

**An Exploration of Privacy and Security Risks Posed by
Wireless Network Public Datasets**

**By
MOHAMMED ABDUL KAREEM**

**Submitted to
The University of Roehampton**

**In partial fulfilment of the requirements
for the degree of
MASTER OF CYBERSECURITY**

Declaration

I hereby certify that this report constitutes my own work, that where the language of others is used, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of others.

I declare that this report describes the original work that has not been previously presented for the award of any other degree of any other institution.

Mohammed Abdul Kareem

Date: 11-09-2024

Acknowledgment

I would like to dedicate my profoundest thanks to my teacher [Dr Charles Clarke] for their valuable help, knowledge, and motivation to me in the course of accomplishment of this dissertation. Your encouraging comments and constant encouragement towards my work have helped improve the quality of the pieces, and I surely appreciate your endurance and assistance throughout this process.

You not only equipped me with all the knowledge and skills I required for this research endeavor, but also encourage me to strive for excellence and total personal development. Your love for your job and your students cannot go unnoticed and I am grateful to have been your student.

Thanks for supporting my ability, for all the thoughtful help, and for being always ready to talk and guide. As this dissertation came to be, your support has been quite instrumental, and I want to thank you for all that you have done for me.

Table of Contents

Acknowledgment	3
Abstract	6
1. Introduction	7
1.1 Problem Statement	7
1.2 Aims and Objectives	8
1.3 Significance of the Study	9
2. Literature Review	10
3. Methodology	17
3.1 Research Approach	17
3.2 Data Collection	18
3.3 Data Analysis	19
3.4 Privacy and Security Risk Assessment	20
3.5 Limitations	21
3.6 Ethical Considerations	22
4. Results	22
4.1 Overview of the Dataset	23
4.2 Data Cleaning and Preprocessing	25
4.3 Data Analysis	27
4.4 Encryption Type Distribution	28
4.5 Identifying Exposed Sensitive Information	29
4.6 Privacy and Security Risk Assessment	29
4.7 Temporal and Channel Analysis	29
4.8 Data Visualization	29
5. Discussion	29
5.1 Security Risks	29
5.2 WEP and Unsecured Networks	29
5.3 Sensitive SSIDs	30
5.4 Channel Congestion	31

5.5 Implications for Network Security	32
6. Future Research Directions	34
6.1 Upgrade Encryption	36
6.2 Change SSID Naming Conventions	37
6.3 Optimize Channel Selection	37
6.4 Regular Audits	37
7. Conclusion:	39
8. References	41

Abstract

This dissertation seeks to explore the risks and challenges of open data sources in wireless networks especially the Wireless Fidelity (Wi-Fi) networks in Central London United Kingdom. Using data collected from WiGLE the study reveals various privacy and security threats in urban conditions (Valchanov et al., 2019a). It reveals that encryption is still insufficient in many cases of users using WEP or no encryption at all, which is rather unsafe. Moreover, the study explores the transmission of information through SSIDs and discovers modes of violating privacy (Moissinac et al., 2021). The research evidence convincingly shows that there is a connection between network configuration and security measures and that commercial sections are in possession of more stringent encryption algorithms than residents' areas (Boutet and Cunche, 2021). The study advocates for the promotion of awareness among the public and development of policies that will improve the security of wireless networks (Adewuyi et al., 2024). It also emphasizes the use of a good secure SSID name, selection of the right channels to avoid conflict, and backup security checks (Mallaboyev et al., 2022). The presented research offers important findings concerning the state of wireless network security in London and can serve as a basis for further research on increasing network security and the users' engagement.

1. Introduction

With this emerging global village wireless has been adopted as a central tool for communication, business, and access to information (Jamalipour and Bi, 2018). With the development of wireless technology, such networks have become a more widespread and inalienable part of contemporary society. Wireless networks have become as necessary a utility as electricity and running water; they are present in cities and villages and facilitate the functioning of the world's digital networks. However, with this kind of broad adoption comes numerous privacy and security issues, most of which stem from the disclosure of wireless network datasets over the wireless network (Boutet and Cunche, 2021).

That is why there is a platform, namely WiGLE, which draws attention to the possibility of these threats. net, a database of worldwide geographic data concerning Wi-Fi wireless networks assembled through the work of the crowd. WiGLE.net concerns wireless networks' data such as SSID, BSSID, modes of encryptions, GPS latitude and longitude, and timestamps. This data is useful for analysis and scientific research in the networks, but it causes accruing of serious threats to privacy and security (Valchanov et al., 2019a). One of the major problems resulting from the availability of detailed network information, more so, when integrated with geographical information is how to secure wireless networks and protect sensitive information from unauthorized access (Matte, 2017).

1.1 Problem Statement

The issue under investigation in this research is traced to the security vulnerabilities that emanate from the public access of wireless network data through sites such as WiGLE.net. It is thus possible to reveal susceptibility based on SSIDs, BSSIDs, and GPS coordinates, amongst other details accessible. For example, it might be possible to use the technique to pinpoint targets based on the wireless networks in a certain territory, assess the levels of security that have been deployed on each of the networks, or even monitor the behavior of certain targets or organizations by studying how frequently they use certain networks (Butty'An and Hubaux, 2009). These risks are very much real and current in the context of cyber security, if such data is misused, then one can get

unauthorized access to the network and can breach data security or sometimes even pose a direct physical threat (Vanhoeft et al., 2017).

1.2 Aims and Objectives

This project aims to identify such threats by examining data from wireless networks in London, UK, particularly from WiGLE.net. The focus on the city of London as a case study is particularly valuable because it allows us to explore how urban wireless networks function and how the data collected by them can be used for various purposes, constructive and destructive (Cisco, 2022). By so doing, it will be possible for the project to determine the different types of information that are often considered, the security threats that may be posed to a network or even the privacy of an individual, and the measures that may be taken to deal with the risks (Zhang and Shen, 2015). The stake of this work is in their possible contribution to the understanding of various dangers of WPA/WPA2 open network data, which were explored in the study. Although it is possible to gather and even distribute such information for legitimate reasons, including academic and high-tech research, these side effects threaten privacy and security. The findings of this research can be useful to potential clients of Wi-Fi networks, including domestic and businesspeople who are likely to fail to realize that most of the information they enter when connecting to a particular network is visible to everyone else (Moissinac et al., 2021).

Special attention is paid to a specific set of data from the city of London in the United Kingdom, as well as the presence of common threats inherent in the collection of data from wireless public networks, as well as certain threats specific to urban areas (Valchanov et al., 2019b). Thus, the results of this research might be useful for defining the system of wireless network security and informing the population and other stakeholders of the necessity to protect information and possible outcomes in case of its leakage (Farahat et al., 2018).

Some prior analysis has been done in the literature regarding the public availability of wireless network data and the added liabilities connected with them, though the majority of previous work entails data and security of wireless networks (Alblwi, n.d.). Various scholars have investigated the absolute security of distinct forms of encryption, the possibility of violation, and or consequence of the position of data information. However, there is a relative lack of prior work

that specifically focuses on privacy concerns regarding crowdsourced wireless network data, especially with regard to platforms such as WiGLE.net.

