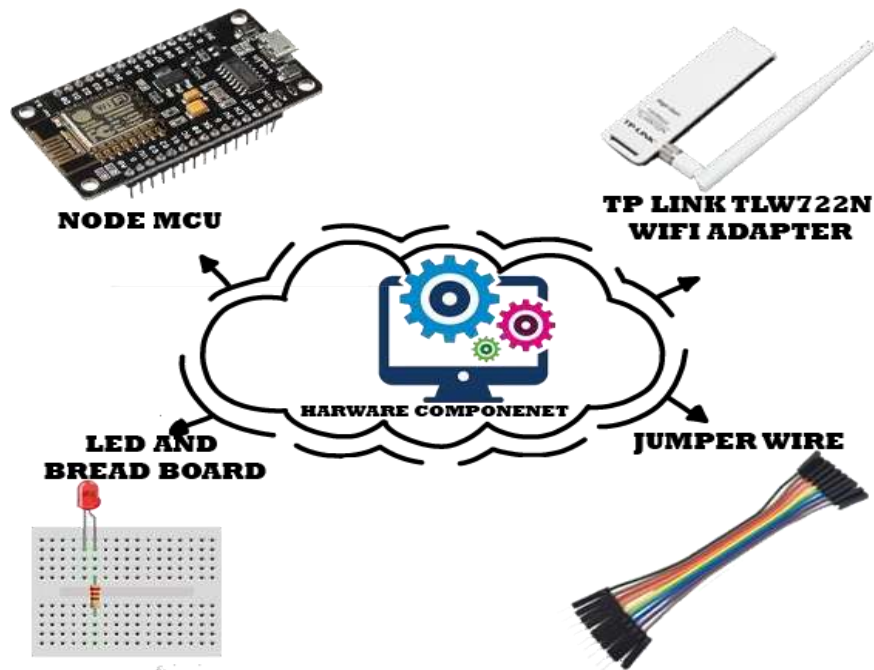


Figure 22: Tools

Node MCU

With the rise in internet the rise of IOT application is also going on where the most important part is to connect the different IOT object. For the development of the solution of De authentication detector this device i.e. Node MCU is needed which helps to connect the different object together and promotes for the transfer of the WIFI Protocol by detecting them. A use device is used to connect the Node MCU to the PC which helps to inject the source code for the detection of packet and responds accordingly by lighting the colored light. (mario guzman, 2020)

Benefits

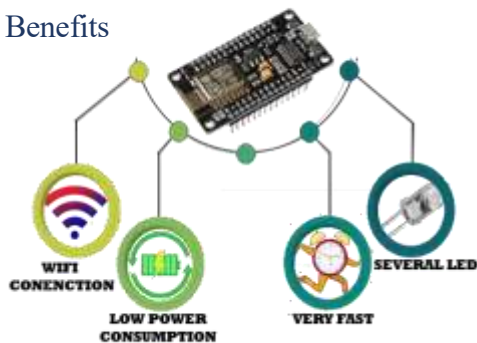


Figure 23: NODE MCU Benefits

- ✓ Support the connection of WIFI Networks
- ✓ Portable and Low Power Consumption
- ✓ Very Fast and Highly Secured
- ✓ Several LED Light for Signal

Jumper Wire

This wire plays vital role for the prototype development as it does not required soldering to connect different point. It is used to connect LED to the Node MCU device. It actually used within breadboards so that, the structure can be changed with requirements. This wire is manufactured in different colour which is only used to distributed the points accordingly.

▪ Benefits



Figure 24: Jumper Wire Benefits

- ✓ Improvement of quality
- ✓ Reduction of Short Circuit

TP Link TLW722N WIFI Adapter

This adapter is used as a primary tool for the injection of packet which supports packet injection. This can be used to generate the De Authentication Frame. The frame generated by this adapter later will be used by the Node MCU device to detect the frame and indicate it by lighting the LED light.

▪ Benefits

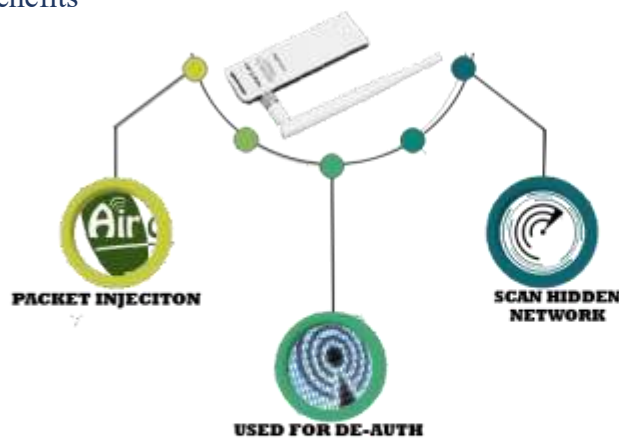


Figure 25: WIFI Adapter Benefits

- ✓ Support of the Packet Injection Mode
- ✓ Can be used for Scanning the Hidden Network
- ✓ Used for De Authentication Attack

LED and Bread Board

The Bread Board is also used for the project prototype. It is used to assemble the hardware equipment which also helps to prevent from short circuit. The LED will be used here to light the different colour whenever detecting the De Auth Packet or when ever the device connected to the WIFI Network.

■ Benefits

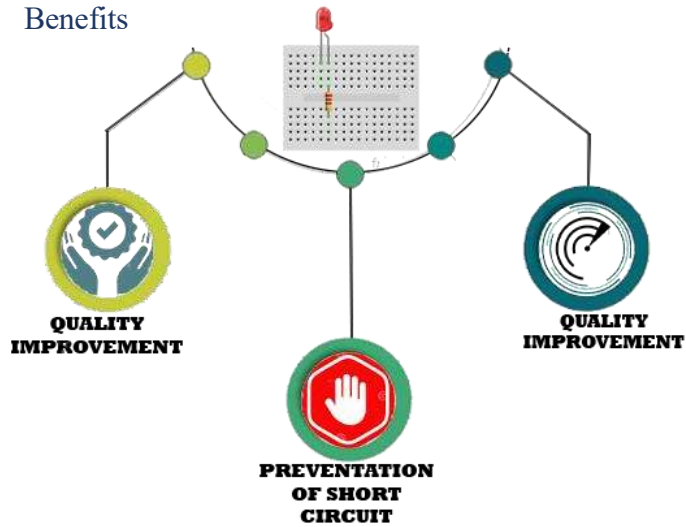


Figure 26: Bread Board Benefits

- ✓ Improvement of Quality
- ✓ Prevention of Short Circuit
- ✓ LED used to give the specific Signal about what happening

