International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security and Privacy of Public WiFi

T. Charan Sahu

Student, Department of Information Technology, GMR Institute of Technology

ABSTRACT:

Wireless local area networks are becoming more and more common in the modern world, which is powered by technology and network connections. People are using public WIFI in bus stop, airport, railway station etc. A wireless technology called WIFI enables devices to such as computer, laptops, smart phones to interface with internet to exchange the information with each other. WIFI can be good application for IOT (internet of things) devices. Nowadays, people being almost depend on ECAST, ecommerce. People are quiet interested in using the free WIFI, which could be inconvenient for their privacy. Weak security exists on public WIFI. HTTPS internet traffic using TSL (transport layer security) and is encrypted to given data privacy. By using public WIFI we are simply leak our privacy. The main objective of this paper is to study the way of data leakage using brute force, WPS pixie attack, krama attack, DOS (denial of services), malware attack. To increase the privacy and reduce the leakage of data process like VPN (virtual private network), increase bandwidth, increase space, fire wall security would be implemented.

KEYWORD: ***WIFI, security, privacy, internet traffic, HTTPS, IOT (internet of things), TSL (transport layer security), VPN (virtual private network).***

INTRODUCTION

In recent years, technology and network connections have made it possible for more individuals to use the internet, which is a tool that is crucial for daily work. A WIFI is a wireless network protocol that is often used for Internet access and device local area networking. The IEEE 802.11 set of specifications forms the foundation for Wi-Fi.. Nearby digital devices may communicate with one other via radio waves thanks to Wi-Fi. These are the computer networks that are utilised the most throughout the globe. In order to link desktop and laptop computers, tablet computers, cellphones, smart TVs, printers, and smart speakers to a wireless router so they can access the Internet, they are used in home and small business networks on a worldwide scale. in wireless access points to provide mobile devices with access to the public Internet in public places including coffee shops, hotels, libraries, and airports. Accordingly, a recent survey indicated that 70% of tablet owners and 53% of smartphone and tablet users, respectively, claimed to have utilised public Wi-Fi hotspots. This suggests that everyone interested in using public Wi-Fi is exposing our privacy in the process. However, as data shared over public Wi-Fi may be readily intercepted, many mobile device and laptop users are endangering their private information, digital identity, and money. Additionally, if their computer or device is not protected by an effective security and anti-malware application, the risks are greatly increased. It's a convenient way to check your emails and stay up to date when you're on the move. social media or use the internet. But con artists regularly snoop on public Wi-Fi networks and eavesdrop on information flowing across the connection. This gives the criminal access to the passwords for users' accounts, their financial information, and other data. social media or use the internet. But con artists regularly snoop on public Wi-Fi networks and eavesdrop on information flowing across the connection. This gives the criminal access to the passwords for users' accounts, their financial information, and other data.

LITERATURE SURVEY

Paper[1] : This greatly expands the number of hotspots a company may offer, but it frequently takes place without the customers' consent and occasionally without disclosing it to them. The use of the routers by customers raises a number of privacy and security issues.We used open coding in conjunction with a grounded theory method to develop a set of codes for these comments. We developed a preliminary set of codes after reading the comments, and we enhanced the coding over the course of three careful iterations of the data.ISPs and IT specialists who devise ways to profit from this surplus must be aware of the societal aspects relating to privacy and security concerns. They may lessen a lot of conflict by offering compensation and being transparent.

Paper[2] : The method for counting mobile devices that we present in this work involves examining WiFi probe requests made by smart devices at particular times and locations. Our goal is to resolve the problem by employing a methodology that withstands Media Access Control (MAC) address randomization strategies.The method proposed for estimating the number of devices by analysing Wi-Fi probe requests demonstrated a very significant correlation with the actual number of people present in the area, with a Pearson's correlation coefficient of 0.896. Despite this, the mechanism was able to achieve a good correlation and a low mean relative error of 0.087, which is amazing precision for the indicator. was given in this study, was shown to be more accurate than both the Linear Regression (LR) According to the findings, the state machine modeling-based Sherlock methodology, which and Support Vector Regression (SVR) based approaches, both proposed in [51]. The mean relative errors produced using the Sherlock method were 340% and 243% higher, respectively, than those obtained using the LR-based and SVR-based procedures.