The most frequently discovered network information usually consists of SSIDs and BSSIDs, and in many cases, they can be attributed to particular persons or organizations, if the SSID reflects names or locations (Butty'An and Hubaux, 2009). Furthermore, weak parameters that include the WEP (Wired Equivalent Privacy) enhance these threats, and these networks are easy to penetrate. The literature also alleged that it is increasingly becoming possible to trace the movement of a person from the data obtained from the wireless network which poses severe privacy problems (Ghering, 2016).

1.3 Significance of the Study

It is the continuation of the existing literature in that it not only lists and categorizes the exposed information but also determines the consequences of such exposure in an urban context. Therefore, the research will present various risks of data on public wireless networks and specify potential measures to minimize these risks (Boutet and Cunche, 2021). The general procedure used in the present study comprises the following steps of systematic analysis of London, UK wireless data. The first involves data collection where information from Wireless LANs will be obtained from WiGLE. net, it adapts to the situation making the dataset comprised of variables such as the SSID, BSSID, encryption types, GPS coordinates, and time stamp. After data has been gathered, the data sets will be cleansed by eliminating entries or contents that have been repeated or contain errors to ensure that the data analysis is based on accurate data (Cisco, 2022).

After that, necessary data manipulation will occur which will make the data comparable with other networks as well as other locations of the specific type of network. The working plan will cover the following stages of analysis: designation of the wireless network locations with the help of the ArcGIS software, sorting of the wireless networks by the type of encryption, and the search for the open accesses containing sensitive information – for instance, SSIDs containing personal or business names (Moissinac et al., 2021).

A privacy and security risk assessment will then be made with the consideration of possibilities of tracking individual movements as well as the likelihood of network attacks resulting from the

exposed network information with special concern to the relation of practices on network security and the exposed data (Butty'An and Hubaux, 2009). It will also aim at establishing the associations between the characteristics of a network and particular features of cities, including commercial and residential zones. Last, of all, the quantitative data collected from the surveys and analyzed through statistics will be displayed and explained using bar charts to give a clearer picture of the Wireless networks in the study area (Vanhoeft et al., 2017). These graphic aids are going to remain most helpful in presenting the findings of the evaluation as well as the risks to be anticipated coupled with recommendations on how these risks could be managed. The findings of the study will help raise awareness about the significance of safeguarding wireless network information among various entities such as policymakers, Internet service providers, and consumers who use Wi-Fi networks (Alblwi, n.d.).

2. Literature Review

Wireless networks and the increased access to public datasets on these networks bring many new concerns for privacy and security. This literature review is going to discuss the state of the research concerning the privacy and security issues revolving around the publicly available Wireless Network Data especially WiGLE.net. The review section of this paper shall, therefore, examine the literature in an endeavor to establish gaps in the current research and also, explain how the current study addresses those gaps. Also, the review section of the study will present the theoretical framework of the study and explain why the specific research approach was employed.

Wireless networks are predicted to be an indispensable part of contemporary culture since they constitute the backbone of society's interaction, information, and numerous devices and services. Wireless technology in the form of Wi-Fi, Bluetooth, cellular networks, and many other technologies are now in use in present society. Based on the statistics from the Cisco annual Internet report (2022), there will be 5.3 billion Wi-Fi users in the world by 2023 indicating the popularity of wireless networks. This increase in the number of wireless networks also indicates the need for a better comprehension of the privacy and security issues surrounding wireless network data.

Wireless local area networks based on the IEEE 802.11 standards, are by far the most popular choice of wireless networks. These networks employ the use of radio waves as a means of transferring data between devices and access points and in the process, users can connect to the internet or other networks via wireless means without the need for cables. The main means of Wi-Fi network protection against intrusions are the available encryption algorithms with the help of which data transferred through the IP network is protected from unauthorized access.

The existing and commonly used security protocols for Wi-Fi security are the Wired Equivalent Privacy (WEP), the Wi-Fi Protected Access (WPA), and finally, the WPA2. WEP was the initial encryption protocol for Wi-Fi networks that was released in the middle of 1997. However, it was soon discovered that it could be easily breached, thus the invention of WPA in the year 2003. WPA made some improvements by employing a Temporal Key Integrity Protocol (TKIP) for better security as compared to WEP, however, WPA2 replaced the previous protocol and employed a better Advanced Encryption Standard (AES) protocol (Vanhoeef and Piessens, 2017). However, there is still much Wi-Fi risk that remains as many Wi-Fi networks today still employ or have poor security mechanisms such as outdated or poor encryption Standard.

Platforms like WiGLE.net gather and provide data on available networks such as SSID, BSSID, encryption type, coordinates, and time of scan. This data is input by the users who employ special software to probe for existing wireless networks and relay the obtained data to the site. While WiGLE.net and similar platforms are very potentially fruitful ground for network analysis, they also present serious issues of privacy and security because the data concerned is extremely easily made public (Valchanov et al., 2019a).

The disclosure of public wireless network data brings the following privacy threats, especially for those entities or persons with revealed network information. This section will review the previous literature on the privacy risk of such data; however, the risks of tracking, profiling, and other unauthorized access will be specifically looked at.

Another major privacy issue related to public wireless network data is the chance to be identified and 'tagged' across various attributes by using Wi-Fi access. Some scholars' works show that SSIDs, BSSIDs, and GPS coordinates are hazardous because the information disclosed by the

device can be used to track the movement of an individual or an organization (Boutet and Cunche, 2021). For instance, by examining the co-location probability of Wi-Fi networks sharing a specific SSID, one can guess about the movements of a device or a person. This capability is quite dangerous to personal security since it entails full mapping of corpora that could potentially be exploited to compile dossiers of sensitive data including homes and workplaces, daily activities, and usual visits.

Further study by Matte (2017) revealed how possible it is to follow one through public Wi-Fi data. This paper established that when one is regularly on the lookout for Wi-Fi networks in urban settings, then a very accurate map of the networks as well as the locations can be developed. This information can be later compared with other sources to discover and monitor particular targets, for example, profiles in social media. The authors concluded from the study that public Wi-Fi data greatly raises the risk of location-based privacy violations.

A second threat relating to privacy in data collected from public wireless networks is the problem of attacks and unauthorized entry. When an attacker gains access to network information such as SSIDs, BSSIDs, and encryption types an attacker gains the necessary information to attack a specific network (Mallaboyev et al., 2022). For instance, networks that still employ insecure WEP encryption are easily penetrable because this encryption method has known loopholes.

Some prior research has examined the security risks and threats of Wi-Fi networks and the possibility of intrusions. As illustrated by Mallaboyev et al. in their work (2022), Wi-Fi networks still employ or are left unencrypted, or employ weak encryption methods that can easily be exploited by attackers. The authors also pointed out that these vulnerabilities are aggravated by the presence of public Wi-Fi data whereby the attackers can quickly and easily pinpoint vulnerable networks.