Technology



Figure 27: Technology

Arduino IDE

It is a software requirement for the development of the project prototype. This IDE allows to edit and write the code. It is used to inject the code withing the Arduino hardware to perform the specific tasks. It also makes easier to communicate with the hardware used. The benefits of this IDE is that it can be used within any Arduino board. (Liam Aljundi, 2022)

■ Benefits

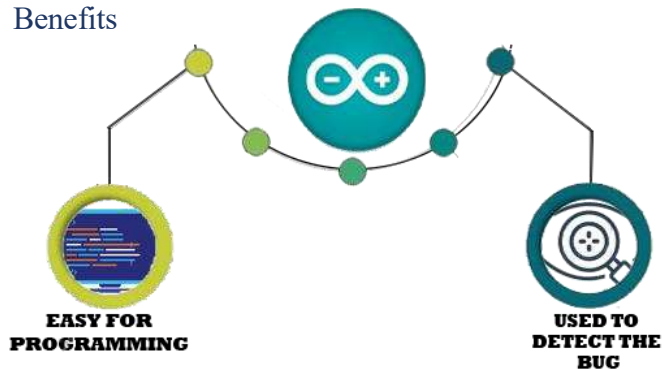


Figure 28: Benefits of Arduino IDE

- ✓ Easy For Programming
- ✓ Can be used to decode the BUG

C Programming

All the code for the detection of de auth frames are written on C Programming. The reason behind the selection of this language is because it can be easily supported by any Arduino board and the compilation speed of the C Programming is fast.

▪ Benefits

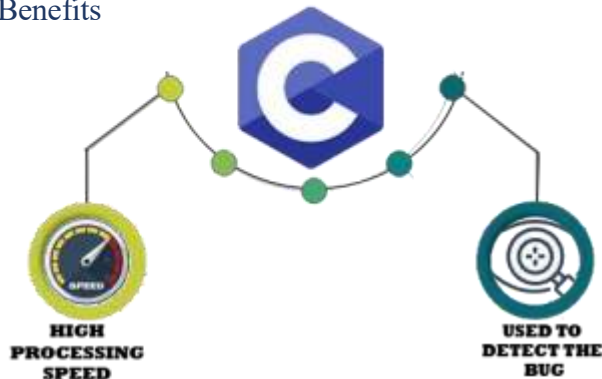


Figure 29: Benefits of C Programing

- ✓ Very high processing speed
- ✓ Helps in debugging

Airmon-NG

This software allows to scan the nearby WIFI SSID which is broadcast openly. This frame work allows to select the specific WIFI SSID and shows the connected device within it by showing the MAC address. It helps during the packet injection of De Auth Frame from WIFI Adapter towards the router where the Prototype will be used to detect the De Authentication Attack by lighting the LED. (Said, 2020)

▪ Benefits

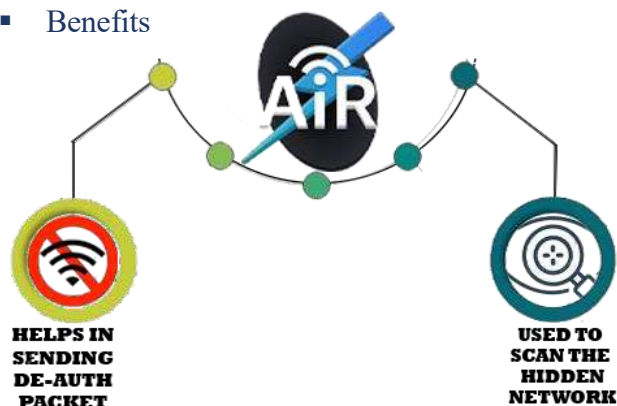


Figure 30: Benefits of Airmon-NG

- ✓ Helps to send de auth packet
- ✓ Helps to scan the hidden network

Kali Linux

Linux is used here for the programming of NODE MCU. It is also used to check the vulnerability of the network using different framework available.

- Benefits

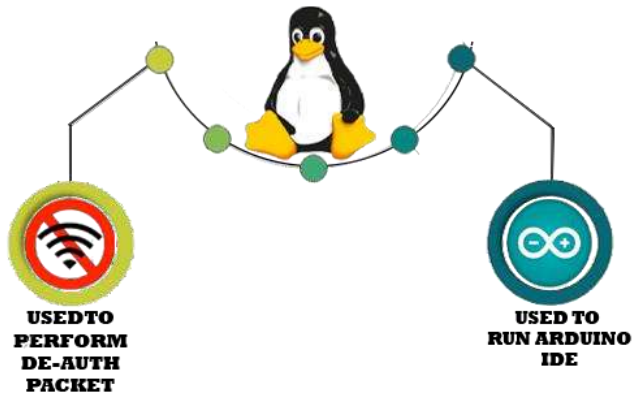


Figure 31: Benefits of Kali Linux

- ✓ Helps to perform the De Auth Attack
- ✓ Used to run the Arduino IDE

Virtual Machine

This software helps to run the multiple application at the same time. It is used here to run the Kali Linux machine virtually which will be used for the Project Development.

- Benefits

- ✓ It helps to run the Kali Linux
- ✓ Helps to run the different software at a same time

Techniques for Better Improvement



Figure 32: Technology for Better Improvement

Security

Integrity as well as security usually go hand in hand. System reliability and stability is adequate to avert system failure, illegal accessing to proposed system, computer infected by viruses, and protection of the confidentiality of information and data that is entering the system. In order to keep the data secured and information safe information security is important. This play important role withing the organization to protect the data and information against intruders from the technical system. Data is everything which can compromise the user privacy so it's better not to provide the recorded data to unofficial or unwanted reason. Encrypting sensitive information first is technique to make absolutely sure it does not reach the incorrect hands. The cost of resources needed for decryption of encrypted information might be sufficient to discourage a hacker from taking further action. (Dan Rafter, 2022)



Figure 33: Security

Numerous solutions are available to assist users in encrypting the information as well as traffic. System security is designed to make sure that service is delivered despite facing challenges. System security can be obtained through the use of a variety of strategies, such as strong encryption system, strong passwords. System security's main goal is to restrict system vulnerability to real potential threats while also guaranteeing that produced systems offer protection from them. In order to find and eliminate these vulnerabilities in systems to the recognized platform risks, techniques are implemented across all stages of system development. Data security is to the entire measures the firm uses to prevent the unintentional or intentional access, manipulation, theft, sale, or even other exploitation of the content they have on hand. Observing how data receives as well as departs after it has been stored. What sources are there for consumer data? These ports of entry and departure may reveal to just be significant weaknesses and should be watched. Ensure the information has been encrypted and that the user has taken the necessary steps to protect it if it's necessary to transmit it to the receiver.