Paper[3] : This chapter offers an architectural idea for short-range wireless networks (WIFI) and high-speed backbone wireless networks (5G networks). The security ramifications of linking wi-fi to 5G networks are also covered in this chapter.One approach to developing the security protocol is to address the security issues that arise in both wireless and cellular networks. With this style of security protocol architecture, the attacks outlined in Tables 7.1 and 7.2 can be handled by a single security protocol at the interoperable gateway. The security protocol needs to be specified separately for each layer of the protocol stack because 5G and Wi-Fi interoperability can happen at any level of the protocol stack (see "Interoperability of Wi-Fi with 5G Networks").Security issues are crucial when it comes to connectivity for everyone, everywhere, and anything. This chapter provides a brief explanation of the security factors that must be taken into account for WiFi and WiFi networks to work with 5G networks. In addition, a description of how WiFi and WiFi networks interact at different protocol stack tiers. A succinct explanation of the security concerns and contributing elements for WiFi and the WiFi network architecture is also given. Future security issues and potential solutions will be briefly discussed when the 5G network solution has been built and assessed.

Paper [4]: In this study, security concerns associated with the design of smart cities are identified and investigated, as well as potential cyber-attack scenarios in the creation of services and operational environment. The ripple effects of each attack are also looked at. The study's analysis conclusions can be applied to future security technology applications and research.These security dangers and attacks will lead to assaults on sensor equipment installed in the terminal, invasions of personal privacy owing to CCTV video leaks, and the propagation of cyberattacks from one service area to another. Therefore, maintaining cyber security is essential for the creation and administration of smart cities. When implementing security controls and creating smart city security technology, the study's analysis of security threats and probable attack scenarios can serve as a guide. Security solutions that can manage the probable assault scenarios looked at in this study's research will need to be researched and developed in subsequent studies. To ensure the cyber security of the smart city, it will be necessary to develop and implement security technology for sensors, provide a privacy protection measure over the processing of CCTV video information, and promote security measures for information linkage and sharing systems between smart city services.

Paper [5]: The main contribution of this research is the use of cyber threat intelligence to improve cybersecurity practises at CSC. We integrate CSC concepts with CTI so that CTI can methodically assist security initiatives for the digital supply chain. Finally, we recommend measures based on the CTI information to assist the CSC organisation in improving its overall cybersecurity approach.CTI criteria may be used to evaluate the system's susceptibility to known-known attacks, unknown-unknown attacks, and known unknown assaults. Important CSC assaults including APT, penetration, manipulation, and command & control assaults are among them. TTPs are the specific attack strategies employed by the adversary; they employ people, infrastructure, capabilities, and tools. It provides CTI information on the victim's target in order to exploit targets being attacked (who, what, or where). The CTI life cycle phase gave us the expected effects, stages of the death chain, handling recommendations, and resources of the TTP information.The CTI gained will guide the strategic, tactical, and operational management roles and responsibilities. Operational level managers can link attacks, identify attack specifics and TTPs, and provide control statement solutions using the CTI indications. Tactical level managers could use CTI to evaluate and prioritise indicators for configuration, audit, monitoring, and escalating threat warnings to the relevant sources for security product purchases. Strategic CTI will aid in resource allocation, top management approval, and the creation of a model for executive summaries.