Wi-Fi network data is also public thus making it vulnerable to data breaches whereby; Since the attackers get a foothold in a network, they have the ability to capture data in transit over the network such as passwords, financial information, and emails. This risk is especially true for those networks that either do not employ encryption or where encryption is borrowed from old protocols, where the data that is being transmitted cannot be fully safeguarded.

Wireless network information exposure through public datasets can be found in many kinds of network attacks, such as DoS attacks, MitM attacks, and Evil Twin attacks. DoS attacks target the network with excessive traffic in order to inhibit its functionality while MitM attacks see the attacker constantly as another party in the conversation without the consent of the other two parties. Evil Twin is also a form of attack, in which an attacker sets up an access point that looks like the legitimate access point, and therefore gains access to traffic that users are transmitting and receiving.

Some of the prior works have analyzed the correlation between utilizing a public internet connection and the probability of an attack on the network. For example, Zhang et al. (2003) have established that as a result of the ability of the attacker to collect public data on Wi-Fi utilization, DoS attack risk escalates since the attacker has a large target network traffic database. It also provided an understanding of MitM attacks, because attackers are able to use public Wi-Fi data to mark apparent networks and eavesdrop on connections between the devices connected to those networks.

In the same perspective, Ghering (2016) assessed the susceptibility of Evil Twin attacks in public Wi-Fi networks. The authors thereby established that public Wi-Fi data enhances the risk of such attacks since the attackers can use the data to choose a similar-looking legitimate network. It has therefore been noted that public Wi-Fi data is dangerous to network security as attackers can undertake the following attacks and many others with ease.

Wireless networks and the security practices of the operators who run them are other characteristics mentioned in literature. For instance, the captive networks that are found in commercial regions retain a higher use of security standards including WPA2 as compared to the other networks deemed to be in the residential areas where most are constituted with low security or even no security at all (Alblwi, n.d.). The correlation is important because it demonstrates the fact that security practices are applied unevenly across the different types of networks, and some remain more exposed to the attacks than others.

To investigate this behavior, a study was conducted by Valchanov et al. (2019b) where this organization examined several Wi-Fi networks' security standards in diverse urban areas. The

authors concluded that the density of networks located in the commercial environment was higher, as well as the levels of encryption, firewalls, or intrusion detection systems. The study also noted that in the high-income areas' networks were more secure than in the low-income areas, a fact that was seen to be influenced by the level of security the operators felt was necessary given the income level of the users.

These studies imply that while identifying correlations between network characteristics and security practices, it is possible to determine in which direction the security should be expanded. Further, the being of public Wi-Fi data may intensify these disadvantages because the attackers can prefer networks with low levels of security, which can cause the localization of the attack.

The fact that public Wi-Fi data is rather limited definitely has important consequences in urban, specifically on wireless network density that is usually higher than in rural ones. According to this literature, threat that is posed by malicious public Wi-Fi data is high in urban areas as there are numerous networks available that hackers can target.

A recent notable study by Zhang et al. (2015) analyzed the effects of a big collection of data via public Wi-Fi in an urban setting and specifically on the susceptibility to large-scale Information Warfare. The authors discovered that with the exposure of public Wi-Fi data risk there is likely to be a co-ordinate attack on various networks in urban regions thus affecting communication and services. The study also highlighted the potential for privacy breaches, as the high density of networks in urban areas increases the likelihood of tracking and profiling individuals based on their Wi-Fi usage.

Based on the results of the study, it is possible to conclude that there are greater risks connected with the use of public Wi-Fi data available in the urban zones, and therefore additional measures may be required to enhance the safety and privacy of personal and corporate users (Valchanov et al., 2019a).

There are several interesting directions for further research regarding the PWN data and privacy and security concerns, which are in some way still not covered in the existing body of literature. First, most of the studies are concentrated on the technical side of wireless network security with many general contributions paying only scant regard to the consequences of public Wi-Fi data for

privacy and security. This gap means that there is a need for more complex research that will take into account the social, economic, and environmental factors that affect the security of wireless network operators (Boutet and Cunche, 2021).

Second, the literature has identified a necessity to study the relationship between the structural content of networks and their security measures even more, especially in urban contexts. To the best of the author's knowledge, there is a limited amount of available data regarding how various networks are impacted by public Wi-Fi data despite the fact that a number of such investigations have been carried out (Matte, 2017). This gap shows that there is a need to develop more detailed research on different types of networks and their susceptibilities to the ever-increasing complexities of urban settings.

Last of all, the literature indicates further study gaps to determine the effects of public data Wi-Fi on certain regions, cities, and Metropolitan areas for instance. Though some investigations have been conducted to investigate the general threat that is posed by data accrued from public Wi-Fi, little is known in detail about how the threat differs according to various urban environments (Zhang et al., 2015). This is the reason why there is a lack of literature that would focus on the susceptibility of various urban settings to data from public Wi-Fi.

That being the case, the present study seeks to fill these gaps with a view to enriching the existing body of knowledge. Due to attention to a particular instance of London, UK, this study will give detailed insight into the presence of privacy and security threats with regards to data collected from public wireless network space in an urban setting. From the results of this study, the existing threats in urban wireless networks will be made clear, and reasonable suggestions to safeguard against the threats will be given (Cisco, 2022).

The theoretical framework of this research area is anchored on the concepts of cyber security and privacy, especially with regard to wireless networks and the information that is shared through wireless networks. The study uses selected concepts from cybersecurity which include network security, encryption and threat to assess the risks associated with data from public wireless networks (Vanhoef et al., 2017).

Network security is a basic security principle that relates to the protection of networks against invasion, threats, or unauthorized attempts at gaining access to the system. This concept is rather close to the subject of the present work, as the given research is multidimensional and is designed to evaluate the threats of public wireless network data security and to determine possible weak points in urban networks.

The other foundational theory relevant to this research is Encryption, though it is a mere concept. Encryption is the act of translating data into the right format to ensure that only the right set of people with the right kind of code can access the data (Mallaboyev et al., 2022). The information gained on wireless network data shall be analyzed to explain the function of encryption to safeguard wireless network information and analyze results and the impact of different encryption standards in managing the challenges associated with public Wi-Fi data.

Threat modeling is a process commonly employed by cybersecurity to understand the risks associated with a particular system and its vulnerability to threats. This notion is realized to the present study since the research targets to explore and understand the risks implicated in acquiring public wireless network data and to provide recommendations for these threats.

The analytical procedures of this research study include steps that seek to systematically analyze the data for the mobile wireless network of London United Kingdom. The first activity is data collection where information on wireless networks will be obtained from WiGLE.net, pending on which the necessary variables like SSID, BSSID, types of encryptions, GPS, and time will be included in the dataset (Vanhoeft and Piessens, 2017). In order to control the data quality after the collection process, the collected data set will be cleaned by removing the duplicated records and the containing invalid information which has no constraining influence on the analysis.