Availability

For the proper access of the data and information of the user and system different software are used and are employs within the system. Because of this, it is easier for the effective use of the data and information gathered. Availability generally means the dimensions of the system to perform any activity whenever the users request to do. A specific program is written to make sure that the data is safely stored within the system whenever the program failure is occurred within the proposed system.

User experience

User experience is very important for the success of the system or any program. The proposed system is very easy to use and it only required to connect it to the WIFI Network and a power supply. Whenever the de auth attack occurs within the system it gently notifies the user by lighting the LED which make user to aware to implement the more secured security and encryption standards. Very fast performance, easier to use, efficient and portable to carry make the experience of the user really good.

Attributes of Technical Quality

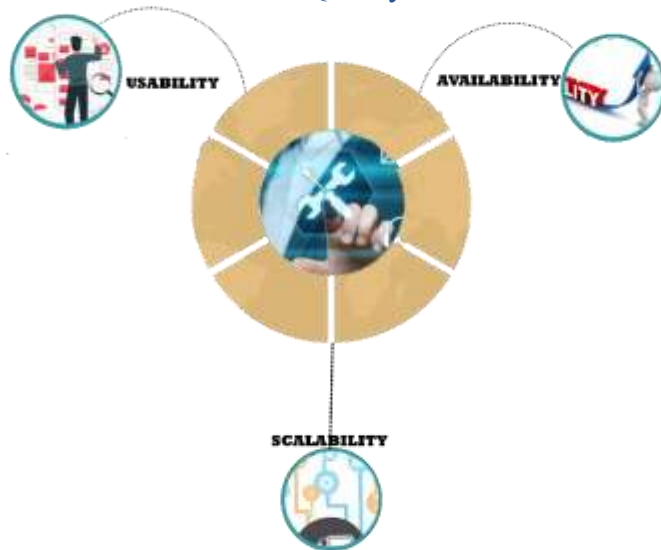


Figure 34: Technical Quality Attributes

Findings

Overview

The main aim of this report is to make Private WIFI Network more secure and reliable by subjecting it's different security issues, development of De Authentication detection device, verification of the source of De Authentication Packets and solution for different attacks which will compromise the integrity and confidentiality of the data of users due to the weak implementation of security system in WIFI. There are altogether of three components are build of the main tasks namely: structural factors should be taken into account while creating a prototype system for choosing or designing security measures for WLAN, the execution flaws which might impede the execution of WLAN authorization and access controlled assurance in a particular WLAN and level of vulnerability in the WLAN encryption suite, authenticity as well as security systems, and program that implements authenticity and security systems in a WIFI is exposed by common threats.

To comprehend the key concepts inside this subject area, the research did a thorough literature review. Finally, fundamental voids were found and a hypothetical design was developed. There would be problems that needed to be resolved. As a result, the research's qualitative as well as literature assessment as well as survey foci were chosen. The assault strains of security mechanisms and configurations that could be deployed in WLAN were examined using a technique for analyzing assault responsiveness known as the De Authentication Detector. The algorithms were devised as a result of the survey method and threat resistance study. For testing, a de auth attack removal sample system has been created. The architecture

established includes the construction and deployment of security mechanisms for WLAN security, according to the findings of various validation methodologies.

Research Question Conclusion

This investigation is really beneficial because it offers a number of chances for further inquiry. The author summarizes the main study topic and its primary findings in this part, which together provide substantial improvements. Throughout a survey method, literature review and evaluation, professional elaboration, and analytical approaches, the study tried to provide answers to these concerns.

Question One

Which structural factors should be taken into account while creating a prototype system for choosing or designing security measures for WLAN?

Through literature investigation, the pertinent design patterns for creating a prototype system for the choosing or architecture in addition to the implementation of security mechanisms for WIFI authorization and management system was identified. In addition to making the elements obvious, but it is also possible to determine the severity of each individual parts value as well as the total impact of a mixture of parameters. Through with a sample research, the corresponding security configurations as well as capabilities were discovered. For every one of the design features, dynamic programming tables that correspond security mechanisms as well as customization to security requirements was created.

Question Two

What level of vulnerability in the WLAN encryption suite, authenticity as well as security systems, and program that implements authenticity and security systems in a WIFI is exposed by common threats?

Several vulnerabilities exploited to launch attacks on WLAN encryption suite, authenticity as well as security systems, and program that implements authenticity and security systems in a WIFI was examined. The results from this examination shows that vulnerable security features as well as configuration mechanism were exploited over the WIFI Network system.

Question Three

What are the execution flaws which might impede the execution of WLAN authorization and access control assurance in a particular WLAN?