Public WiFi Security Challenges:

Application layer

The caching, scheduling, and transcoding of video traffic are the primary goals of application-traffic-based optimizers. Statistics and user behaviour analytics are simply two applications of an application-based optimizer's architecture. These technologies are employed to build a transparent network of traffic classifiers, load balancers, and the functionality of the application itself. There isn't a standard TCP/IP solution available that Network/transport layer caching and explicit HTTP proxies can communicate with one another. the application layer has problems. Therefore, HTTP/2 is designed to address the present Implementation Difficulty. However, this will lead to more issues brought on by the requirement for difficult encryption. Knowing application-specific features in any of the various network interfaces is an option for establishing interoperability at the new apps, which are developed so they may connect with the "Application layer." the elements that influence switching choices. Every time a socket is opened, the programme code needs to be updated in order to link the socket to the interface specified by the application. The switching module is used, not the normal interface. Security providing to application-level interoperability is essential to protecting the data of numerous apps. Applications will frequently provide the user with a variety of sensitive services, all of which need to be protected from intrusion. In order to provide comprehensive application-level security that is compatible with a range of networking technologies, new application-level security protocols are being created as part of the standardisation of the Internet.

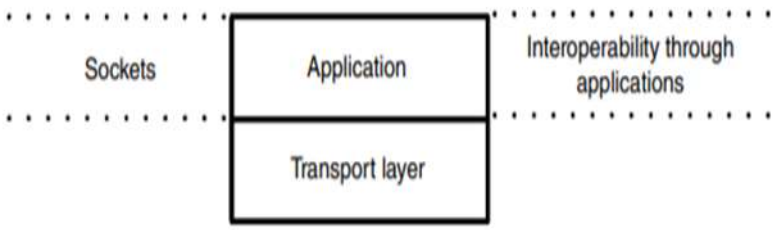


Figure: WiFi interoperability at application layer

Transport Layer

Maintaining end-to-end TCP connections when switching between various interfaces is the main challenge in establishing interoperability at the transport layer (Figure 7.4). A TCP connection is made up of four tuples: Source IP, Source Port, Destination IP, and Destination Port. Since different network interfaces have different IP addresses, switching the network interface will sever the end-to-end TCP connection. Redirectable Sockets, often known as RedSocks, are one solution for such issues. With pTCp [10], smooth interoperability at the transport layer can be achieved by aggregating bandwidth, which is done by stripping data across the several TCP connections.Using current TCP proxies, mobile carriers modify network performance to meet desired needs. End-to-end TCP congestion control is currently unable to span heterogeneous networks (cellular and wireless networks). This is due to increased packet loss and end-to-end latency. Furthermore, it is crucial to stress that TCP-based solutions now in use are ineffective, especially in mobile networks where the system is actually intended to provide virtual-circuit-like functionality. Therefore, due to significant buffering, variable latency, a lack of AQM, and congestion notification, regular TCP will perform worse in 5G networks. One solution to this issue is to use TCP proxies, which can lower the performance cost of interoperability problems. Additionally, security at the Transport layer interoperability For connection-oriented (TCP) or connection-less (UDP) end-to-end data transmission between the source and the destination, it is crucial to provide the application with data security. The security of transport layer protocols that provide end-to-end service to multiple applications is essential for transport layer interoperability. The introduction of TLS in HTTP/2 will lead to the rapid adoption of end-to-end encryption at the Transport layer.