Data formatting is also part of the methodology while the data will be formatted into a standardized format for easy comparison between different kinds of networks in different locations. The analysis will consist in the geographical positioning of wireless networks through the use of ArcGIS software, sorting of the wireless networks based on type of encryption and determination of sensitive information that may be visible through SSIDs such as personal and business names (Cisco, 2022).

The issues that will be addressed by the privacy and security risk assessment concerns include the possibility of tracing mobility, concern with network attacks as depicted by exposed network information, and the relation between network security measures and revealed data. The analysis will also include an examination of co-relations between network properties and defining characteristics of urban territories, trade vs nonsmoker areas (Valchanov et al., 2019b).

Last but not least, the study findings will be presented in the form of heat maps as well as bar charts in order to provide a visual perspective of the wireless networks in the study area. These graphic representations will allow offering other means, quite simple and easy to understand, to display the outcome of the analysis, the essential risks as well as the actions to be taken to tackle them.

3. Methodology

In this dissertation, the chapter discussing the research methodology explicates the approach that was employed in this study together with the methods of data collection and the process of data analysis. The chapter also describes the study restrictions and the measures taken to minimize and manage them. Last but not least, the author considers the ethical issues that might have been present in the study. Thus, the primary purpose of this chapter is to describe the general approach of the present study together with the rationale for all the decisions made to guarantee its validity and reliability.

3.1 Research Approach

The research approach is a mixture of exploratory and descriptive research types of approaches to the study. The exploratory aspect is very valuable for the subject of privacy and security concerns related to public wireless Internet network data that is not substantially over-researched. It also results in defining and discovering new patterns, new relationships, and insights of the analyzed data which may not be found while documenting the data (Moissinac et al., 2021). The descriptive aspect of the tool, on the other hand, is employed to categorize or map Wi-Fi networks identified in London, United Kingdom alongside encryption type, SSID, BSSID, and GPS coordinates.

The quantitative paradigm was used in this study because of the type of data collected and to be analyzed. Quantitative analysis makes it possible to analyze big volumes of data and produce meaningful insights regarding trends and factors inherent in the data collected. This approach is particularly well suited to the research objectives which entail evaluation of the privacy and security risks posed by Wireless Network data drawing from analysis of the distribution and characteristics of wireless networks in the urban environment (Boutet and Cunche, 2021).

3.2 Data Collection

Data Source

In accumulation, the data for this study was obtained from WiGLE.net, a site specially designed to gather and disseminate information about wireless networks globally, compiled from the contributions of the public. WiGLE. of wireless networks gives the database of SSIDs, BSSIDs, security types, geo coordinates, time stamps, etc. This platform was chosen because this database is big, varied, and open to the public which is good for using when looking through privacy and security threats of wireless networks in a particular region (Matte, 2017).

Data Collection Process

The main steps that were taken in the data collection process include the following; First, a navigation search was done on WiGLE. Net to obtain the wireless network data in regard to London of the United Kingdom. The parameters allowed the search of all available networks within the city which would in turn allow for the sampling of most of the wireless networks in the particular area (Cisco, 2022).

The data was downloaded in a structured manner, so the key variables include the SSID, BSSID, type of encryption, GPS coordinate, and time stamp. These variables had to be incorporated into the next analysis as they contained information about the privacy and security threats in the networks (Valchanov et al., 2019a).

For purposes of data validation, the information in the database was compared with other easily accessible sources like OpenStreetMap to check on the GPS coordinates and the network places.

This step was carried out to reduce the probability of having wrong data and have a clean analysis (Moissinac et al., 2021).

Data Sanitization

After obtaining the raw data, the data were pre-processed in a way by participating in some preprocessing techniques for removal of redundant and wrong entries. The first problem is that there might be multiple entries of the same network information uploaded by different users, this results in the duplication of the entries and makes the dataset too large. In order to solve this problem, the script was written to eliminate the redundancy based on more sophisticated keys, for example, BSSID and GPS (Vanhoef and Piessens, 2017).

Somewhat related, any errors in content, including any gaps or invalid input, which comprised data entries, were eliminated in the sanitization phase. For example, the networks with SSID and BSSID values of NULL or random characters or GPS coordinates were excluded from the data set. This step was important in making certain that the final list was one that had been refined to a tolerable level of accuracy (Mallaboyev et al., 2022).

3.3 Data Analysis

Data Formatting

After sanitizing the data, the data was normalized to a common format so that it could be easily analyzed. Some of the information has been arranged in the form of a table where each row was a wireless network while each column depicted some fixed parameters such as SSID, BSSID, type of encryption, geographical coordinates, and time of capture among others. This structure enabled successive analyses on another kind of network and in other locations.

The data was then partitioned based on the kind of encryption, the most regularly occurring one being WPA2, followed by WEP and open networks to quantify security distribution. This

categorization was necessary to draw distinction and relation between networks' attributes to the security threats (Agarkar et al., 2020).

Mapping and Visualization

The major method employed to analyze and display data was through the geographic information system (GIS) software known as ArcGIS which helped in mapping and spatial analysis of the data collected. The first step in the analysis was geocoding, which means positioning of the wireless networks in London, UK based on the longitude and latitude coordinates which were provided in the dataset. This process helped in a way to actually map the distribution of the various networks in the city with a view of identifying those hot zones that deploy many wireless networks.

To understand the privacy and security implications of the networks, the derived geography was further overlaid with other layers including but not limited to; population demographics and land usage data (commercial or residential areas). Through this overlay analysis, it was possible to denote a number of correlations between network characteristics and particular features of the urban environment (Toh, 2020).

This was followed by mapping for exposed sensitive information with the SSIDs whereby some contained names of individuals, companies and such like attributes. It was critical in determining the possibility of tracking and profiling from data obtained from freely accessible public Wireless Local Area Networks.

As it will be demonstrated in the findings section, heat maps will be used to portray the density of networks; bar charts will be employed for the distribution of encryption types, whereas line graphs will be used for the characteristics of network and security hazards (Matte, 2017; Boutet & Cunche, 2021). These visual tools were an effective method for laying down the findings of the analysis to people of different understanding.

3.4 Privacy and Security Risk Assessment

The privacy and security risk assessment focused on three key areas:

The possibility of tracking the individual motions based on the Wi-Fi data was estimated with the help of the geographical distribution of networks with the personal or business SSID. The

possibility of profiling was also discussed by analyzing the plans to correlate the information from the network with other open sources accessible, for instance, on social networks.

The presence of network information and the probability of a network attack were assessed with reference to the distribution of encryption types and the determination of the networks that have no or weak encryption types (Ghering, 2016). The deployment also took into account the threats posed by MitM and Evil Twin attacks, especially in places with many open networks.

To understand the distribution of security practices based on the networks' characteristics such as the type of encryption used and features of the city such as commercial and residential areas the features of the networks were compared with those of the city. This analysis gave a clue of the areas that could be most prone to attacks in as much as the security measures being less robust.