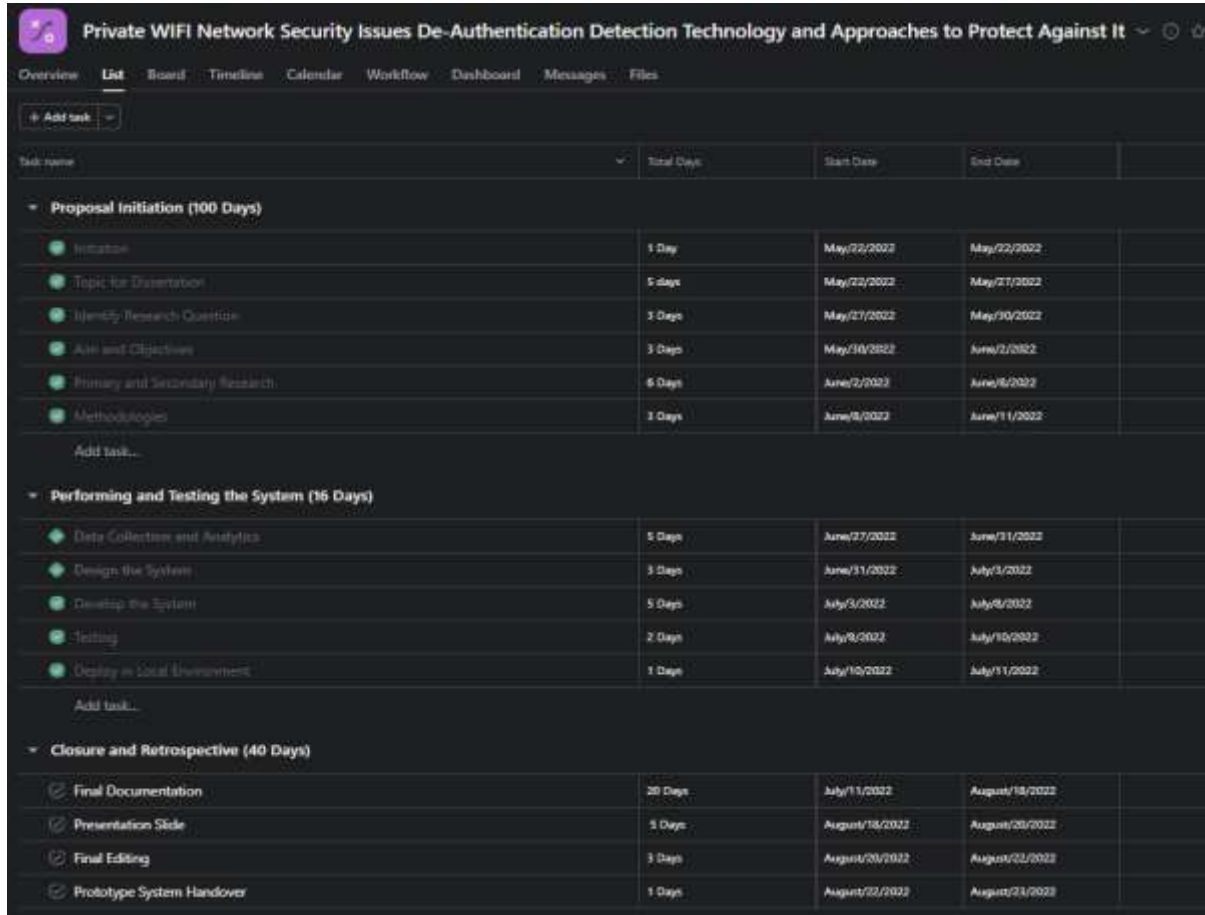
The outcomes of a survey method reveal that numerous individuals had set up identification and wireless route security procedures which are extremely susceptible. This indicates that a large number of these solutions are vulnerable to intrusion, sniffing of sensitive information including identification sessions, as well as WLAN masquerading and replication. The study also discovered several security settings and characteristics that are applied to different objects that affect WLAN protection throughout verification and control systems.

Risk Plan

Issue	Impact	Priority	Status	Resolution
Research topic Selection	High	High	Solved	Consulted with the teachers and conducted a feasibility study on many topics
Literature Review Writing	Medium	Medium	Solved	Suggestions from instructors, multiple online classes
Finding Research Sources	High	High	Solved	Researched content in different sites, book, journals, articles
Requirement Change	High	High	Solved	Information and evidence were gathered and combined together for strong solution
Complexity in Making Diagrams	Low	Medium	Solved	Use of Photoshop for Infographics Designing
Issue of Plagiarism	High	High	Solved	Proper Citation and Reference were done in the copied text

Figure 35: Risks Plan

Project Plan



The screenshot displays a project management interface with a task list. The project title is "Private WIFI Network Security Issues De-Authentication Detection Technology and Approaches to Protect Against It". The interface includes a navigation bar with options: Overview, List, Board, Timeline, Calendar, Workflow, Dashboard, Messages, and Files. A "Add task" button is visible. The task list is organized into three main sections: "Proposal Initiation (100 Days)", "Performing and Testing the System (16 Days)", and "Closure and Retrospective (40 Days)". Each section contains a list of tasks with their respective durations, start dates, and end dates.

Task name	Total Days	Start Date	End Date
Proposal Initiation (100 Days)			
Initiation	1 Day	May/22/2022	May/22/2022
Topic for Dissertation	5 days	May/22/2022	May/27/2022
Identify Research Question	3 Days	May/27/2022	May/30/2022
Aim and Objectives	3 Days	May/30/2022	June/2/2022
Primary and Secondary Research	6 Days	June/2/2022	June/6/2022
Methodologies	3 Days	June/6/2022	June/11/2022
Performing and Testing the System (16 Days)			
Data Collection and Analysis	5 Days	June/27/2022	June/31/2022
Design the System	3 Days	June/31/2022	July/3/2022
Develop the System	5 Days	July/3/2022	July/8/2022
Testing	2 Days	July/8/2022	July/10/2022
Deploy in local environment	1 Days	July/10/2022	July/11/2022
Closure and Retrospective (40 Days)			
Final Documentation	20 Days	July/11/2022	August/18/2022
Presentation Slide	5 Days	August/18/2022	August/23/2022
Final Editing	3 Days	August/23/2022	August/26/2022
Prototype System Handover	1 Days	August/26/2022	August/27/2022