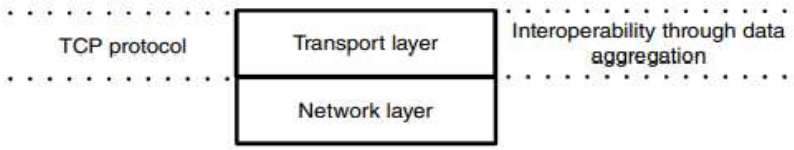


Figure Wi-Fi interoperability at Transport layer

Network Layer

Existing networks, both wired and wireless, heavily depend on Internet technologies (IP-based networks). A substantial amount of additional hardware must be built in order to support the functions of non-IP based networks. Let's examine a mobility management example. In order to provide "seamless connectivity," 4G networks are deploying an anchor point-based mobility approach through tunnelling. This can be accomplished via proxy-MIP- or GTP-based technology. This type of solution's centralized design suffers from the usual efficiency, scalability, and security problems. As a result, work on creating novel solutions to satisfy the needs of internet access, such as Selected Traffic Offload, began. The most prevalent use case for mobile Internet connectivity is outlined in [9], and it is not required to have perfect IP connectivity. A challenge to achieving interoperability at the network layer is the maintaining of a single static IP address (IPv4 or IPv6) for the mobile device across several network interfaces. The concept of optimized Mobile IP allows for the creation of a single mobile device with a static IP address. A mobile device is considered to have left the home network and entered a foreign network each time it switches to a new network interface. It is easy to ensure that a "source IP address" is used to provide end-to-end communication employing encapsulation and tunnelling. However, both Wi-Fi APs and cellular BSs need to support Mobile IP protocol for this strategy to function (tunneling and encapsulation at Foreign Agents). Protecting the security of L3 data is crucial for interoperability at the network layer (IP packets). Mobile IP, a network layer technology, provides global Internet connectivity using IP-in-IP encapsulation and L3 tunnelling. A thorough security architecture has been created by contemporary research to protect L3 data using IP security (IPsec). Using mobile IP with IPsec is one way to secure application data (IP packets) at the network layer. Optimized Mobile IP is made to select the optimal packet traversal path between source and destination. A mobile device could be made using the concept of optimized Mobile IP. It is considered to have left the home network and entered a foreign network once it switches to a new network interface. Utilizing tunnelling and encapsulation makes it straightforward. It is necessary to guarantee the use of a "source IP address" for end-to-end communication. However, for this strategy to function, both Wi-Fi APs and cellular BSs must support the IP protocol for mobility (tunneling and encapsulation at Foreign Agents).

Protecting the security of L3 data is crucial for interoperability at the network layer (IP packets). Universal and Anywhere Internet connection is provided by Mobile IP, a network layer protocol, via L3 tunnelling and IP-in-IP encapsulation. Modern research has created a thorough security strategy to deliver the IP security that safeguards the L3 data (IPsec). Mobile IP is one way to provide network-layer security for application data with IPsec (IP packets). The goal of Optimized Mobile IP is to select the best packet traversal path between the source and the target location.

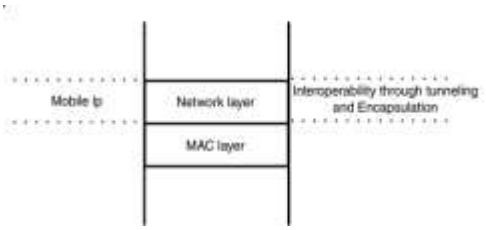


Figure WiFi Interoperability at the Network Layer

MAC Layer

AMAC is a member of the Adapt Net protocol family. Here is a two-layered MAC protocol that can let cellular and wireless networks communicate with one another. The master sublayer equivalent of a virtual cube. modifying the module to offer user-based interoperability.

It is essential to guarantee the security of the application data when switching between packets (or frames) of different connection technologies (WiFi). Protect the data from intruders. Generally speaking, changing the data is easy for hackers. when it comes to interoperability, the L2 packet switch needs to be able to communicate with a variety of technology protocols. Consequently, To ensure application data protection at "Network Interface" switching, it is critical for network designers to consider MAC level interoperability security considerations

VI. METHODOLOGY

The Indian Government, as well as Governments throughout the world, have launched plans for providing public Wi-Fi because they recognise the internet as a necessary tool for day-to-day work and have made it easier for people to use it in recent years]. However, privacy hazards associated with utilising public Wi-Fi have also been raised nationally and will be covered in this study. This case study aims to analyse the privacy policies of two Internet service providers in India, Tata Docomo and D-VoiS, which provide public Wi-Fi services in Bangalore city against the indicators listed under the Ranking Digital Rights project[4], as well as the Information Technology (Reasonable security practises and procedures and sensitive data) [Reasonable security practises and procedures and sensitive data] [Reasonable security practises and procedures] [Reasonable security practises and procedures and sensitive data Rules, 2011 (personal data or information) (personal data or information) [5. Based on this analysis, this paper will provide significant recommendations for these ISPs to adhere to in order to guarantee sound privacy policies and practises and to build a framework and ecosystem that are balanced with respect to crucial privacy considerations, particularly those related to public Wi-Fi.