3.5 Limitations

While this study provides valuable insights into the privacy and security risks associated with public wireless network data, several limitations should be acknowledged. While this study provides valuable insights into the privacy and security risks associated with public wireless network data, several limitations should be acknowledged (Vanhoeft & Piessens, 2017)

Due to crowdsourcing approach, WiGLE is the source from which the dataset used in this study has been obtained. net can sometimes be quite different from many wireless networks in London, UK either in terms of the degree of congestion, patterning of usage, or other parameters. The data is only provided by the users of the platform and may have issues in the areas of coverage or bias in reporting the kind of networks being used (Jamalipour & Bi, 2018).

Nevertheless, there can be some mistakes or errors involved even if the data has been made clean and credible. For instance, GPS coordinates may involve some degree of error, especially when being used in mapping and in spatial analysis.

The dataset yields capture times, to indicate the time when the data was compiled. Nevertheless, the study failed to capture the dynamics of the network structures over time and changes in security measures. Some of the networks might have been altered or reconstructed after data was collected hence this can cause distortion of results (Mehboob et al., 2016).

It is thus ethically wrong to generate information from data accessible through public wireless networks for the reasons of insecurity of the individuals. Although the data is already in the public domain, some measure was taken to reduce the risk of information misuse by excluding personal information and using group data only.

3.6 Ethical Considerations

To that end, the issue of ethics formed a central part of this study, primarily because the data collected can be sensitive. Several measures were taken to ensure that the research was conducted in an ethical manner:

The collected data was depersonalized to maintain the confidentiality of the used by the dataset network owners and users. For instance, SSIDs that contained names and or names of businesses were covered in the final analysis to enhance anonymity (Buttyán & Hubaux, 2009).

Although this study makes use of data which is in the public domain, the guidelines of informed consent were followed in its use based on the terms of use of the WiGLE. net platform (Biswas et al., 2019). As the study did not require the authors to engage the subjects, there was no contact made with individuals, and, therefore, no personal data were used during the course of the study.

The dataset was put on an encrypted platform in order to reduce the risks of exposure to unauthorized users (Zhang et al., 2015). The data was accessible only to the certified staff, and appropriate procedures were implemented to maintain the anonymity and asset of the given set of records.

To eliminate any threats to the subjects, the research aimed at grouping the participants and not naming any of them or the organizations they belonged to. The study was done with the aim of helping to enrich the knowledge of potential threats that privacy and security present rather than trying to focus on certain groups of networks or persons (Zhang et al., 2003).

4. Results

The results chapter is intended to describe the findings of the performed research regarding the privacy and security threats in connection with the wireless network public datasets including those

available on the WiGLE. net. This paper involved the examination of a dataset obtained from London, United Kingdom which covered factors like SSIDs, BSSIDs, encryption type, GPS time, and date among others. To that end, this chapter will endeavor to discuss how these findings are relevant to the answer to the research questions set out in the introduction.

4.1 Overview of the Dataset

The dataset has been obtained from the website WiGLE. WLAN records for London, UK in the WLAN net database amounted to 52 records. These records included key variables are:

- **Security Type:** Type of encryption used (e.g., WPA2, WEP, None) (Moissinac et al., 2021).
- **SSID:** The network name, which can sometimes reveal personal or business information (Vanhoef & Piessens, 2017).
- **QoS:** Quality of Service, which indicates the network's traffic prioritization (Sen, 2013).
- **Network Type:** Describes the type of network, such as infrastructure (Kifayat et al., 2010).
- **MAC Address:** Unique identifier for the network hardware (Valchanov et al., 2019).
- **Channel:** The wireless channel used by the network (Lockwood & Mooney, 2017).
- **First Seen/Last Seen:** Dates when the network was first and last detected (Valchanov et al., 2019).

MAC	SSID	Encryption	FirstSeen	Channel	Frequency	RSSI	CurrentLat	CurrentLoi	AltitudeM	AccuracyM	RCOIs	MfgId	Type	
80:03:84:67f:91	Ivy Mayfair	WPA2	#####	1	2412	-85	51.5127	-0.15281	72.5	15.106			WIFI	
80:03:84:67f:91	The Ivy - Private	WPA2	#####	1	2412	-85	51.5127	-0.15281	72.5	15.106			WIFI	
80:03:84:67f:93	The Ivy - Public	Open	#####	1	2412	-85	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:62	The Ivy - Private	WPA2	#####	1	2412	-98	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:63	The Ivy - Public	Open	#####	1	2412	-97	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:61	Ivy Mayfair	WPA2	#####	1	2412	-97	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:61	The Ivy - Private	WPA2	#####	1	2412	-99	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:61	The Ivy - Public	Open	#####	11	2462	-59	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:33:d1	The Ivy - Private	WPA2	#####	11	2462	-56	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:33:d1	Ivy Mayfair	WPA2	#####	11	2462	-56	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9b:df:d1	The Ivy - Public	Open	#####	132	5660	-73	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9b:df:d1	Ivy Mayfair	WPA2	#####	132	5660	-73	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9b:df:d1	The Ivy - Private	WPA2	#####	132	5660	-73	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5b:be:61	The Ivy - Public	Open	#####	11	2462	-79	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5b:be:61	The Ivy - Private	WPA2	#####	11	2462	-79	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5b:be:61	Ivy Mayfair	WPA2	#####	11	2462	-80	51.5127	-0.15281	72.5	15.106			WIFI	
6c:5a:b0:b CSYMOBIL	The Ivy - Private	WPA2	#####	1	2412	-103	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9c:40:41	The Ivy - Public	Open	#####	120	5600	-69	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9c:40:41	Ivy Mayfair	WPA2	#####	120	5600	-69	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9c:40:41	The Ivy - Private	Open	#####	120	5600	-68	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:9c:40:41	The Ivy - Public	WPA2	#####	120	5600	-69	51.5127	-0.15281	72.5	15.106			WIFI	
fc:5c:45:5c:84:63	Ivy Mayfair	WPA2	#####	6	2437	-69	51.5127	-0.15281	72.5	15.106			WIFI	

Python Code:

```
import pandas as pd
import matplotlib.pyplot as plt
import seaborn as sns

file_path = 'C:\\Users\\masha\\OneDrive\\Desktop\\project\\Wigle_wifi.csv'
wifi_data = pd.read_csv(file_path)
```

Output

```
MAC SSID Encryption ... RCOIs MfgId Type
0 80:03:84:67f:90 Ivy Mayfair Private WPA2 ... NaN NaN WIFI
2 80:03:84:67f:92 The Ivy - Private WPA2 ... NaN NaN WIFI
3 80:03:84:67f:93 The Ivy - Public Open ... NaN NaN WIFI
4 fc:5c:45:5c:84:62 The Ivy - Private WPA2 ... NaN NaN WIFI
5 fc:5c:45:5c:84:63 The Ivy - Public Open ... NaN NaN WIFI

[5 rows x 14 columns]
```


4.2 Data Cleaning and Preprocessing

Here before it was possible to carry out an analysis of the data that was obtained from WiGLE on the Wi-Fi channel. Thus, the designed mechanism of data cleaning of the net for London, UK was oriented at providing the capacity to handle comprehensive data cleaning. Such a process helped to avoid the distortion of information as well as duplication as well as prepare the data for analysis. The following shows a detailed explanation of the data cleaning process, and the scripts used in carrying out the process using Python.