Figure 36: Project Plan 1

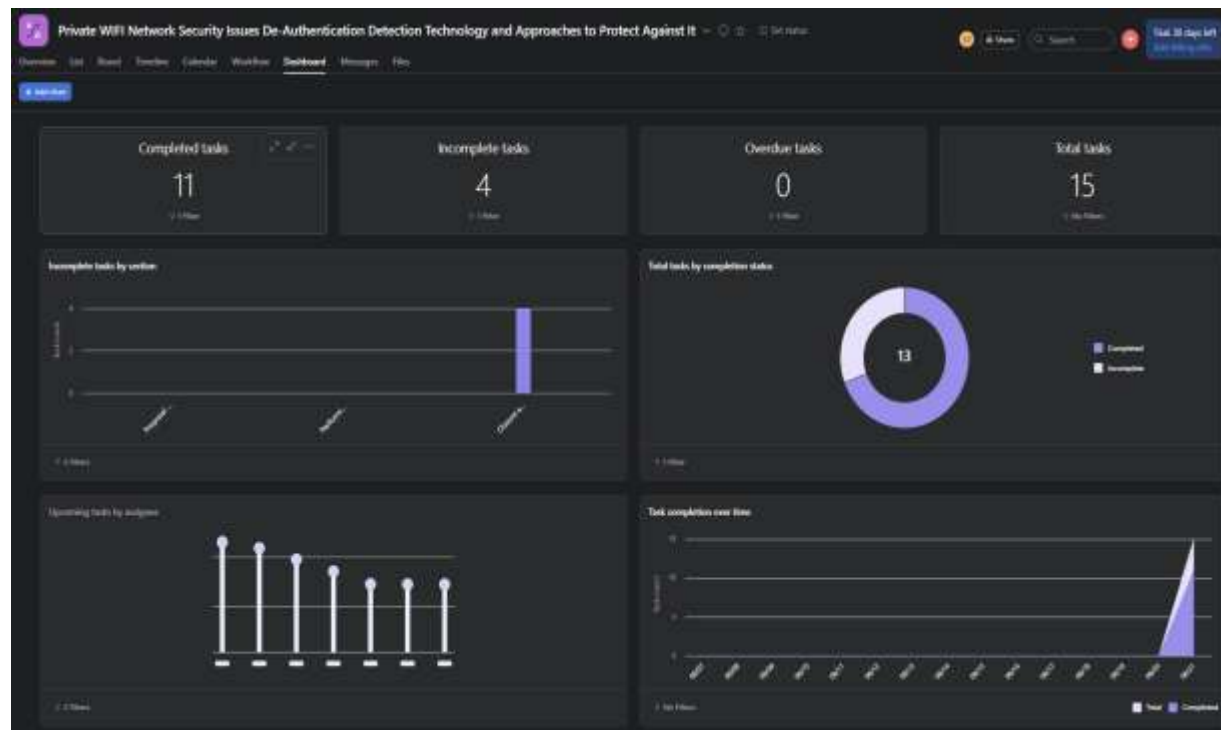


Figure 37: Project Plan 2

Future Work

Although this proposed research has contributed to the corpus of understanding in many ways, many areas still have room for improvement because of the restrictions that were mentioned. The following list includes the areas that should be addressed for future employment:

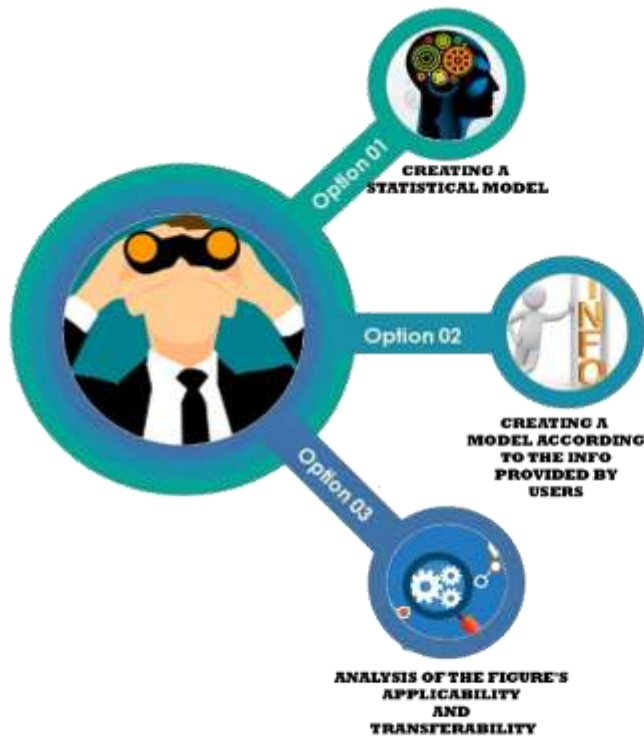


Figure 38: Future Works

Creating a Statistical Model

The study's prototype is mostly qualitative. In contrast to actually intended like these, which yields ranges of small, moderate, as well as strong, modelling techniques seem to be more reliable since they produce outputs with specific parameters.

The framework proposed Depends on Information Provided by Users

The model can be strengthened by future investigations such that it can use information directly collected off devices without posing any moral interference concerns.

Analysis of the Figure's Applicability

We can conclude that evolved framework will contribute to improving WIFI levels of security by shortlisting, layout, and arrangement of far more protected functionalities for WLAN access controls premised on evaluation results, particularly from professionals. This hasn't, nevertheless, been demonstrated. To allay this worry, it is possible to conduct an user research to evaluate the layers of protection in a group of WLANs using the paradigm and a group of WLANs not using it. Depending upon that methodology used in this study, the evaluation can be performed once again using a separate demographic of experts in other situations to increase its generality.

Challenges

Although, a lot of security measure are provided here in this report but there are a lot of challenges lies here. The de authentication detector detection time is one of them. It can detect the de auth packet but can take a longer period of time to detect it. And the prototype also needs to be connect to the WIFI Network every single time which is a real challenges. Similarly, only implementing security standards within WIFI network will not be enough to make it secure. Password length, use of special character, frequently changing of the password are the real challenges which play roles to make WIFI Network insecure if it is not given priority. Wi-Fi has evolved into a necessity both study and play regardless of whether we're in residence, and telecoms companies frequently leverage "hand-over" to W-Fi connections to fulfill bandwidth requirements.



Figure 39: Challenges

Similarly, the cost of the prototype is also higher which would be a real tough decision for the normal users to buy it. Also, hackers are going smart day by day and they are developing new practices to develop new mechanism to penetrate the WIFI Network. The prototype developed is only coded for the detection of attack from specific way. Whenever the hacker use another methods which is not implemented on prototype then it will not work which is the real challenges. So, one of the main tasks is to frequently update the source code for detection mechanism as soon as the new attack mechanism comes. However, because we require access everywhere, at all times, we frequently connect to Wi-Fi networks without giving them much thought, which makes them an ideal target for cybercriminals.

Anyone using a basic packet analyzer who uses an access point that doesn't use cryptography or requires a passcode could easily obtain your account information for critical apps and URL. Hotspots that necessitate a "passcodes for the day" typically secured, but a knowledgeable Wi-Fi hacker can use readily accessible Wi-Fi cracking tools and applications to decompress the communication. In addition, private access gadgets which are not controlled by MDM platforms that really can impose security measures increase the hazards associated with hotspots. Weather the security measures are strong or not. (Sean Wilkins, 2020)

Limitation

This dissertation primarily discusses WLAN security models and techniques that are tailored to meet the requirements of residential users. Because of having generally equivalent dimensions and ease of set-up including using, the approaches discussed in the dissertation are relevant to residential development Wifi equipment. Additionally, the very same kind of malicious attack which may seek to exploit tiny units to achieve the same goals as information spoofing and minor securities fraud kinds could also attempt to penetrate large public places and corporations. The degree of technical complexity throughout this dissertation, however, might not be appropriate for those that are not experts in the topic. As the level of progress at these facilities is outside the scope of the contained information in this document, these documents are neither in any way seek to offer anything in-depth or recommendations for giant industrial settings. Additionally, professional hackers or detectives are more often than not the cybercriminals who attempt to hack such massive systems. They vary in their tactics, goals, dependency on technology, availability of legal counsel, and control over sensitive information. In other words, they are outside the scope of this argument.