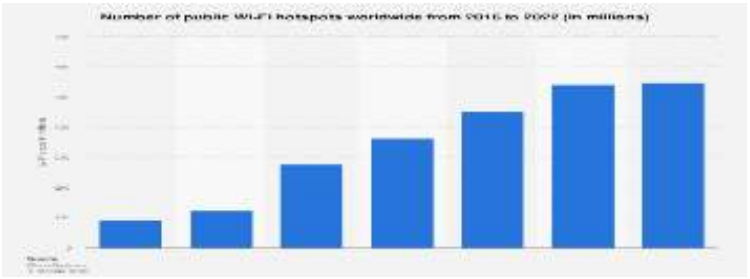


Table- 1 Security issues by a public Wi-Fi:

Security Issue Type	Security Issue Description
Interception	By intercepting information through control and data signalling without altering or erasing it, the attacker violates the victim's right to privacy, which is violated by both the subscriber and the network operator
Reply attacks	Depending on the objective and type of physical access, the intrusion could bring bogus things into the system (such phoney messages). erroneous subscriber data or incorrect service logic
Data leakage	The intruder uses open entry points to collect private information. the specific user data
Analysis of the traffic flow	The intrusive party records the length, rate, time, source, and destination of the traffic flow in order to ascertain the user's location.
DOS attack	An attempt to disable a computer system or network so that its intended users cannot access it is known as a denial-of-service (DoS) attack. DoS attacks do this by bombarding the target with traffic or data that makes it crash.
Brute force attack	Application applications utilise a brute-force attack as a trial-and-error technique to decode encryption keys and login information in order to use them to enter systems without authorization. It is exhausting to use brute force instead of using intelligent techniques.
DDOS attack	A DDoS attack is a sort of cyberthreat that involves making excessive requests to a website or other online resource, which takes it offline. To exert this pressure, the attacker makes use of a sizable computer network, frequently by exploiting "zombie" workstations that malware has taken control of.

Traffic jamming	The intrusion attempts aggressively utilize the WLAN's bandwidth.to overwhelm legitimate traffic with false messages, through transmissions with a high radio frequency. These types of assaults fall into this category: Spam attacks: By flooding with spam, the intrusive party will using wireless communication networks to spread spam. Attacks using denial of service (DoS): the intrusive party prevents the legitimate User traffic is flooded with high frequency to reach the receiver. radio transmissions or phone communications;
MAN IN THE MIDDLE	Man-in-the-middle (MiTM) attacks on computers include the attacker covertly intercepting and relaying communications between two parties who think they are communicating directly to one another. When someone is assaulted, they are eavesdropping in the sense that they hear what is being said and then have complete control over it.
Network injection	Packet injection is a term used in computer networking to describe the process of altering an existing network connection by creating fake packets that appear to be a regular part of the data stream (also known as forging packets or spoofing packets)..

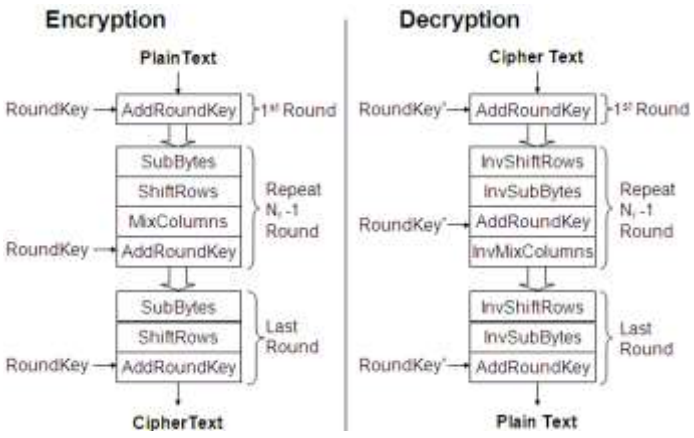
Table-2 Based on methodologies used to cause the attack