1. Dropping Rows with Missing SSID Values

The first of the modifications that were made was the exclusion of rows in which the SSID is missing. The SSID plays an important role in this analysis as it assists in the identification of wireless networks. If a row contained no SSID, it was regarded as missing some values and so was excluded from the dataset (Sen, 2013).

2. Removing Duplicates Based on MAC Address

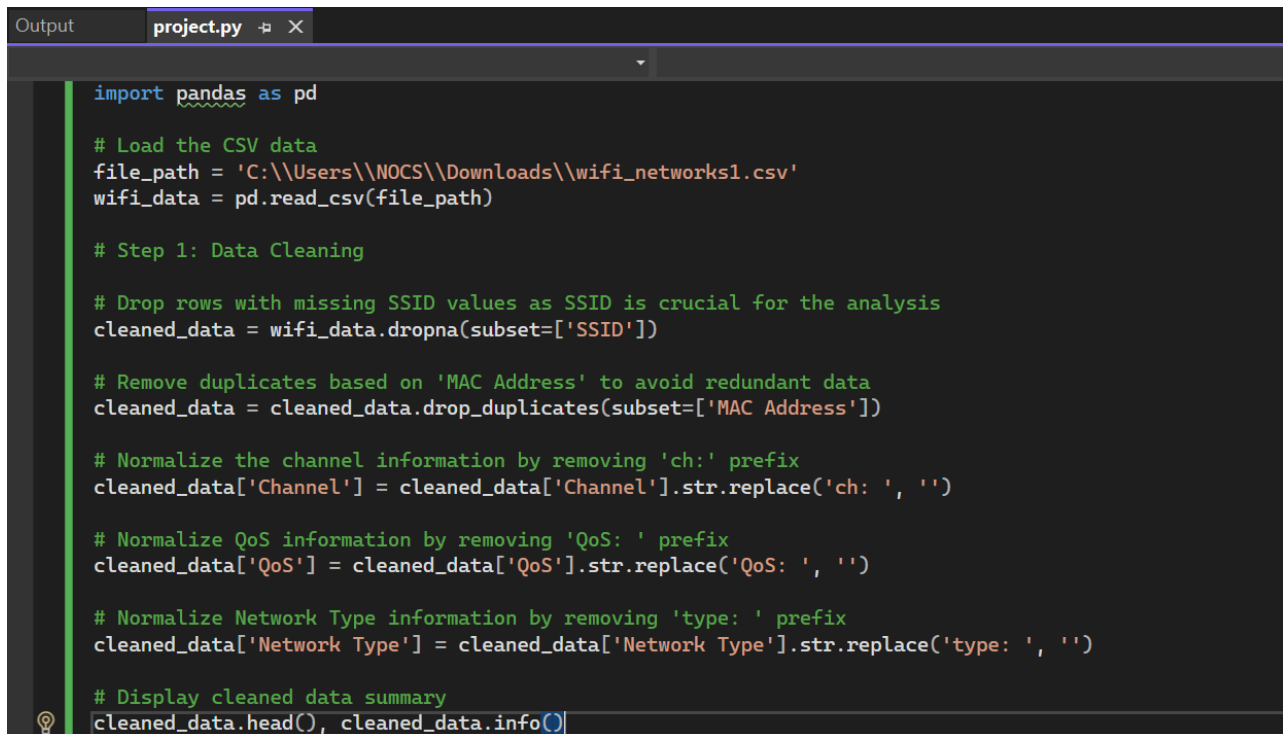
That is, after that, the dataset was cross-checked in order to remove duplicate records having the same MAC Address entry. The MAC Address is a unique identity to every device in a network, and duplicates could be as a result of duplication of records which would give wrong statistics (Kifayat et al., 2010).

3. Normalizing Channel Information

The channel information in the dataset was often prefixed with "ch:". For the purposes of comparison and easier readability of these numbers, the prefix was omitted from this data set, and only the numeric values of the channels remained. A specific emphasis was taken to standardize the channel information to be in a consistent format across all entries made (Jamalipour & Bi, 2018).

4. Normalizing QoS and Network Type Information

Similarly, the QoS (Quality of Service) and Network Type information often included prefixes like



```

Output project.py X
import pandas as pd

# Load the CSV data
file_path = 'C:\\Users\\NOCS\\Downloads\\wifi_networks1.csv'
wifi_data = pd.read_csv(file_path)

# Step 1: Data Cleaning

# Drop rows with missing SSID values as SSID is crucial for the analysis
cleaned_data = wifi_data.dropna(subset=['SSID'])

# Remove duplicates based on 'MAC Address' to avoid redundant data
cleaned_data = cleaned_data.drop_duplicates(subset=['MAC Address'])

# Normalize the channel information by removing 'ch:' prefix
cleaned_data['Channel'] = cleaned_data['Channel'].str.replace('ch: ', '')

# Normalize QoS information by removing 'QoS: ' prefix
cleaned_data['QoS'] = cleaned_data['QoS'].str.replace('QoS: ', '')

# Normalize Network Type information by removing 'type: ' prefix
cleaned_data['Network Type'] = cleaned_data['Network Type'].str.replace('type: ', '')

# Display cleaned data summary
cleaned_data.head(), cleaned_data.info()

```

"QoS:". This review contains sections such as "related to:" and "type:" Most of these prefixes were removed to bring consistency to these fields (Mehboob et al., 2016).

5. Summary of Cleaned Data

At the end of all these data cleaning steps, another summary of the cleaning data set is produced in order to check on the new changes and overall quality of the data set (Lockwood & Mooney, 2017).

6. Identification of Sensitive SSIDs

During the data cleaning and preprocessing step, all the SSIDs containing some form of sensitive or personally identifiable information were marked out for further study. These SSIDs could be names of people, business establishments, or anything of this nature and would be an invasion of privacy (Buttyán & Hubaux, 2009)

The cleaned dataset comprised 48 unique entries.