Reliability

This dissertation incorporates data and citations from textbooks, issued papers, and also other resources. Additionally, it is compared to similar works related to the same matter and in the identical sector. In light of this, it is reasonable to believe that the literature review offers a legitimate work in terms of the data. To make absolutely sure that anyone who possesses tech knowledge may easily read it.

Recommendation

According to the prototype calibration and validation, the majority of users has configured and used incredibly fragile wireless route and security mechanism components. The admin of WIFI installation must formulate a policy with knowledge of information security and the ability to forbid the installation as well as customization of extremely susceptible encryption techniques in order to prevent their deployment. This provides an immense the ability to stop WLAN counterfeiting or replication, eavesdropping of sensitive data like verification network traffic, and unauthorized access. Different strategies, such as disabling SSID Broadcast, help to conceal the AP name, which makes it more difficult for attackers to target the network; using lower signal helps to provide signal in a lower coverage area, which forces attackers to send packets with higher latency, which makes it even harder; using MAC Filtering aids in the blocking of specific suspected MAC Addresses; and using URL blocking aids in the blocking of suspected sites that are hosted to steal credentials.

Conclusion

The features as well as customizations of WLAN system are constantly expanding to enable greater transmission bandwidth, make setup simpler, and satisfy both commercial and technological expectations. Additionally, wi-fi now allows people to connect from virtually every shared environment, including transport hubs, parks, and airlines. Although WLAN can serve as an easy scapegoat for intruders and attackers to grab critical data, it is crucial to concentrate on WLAN protection. Therefore, safeguarding WLAN from harmful attacks is crucial, in addition to the quick growth of its features. This increases performance at work and builds trustworthiness. It's challenging to establish a network with the effective protection configuration. There are several assurance setting approaches including prevention systems depending on the real dimension of the network and even the degree of protection necessary. There are many security methods to comply among each appropriate circumstance, relying upon that internal network setting.