attacks using service logic	The 5G communication's data is the target of the hacker. harming the system by altering, incorporating, or deleting the data stored there
data-based attacks	By simply assaulting the service logic of the various network pieces, the intrusive party seeks to do significant damage.
Message-based attacks	Stopping the flow of control and data transmission to and from the Wi-Fi network by integrating, swapping out ping, replaying, and other forms of attacking the Wi-Fi architecture.

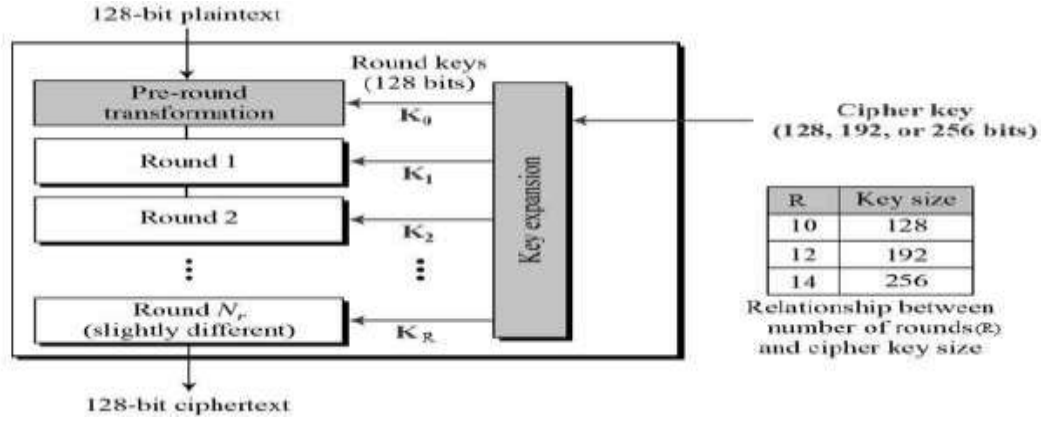
Advanced Encryption Standard

As opposed to a Feistel encryption, AES uses iterative encryption. A "substitution-permutation network" forms the basis of it. It comprises of a number of interrelated processes, some of which shuffle bits around while others replace specific outputs for inputs (substitutions) (permutations). It's noteworthy to notice that AES does all of its calculations using bytes rather than bits. AES treats a plaintext block's 128 bits as 16 bytes as a result. In contrast to DES, the number of rounds in AES can be customised and is based on the key length. For processing as a matrix, these 16 bytes are arranged in four columns and four rows. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The original AES key is used to determine the unique 128-bit round keys used in each of these rounds. The design includes a fixed table (S-box) that is searched up in order to replace the 16 input bytes. The result is represented as a matrix with four rows and four columns. The four rows of the matrix are all shifted to the left. Any entries that "slide off" the row are repositioned on the right side. The second row is shifted one (byte) place to the left, but the first row is left in place. Two places to the left, the third row has been shifted. A new matrix with the same 16 bytes but shifted in relation to the previous one is produced by moving the fourth row three spaces to the left. each other. Now, a distinct mathematical procedure is used to change each four-byte column. After receiving the four bytes of one column as input, this method generates four completely new bytes and inserts them into the original column. The result is a second, fresh matrix with 16 more bytes. It should be emphasised that this stage is not part of the final round. The 16 bytes of the matrix, which are now regarded as 128 bits, are XORed with the 128 bits of the round key. If this is the last round, the output is the ciphertext. If not, the procedure is restarted and the output 128 bits are transformed into 16 bytes. Technique for Decryption An AES ciphertext's decryption process is similar to the encryption process in reverse. Each round is composed of the following four operations: add round key, mix columns, shift rows, and byte substitution. Despite being closely related, the encryption and decryption algorithms must be performed independently since these procedures, unlike the Feistel Cipher, are carried out in reverse order.