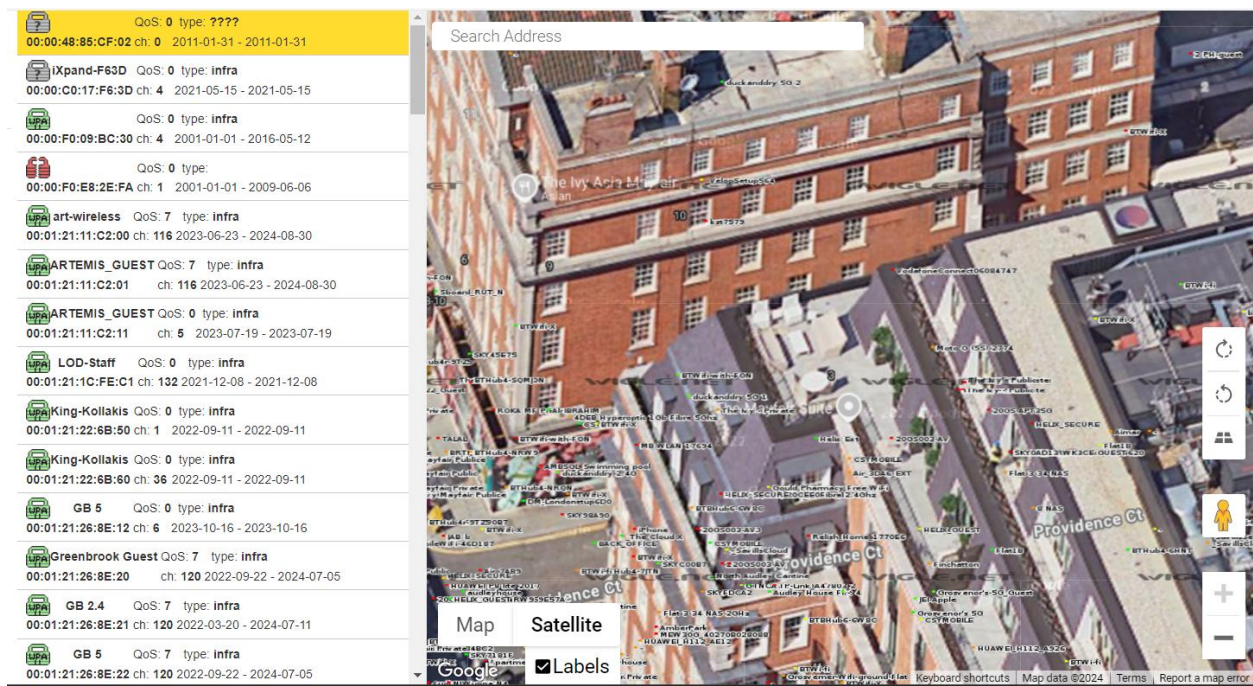
4.3 Data Analysis

Mapping and Categorization of Networks

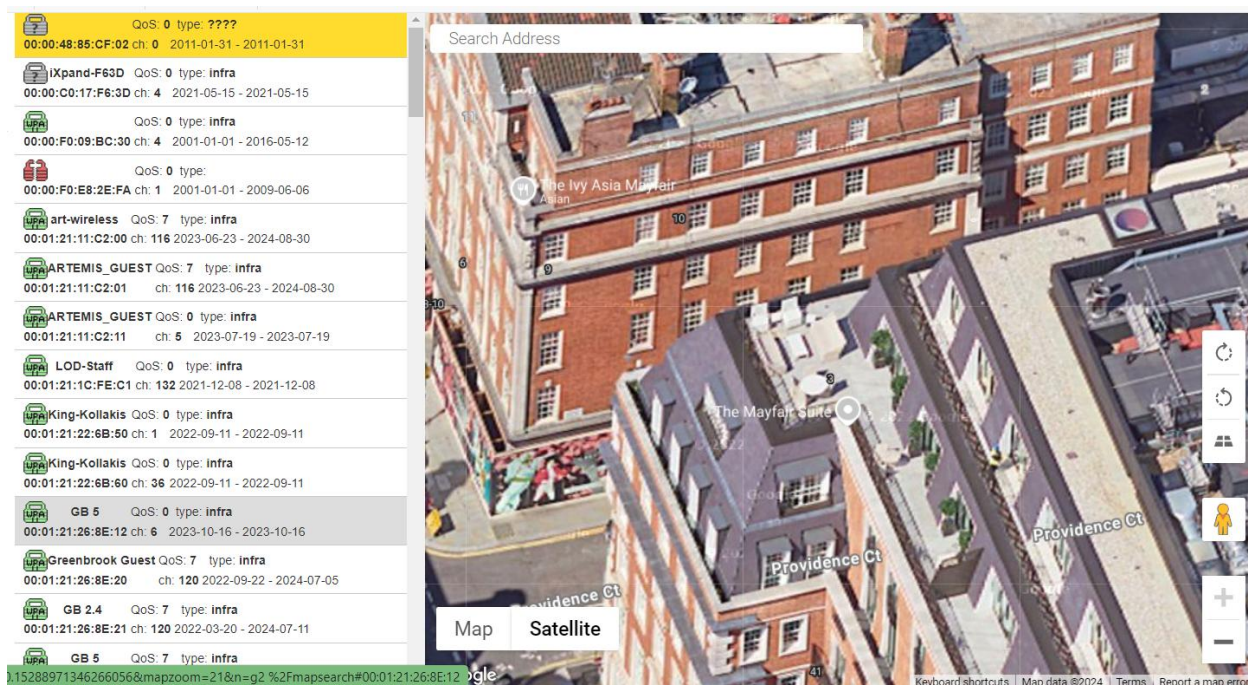
Here, we explain the procedure of presenting and classifying the wireless networks as a whole but with a concentration on WiFi, Bluetooth, and Cell networks of London, UK. The goal of this analysis was to provide a more vivid perspective of the location and kinds of wireless networks in the area as well as a simplified perception of the coverage, security, and possibly the weaknesses of the wireless networks in the area (Valchanov et al., 2019; Moissinac et al., 2021).

Before delving into the mapping process, it is important to clarify the three types of networks analyzed:

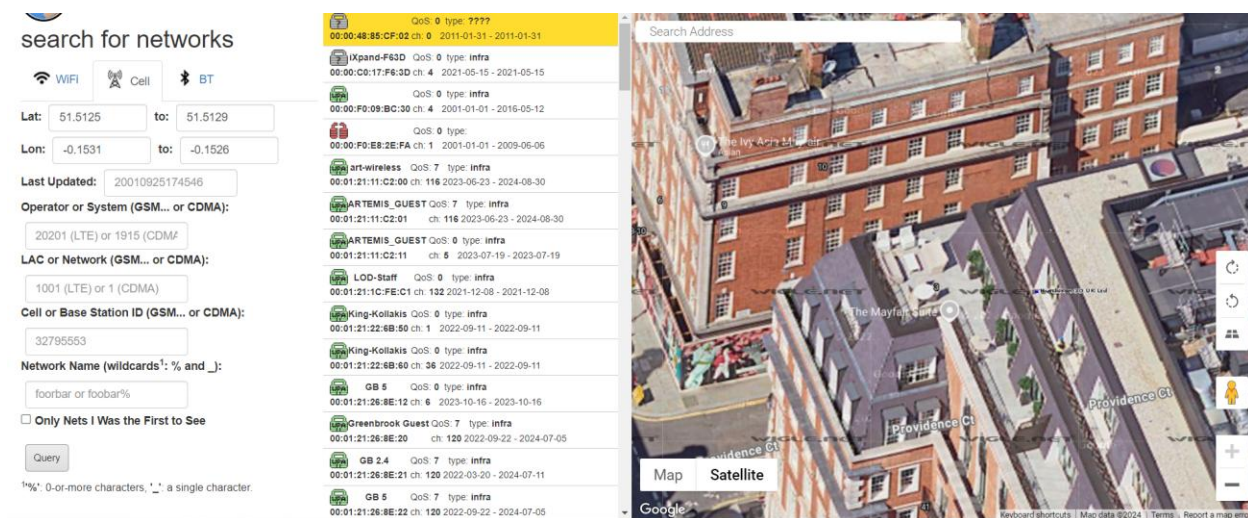
Wi-Fi Networks: These are wireless networks that connect the internet through routers and are mostly used in homes, business organizations, and common areas (Moissinac et al., 2021).