Appendix

Arduino Installation

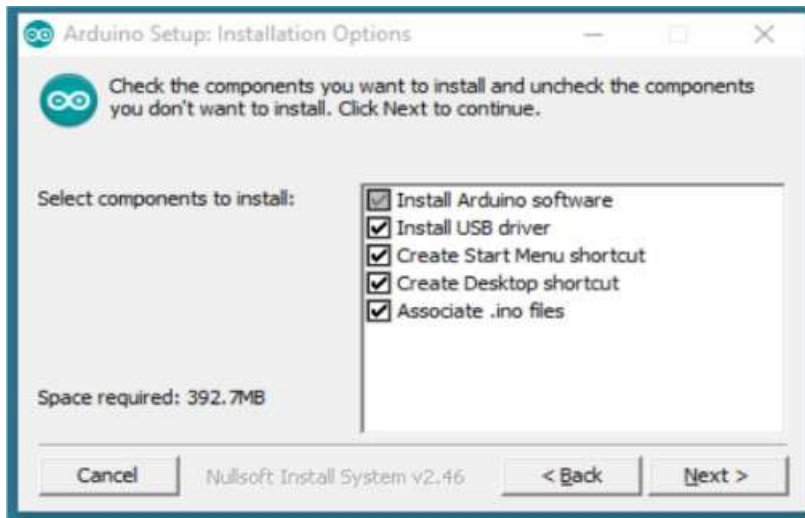


Figure 41: Arduino Installation 1

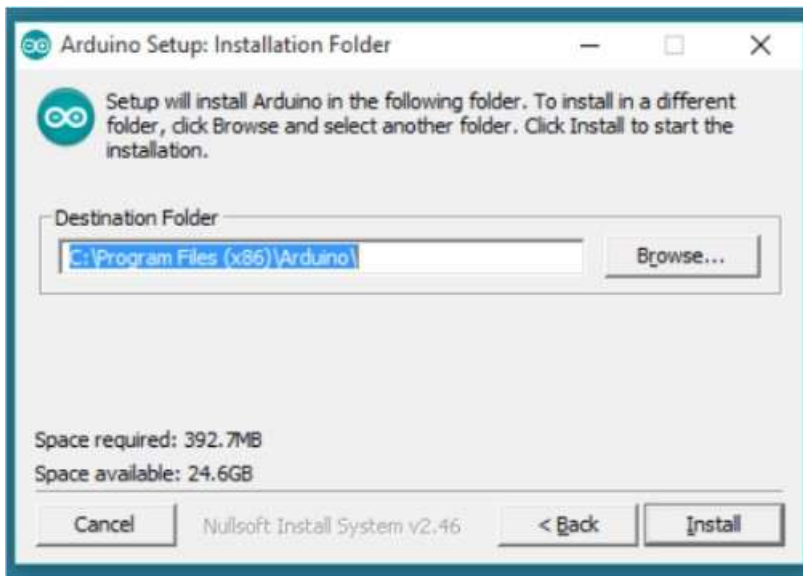


Figure 40: Arduino Installation 2

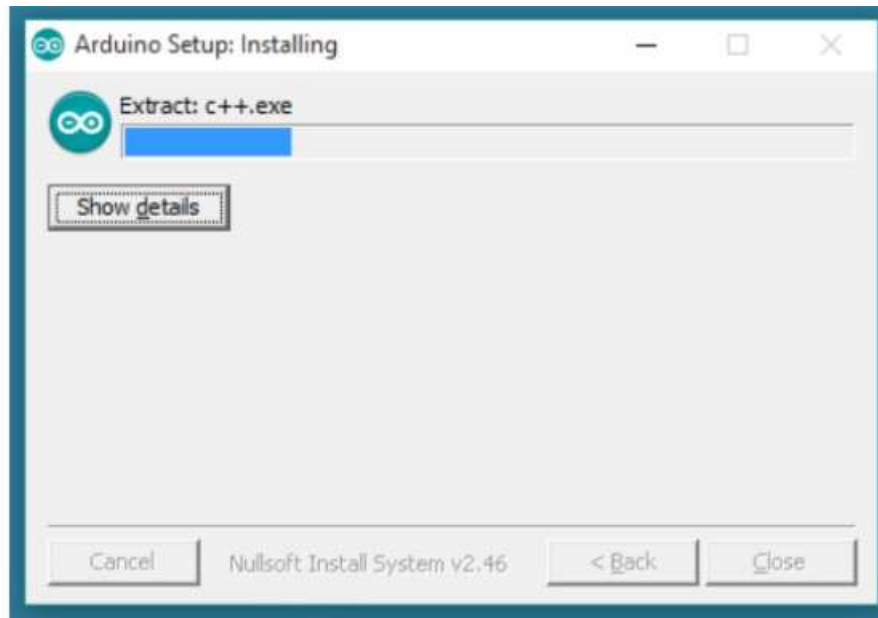


Figure 44: Arduino Installation 3

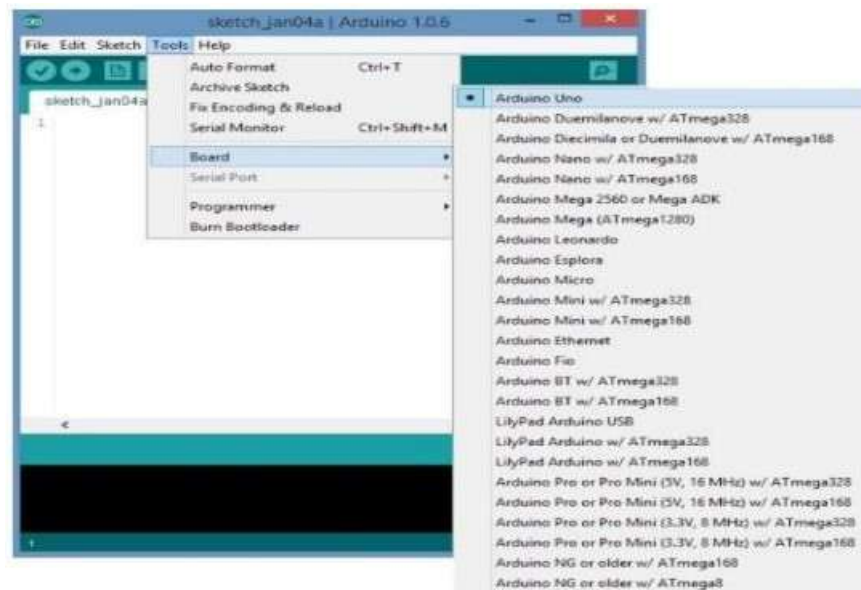


Figure 43: Arduino Installation 4

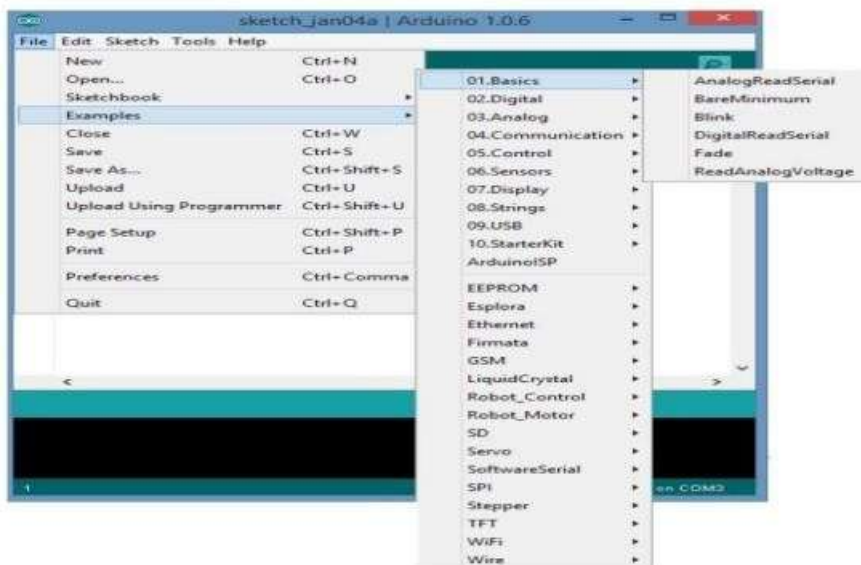


Figure 42: Arduino Installation 5

Code Sample

```
#include "Adafruit_NeoPixel.h"

#if defined(TARGET_LPC1768)
#include <time.h>
#endif

#if defined(NRF52) || defined(NRF52_SERIES)
#include "nrf.h"

// Interrupt is only disabled if there is no PWM device available
// Note: Adafruit Bluefruit nrf52 does not use this option
// #define NRF52_DISABLE_INT
#endif

#if defined(ARDUINO_ARCH_NRF52840)
#if defined __has_include
#if __has_include(<pinDefinitions.h>)
#include <pinDefinitions.h>
#endif
#endif
#endif

/*!
  @brief NeoPixel constructor when length, pin and pixel type are known
  at compile-time.
  @param n Number of NeoPixels in strand.
  @param p Arduino pin number which will drive the NeoPixel data in.
  @param t Pixel type -- add together NEO_* constants defined in
  Adafruit_NeoPixel.h, for example NEO_GRB+NEO_KHZ800 for
  NeoPixels expecting an 800 KHz (vs 400 KHz) data stream
  with color bytes expressed in green, red, blue order per
  pixel.
  @return Adafruit_NeoPixel object. Call the begin() function before use.
  */
Adafruit_NeoPixel::Adafruit_NeoPixel(uint16_t n, int16_t p, neoPixelType t)
  : begun(false), brightness(0), pixels(NULL), endTime(0) {
  updateType(t);
  updateLength(n);
  setPin(p);
```

Figure 45: Code Sample

Git Hub Link

[git@github.com:saurav0607/Code-for-DEAUTH-DETECTOR.git](https://github.com/saurav0607/Code-for-DEAUTH-DETECTOR.git)

System Prototype

```
root@kali:~# aireplay-ng -0 10 -a 80:35:C1:13:C1:2C wlan0mon
09:26:43 Waiting for beacon frame (BSSID: 80:35:C1:13:C1:2C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
09:26:43 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:44 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:45 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:46 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:47 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
09:26:48 Sending DeAuth (code 7) to broadcast -- BSSID: [80:35:C1:13:C1:2C]
```