ENCRYPTION AND DECRYTION OF AES



STRUCTURE OF AES



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Table-3 SOME TOOLS ARE USED TO HACKING THE WIFI

TOOLS	**TOOLS FOR WIFI HACKING**
Aircracking	Air crack-ng, a dangerous suite of tools used for wireless hacking, is well-known in today's online world. The utilities can be used with Linux and Windows operating systems. It's important to remember that Air crack-ng uses other tools to first gather data about its targets.
Wifite	Wep or WPA-encrypted wireless networks can be audited using the tool Wifite. The tools air crack-ng, pyrit, reaver, and tshark are used to do the audit. This programme can be automated and is trustworthy enough to operate unattended with just a few basic settings. Wep or WPA-encrypted wireless networks can be audited using the tool WIFI. The tools air crack-ng, pyrit, reaver, and tshark are used to do the audit. This application is dependable when used unattended and can be used to automate activities with a small number of parameters.
WIFI phisher	A security programme included in this package launches automated phishing attacks against WiFi networks in an effort to gather user credentials or secret passphrases. It is a social engineering approach that, in contrast to previous strategies, does not use brute force. It is a simple method for acquiring login information via captive portals, external login sites, or WPA/WPA2 secret passphrases**.**
nSSIDer	nSSIDer Office is a tool for optimising and debugging Wi-Fi. It looks for wireless networks with the aid of your Wi-Fi adaptor so you can examine their signal quality and channel usage. It also offers a lot of interesting information about each network.
Wireshark	Wireshark is capable of capturing any kind of data that is transmitted over a network, including usernames, email addresses, confidential information, pictures, videos, and anything else. As long as we are able to monitor network traffic, Wireshark can sniff the credentials that are being transmitted across the network.
Cowpatty	While auditing WPA-PSK or WPA2-PSK networks, this tool may be used to discover weak passphrases that were used to build the PMK. Give a dictionary file with potential passphrases, a libpcap capture file containing the 4-way handshake, and the SSID of the network.
Air crack	To assess the security of a Wi-Fi network, utilise the Air crack-ng toolkit, which is part of Kali Linux. It is capable of breaching, monitoring (by gathering packets), and attacking wireless networks. The password-protected WPA/WPA2 Wi-Fi network will be compromised using Air crack-ng in this post.
Airgeddon	An extensive menu-driven third-party tool wrapper for wireless network inspection is called Airgeddon.
omnviews	ommView for Wi-Fi is a popular wireless monitor and packet analyzer application. Its graphical user interface is simple to use. It works

	flawlessly with 802.11 a/b/g/n/ac networks. Every packet is recorded, and a list of the most significant data is displayed. You may receive crucial information such as access points, stations, signal strength, network connections, and protocol dispersion. To decode packets that have been captured, employ user-defined WEP or WPA keys. The main target audience for this product is software developers who are making wireless network software, Wi-Fi network managers, security specialists, and home users who want to monitor their Wi-Fi traffic.

Result and discussion

You can take security measures to protect your wireless network when you're at home. These include turning on encryption, which converts the data you transfer over the internet into a code that no one else can read, using a strong router password, and limiting the devices that can join to your network. However, when using the Wi-Fi at your neighbourhood coffee shop, there isn't much you can do to regulate the network security. If you visit a website that is not encrypted or just uses encryption on the sign-in page, other network users can see what you see and send. Your session can be a ruse for them to log in. Thanks to new hacking tools, even those with limited technological skills can readily execute this activity. things are available online without charge. Your login passwords, contact details, family photos, confidential documents, and personal data could all be at danger. A fraudster could also use your account to test the security of your usernames and passwords on other websites, including those that store your financial data, or to pretend to be you and trick people on your contact lists. If a fraudster gets their hands on your financial or personal information, your identity could be stolen. You can also be sharing your data with the organisations offering the public Wi-Fi when you log on. Many public Wi-Fi hotspots, like those in hotels and airports, may also ask you to install a "digital certificate" before you can access their internet. They might do this to search through your traffic for malware, but it also gives them the ability to read your traffic, even if it is going to a secure site.

Your internet communication is encrypted when you use a VPN, making it impossible for anybody to read it over a public Wi-Fi network. You won't need to worry as much about external security because the VPN will safeguard your connection everywhere you go, even if you aren't utilising a secure Wi-Fi connection. Now that you are aware of the dangers associated with accessing a public Wi-Fi network, you may be asking how to safeguard yourself from these dangers. Well, using a public Wi-Fi VPN is the best option. You might wonder how a VPN protects you when using free Wi-Fi. One benefit is that it encrypts any data transferred from your smartphone over a public Wi-Fi network. In this manner, even if the data is intercepted, it will be meaningless since the hacker would be unable to decode the data. A public WIFI VPN also conceals the IP address of your device, which is a crucial piece of information that hackers would require in order to locate and get access to your computer. They will only be able to view the IP address instead. the VPN server to which you are now logged in. it safe to use a VPN over a public Wi-Fi network at this point? The response is "yes," but only if you pick a reliable VPN provider. As you can see, not every VPN is the same, and many of them employ shoddy encryption. Use caution while utilising free VPNs since they frequently perform the reverse of their intended function by gathering user personal information and selling it to outside parties. In no way! With the exception of a few nations that impose rigorous Internet censorship, such as China, the UAE, Russia, North Korea, Iraq, etc., VPNs are just privacy tools and are completely lawful. Despite this, you may still be held accountable for any unlawful activity carried out while using a VPN, such as breaking copyright laws, hacking, engaging in illicit gambling, downloading protected content, etc. Yes, a VPN secures your online communications, including passwords and other sensitive data. There is one exception, though: if your computer has already been infected with malware known as keyloggers, which records everything you type and transfers it to dubious third parties.

Conclusion

When it comes to everyone, anything, and anything connection, security concerns are essential. The ISPs must have a strong Privacy Policy in place to satisfy the many worries people have about privacy and security when using public Wi-Fi. The Information Technology (Reasonable security practises and procedures and sensitive personal data or information) Rules, 2011, requirements for the security of personal information, and improving the policies in accordance with those requirements will significantly contribute to protecting freedom of expression and ensuring the privacy of user information. Due to the growth of free and public Wi-Fi services in India, it is more crucial than ever to ensure adherence to the country's current data protection laws. This is because privacy and security issues are becoming more and more of a worry. Taking appropriate steps, such as getting consent before collecting the commitment of firm leaders to uphold individual rights, the adoption of security standards, raising public knowledge of security issues, etc. by such corporations must all be taken into account to secure the safety of personal information and lessen the possibility of a data breach. To achieve the standards established by the Ranking Digital Rights initiative and demonstrate dedication to the protection of users' rights to freedom of speech and privacy.

Reference

1. Lee, J., Kim, J., & Seo, J. (2019, January). Cyber attack scenarios on smart city and their ripple effects. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE.
2. Golbeck, J. (2020, October). User concerns with personal routers used as public Wi-fi hotspots. In 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 571-576). IEEE.
3. Anamalamudi, S., Sangi, A. R., Alkatheiri, M., Muhaya, F. T. B., & Liu, C. (2018). 5G-Wlan security. A Comprehensive Guide to 5G Security, 143-163.

4. Oliveira, L., Schneider, D., De Souza, J., & Shen, W. (2019). Mobile device detection through WiFi probe request analysis. IEEE Access, 7, 98579-98588.

5. Yeboah-Ofori, A., Islam, S., & Yeboah-Boateng, E. (2019, May). Cyber threat intelligence for improving cyber supply chain security. In 2019 International Conference on Cyber Security and Internet of Things (ICSIoT) (pp. 28-33). IEEE.