Figure 46: De-Auth Demonstrate

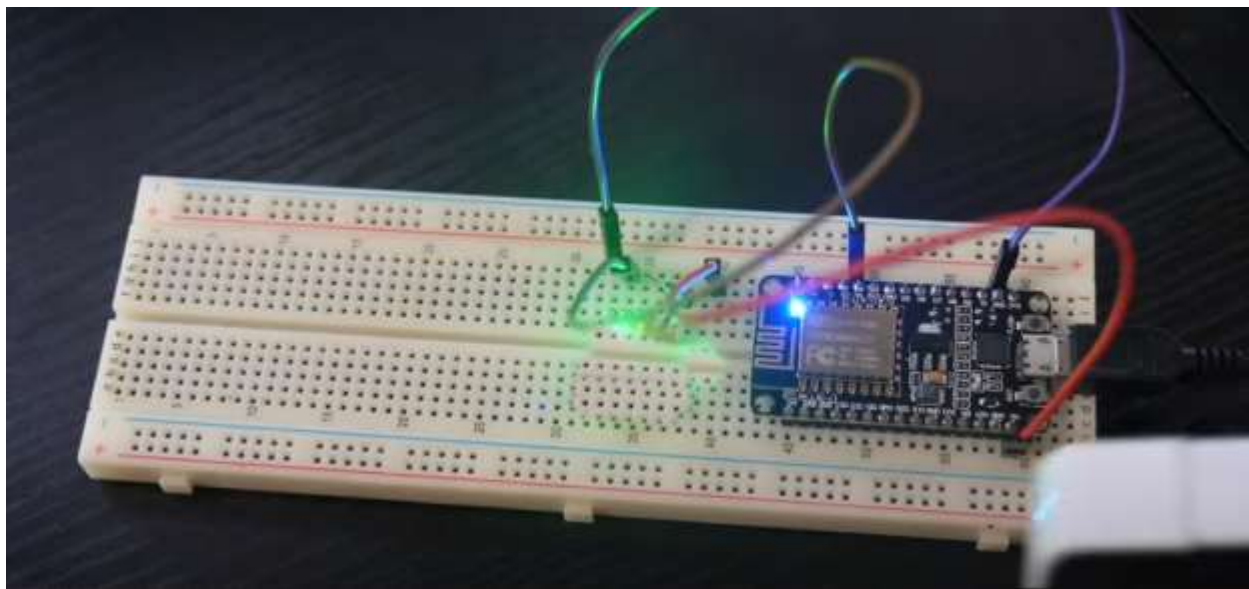


Figure 47: System Prototype

Reference

Bradley Mitchell. (2020). *Is It Worth It to Hide Your Wi-Fi Network?* Lifewire.

<https://www.lifewire.com/disabling-ssid-broadcast-on-wireless-routers-816569>

Cathie. (2022, February 11,). How To Use Webroot Vpn? <https://www.nstec.com/how-to-use-webroot-vpn/>

Chritsy, B. (20012-07-24). *IEEE SA - IEEE 802.11i-2004*. IEEE Standards Association.

<https://standards.ieee.org/ieee/802.11i/3127/>

Cisco. (2020). *Managing Dashboard Administrators and Permissions*. Cisco Meraki.

https://documentation.meraki.com/General_Administration/Managing_Dashboard_Access/Managing_Dashboard_Administrators_and_Permissions

Dan Rafter. (2022). *How to Secure Your Wi-Fi in 7 Simple Steps* | Norton. us.norton.

<https://us.norton.com/internetsecurity-iot-keep-your-home-wifi-safe.html>

ED REFORM. (2011). *How to Hack wifi using Wireshark*. Gadget Hacks.

<https://digiwonk.gadgethacks.com/how-to/hack-wifi-using-wireshark-424506/>

GeeksforGeeks. (2018, -03-18T16:38:54+00:00). Software Engineering | Classical Waterfall Model.

<https://www.geeksforgeeks.org/software-engineering-classical-waterfall-model/>

Gowri Shankar, & Nagesha, A. G. (2016). A Survey on Wireless Security Standards and Future Scope.02(08), 94.

https://www.academia.edu/28424203/A_Survey_on_Wireless_Security_Standards_and_Future_Scope

Inc, M. (2021). *Cisco Meraki | Advanced Malware Protection*. meraki.cisco.

<https://meraki.cisco.com/solutions/amp>

james, k. r. (2020, -04-08T17:48:06+00:00). WPA vs WPA2: Which WiFi Security Should You Use?

<https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/>

Jiri Brejcha. (2020). *10 Things You Need To Know About Cisco Meraki*. gblogs.cisco.

<https://gblogs.cisco.com/uki/10-things-you-need-to-know-about-cisco-meraki/>

Jomilė Nakutavičiūtė. (2020). *What is an evil twin attack? | NordVPN*. nordvpn.

<https://nordvpn.com/blog/evil-twin-attack/>

Kate Brush, & Valerie Silverthorne. (2017). *What is Agile Software Development (Agile Methodologies)?*

SearchSoftwareQuality. <https://www.techtarget.com/searchsoftwarequality/definition/agile-software-development>

KODY. (2018). *How to Detect & Classify Wi-Fi Jamming Packets with the NodeMCU*. WonderHowTo.

<https://null-byte.wonderhowto.com/how-to/detect-classify-wi-fi-jamming-packets-with-nodemcu-0188668/>

kody. (2019). *How to Hack Wi-Fi: Stealing Wi-Fi Passwords with an Evil Twin Attack*. WonderHowTo.

<https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/>

Lawrence, A. (2016, -11-15T14:00:33+00:00). *Cisco Meraki Device Overview*.

<https://www.transparent.ca/uncategorized/cisco-meraki-device-overview/>

Liam Aljundi. (2022). *Using the Arduino Software (IDE) | Arduino Documentation*. docs.arduino.

<https://docs.arduino.cc/learn/starting-guide/the-arduino-software-ide>

mario guzman. (2020). *NodeMCU ESP8266*. Components101. <https://components101.com/development-boards/nodemcu-esp8266-pinout-features-and-datasheet>

MARK B. (2022). *Is Netgear Armor worth it? It depends. ? MBReviews*. mbreviews. <https://www.mbreviews.com/is-netgear-armor-worth-it/>

Max Eddy. (2020). *Webroot Wi-Fi Security VPN Review*. PCMAG. <https://www.pcmag.com/reviews/webroot-wi-fi-security-vpn>

Ruri Ranbe. (2018). *How to Configure a Router to Block Websites*. Small Business - Chron.com. <https://smallbusiness.chron.com/configure-router-block-websites-55204.html>

Said, Y. (2020, "June 15 "). *Using Airmon-ng in Kali Linux 2020.2*. https://linuxhint.com/airmon-ng_kali_linux/

Sarah Lewis. (2018). *What is the Prototyping Model?* SearchCIO. <https://www.techtarget.com/searchcio/definition/Prototyping-Model>

Sean Wilkins. (2020). *Common Wireless Network Security Threats*. pluralsight. <https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats>

stantzouris, d. R. (2020). *Deauthentication Attack using Kali Linux*. SudoRealm. <https://sudorealm.com/blog/deauthentication-attack-using-kali-linux>

Winder, & Davey. (2018). *Secure your Wi-Fi against hackers in 10 steps*. IT PRO. <https://www.itpro.co.uk/general-data-protection-regulation-gdpr/secure-your-wi-fi-against-hackers-in-10-steps>