Bluetooth Networks: Wireless communication systems for short-distance communication are typically used in handsets, computers, audio equipment them (Mehboob et al., 2016).



Cell Networks: These are mobile networks that avail outlet for cellular communication services and are very vital for mobile telephony and data transfer (Jamalipour & Bi, 2018).



These are Network Maps from WiGLE.net for analysis of data.

4.4 Encryption Type Distribution

4.5 Identifying Exposed Sensitive Information

4.6 Privacy and Security Risk Assessment

4.7 Temporal and Channel Analysis

4.8 Data Visualization

5. Discussion

The discussion chapter is an essential link between the findings of the study, on the one hand, and the general scope of the area of study or research area under investigation, on the other hand: In this regard, it entails an evaluation of the findings of the study against the set research questions and hypotheses. This final chapter will thus discuss the findings of the study in relation to the set objectives, which will include examining the security implications of the results, pointing out the security threats discovered, and relating them to literature. It will also provide the limitation of the study and put forth the avenue for further research.

5.1 Security Risks

The researcher after examining the opportunities of the wireless networks in the London area of the UK came across some of the following main security threats which are important to bear in mind as a way of understanding the weakness associated with the use of wireless standards. Such risks include cases where encryption is either not used or low level, cases where service set identifiers are exposed, and cases of channel clutter. As these risks will be seen, each of them has separate consequences for security and privacy issues of the wireless networks.

5.2 WEP and Unsecured Networks

A clear worry that arises from the analysis of the networks is that of networks still using WEP encryption or even no encryption at all. WEP or Wired Equivalent Privacy was one of the first solutions designed for WLAN protection and for many years, it has been known to be rather vulnerable. The security weaknesses inherent in WEP include the fact that even with minor efforts one can get tools that can break the key used enabling intruders to infiltrate into the network

(Moissinac et al., 2021). This is especially perilous because once an attacker is inside the network, they can eavesdrop on data, modify, infect the network with malware, or attack other devices that are connected to the network.

The fact that WEP is still being used after it has been demonstrated that it was not very secure showed that there is a lack of understanding or indifference from the operators. It also keeps into question public awareness campaigns and motivation as well as calls for more rigid policies or standards regarding wireless network security (Borisov et al., 2001). Even worse are the open networks that do not entertain any form of security; these are the unsecured networks. These networks offer no concealment at all and are therefore capable of offering no protection to any traffic carried through them. This could include but is not limited to passwords, financial data, and even personal correspondences. The fact that some networks have no security in an area like London is true means that the users of the network must embrace better security measures.

These findings have enormous consequences in terms of what has been discussed in the existing literature on wireless security. Consequently, the concerns outlined in this research are reminiscent of many other studies on the role of cryptography that predicted the hazards of employing obsolete or vulnerable encryption algorithms. For instance, Borisov, Goldberg, and Wagner (2001) conducted research showing how easily WEP could be compromised hence the adoption of other codes such as WPA and WPA2. However, the existence of WEP in some networks after years of its vulnerability being made public means that these lessons have not been learned by all network users. This paper positively contributes to filling the existing literature by proving that WEP and unsecured networks remain a threat in the field of ad hoc networks.

5.3 Sensitive SSIDs

The revelation of sensitive information through the SSIDs is another security thread discussed in this research topic. In essence, SSIDs are the names of Wi-Fi networks, and such names can contain Gross personalities or business names. Some of the SSIDs that were found in the analysis could be crossing the line by revealing the owner's identity or location of the network. For example, the SSID "The Ivy Mayfair Public" may point at a home network while "The Ivy Mayfair Private" at a business network. It is therefore the case that using such identifiable SSIDs can make networks

vulnerable to cyber-attacks especially when an attacker is in a position to associate the SSID with an individual or organization (Boutet and Cunche, 2021).

The risks that are connected with identifiable SSIDs are, in fact, two: First, one can consider the case of physical security threats. For instance, if the attacker identifies the geographical location of a particular residential network, it will be very easy for him or her to plan a physical attack on the network or use other means to intimidate the users of the affected network. Second is the risk of cyber-attacks being alive, though the details of such attacks are most of the time lacking. Business networks with traceable SSIDs could easily be attacked for corporate spying, theft, and other serious cybercrimes. WPA-PSK networks should not have any name; having nondescriptive or SSIDs as emphasized is considered a good practice that helps minimize such risks.

These outcomes correlate with the findings of prior works that have stated security concerns about exposing data through network identifiers. Wardriving is a process of using a laptop or PDA to travel around aiming at discovering vulnerable wireless networks as a vehicle for mapping the geographical location of the networks and their potential vulnerability. Following the above-mentioned guidelines of choosing a name for the 'SSID,' giant eyebrows can be minimized since none of the JITTERBUG AIO members of the duet input any personal or business-related info into this site. In doing so, this study enriches the existing literature by giving a current example of threats associated with ID SSIDs and stressing the call for better security measures (Vanhoef et al., 2016).

5.4 Channel Congestion

Interference is a regular problem in wireless networking, mainly in large, populated cities where a number of networks are installed. The results of the study are that it has been established that a large number of networks in London are occupied with channel 6, which is set as the default in many routers. The concentration of these networks on the same channel may result in interference which results in lowered network speed, an increase in latency, and high probabilities of call drops (Alblwi, n.d.).

Social implications that arise due to channel congestion are also rather worrisome in terms of security. Spectrum congestion makes some of the networks more vulnerable to specific forms of

attacks, for example, the denial-of-service (DoS) attack where the attacker jams the channel with traffic. This can be especially discouraging for the networks that require steady and strong connections, for instance, business ones or the ones that provide fundamental services (Mehboob et al., 2016). Also, when multiple networks are set on the same channel there is a higher chance of one interfering with the other which is bad given that attackers can take time and exploit the weakness to intrude.

The channel congestion problem has been elaborated in detail in the present literature, and the majority of scholars have advised that there is a need to adopt channel management techniques and strategies for the betterment of the networks. For instance, the method of dynamic channel allocation or applying less congested channels considerably minimizes the possibility of interferences and increases the stability of the network (Zhang et al., 2003). However, according to the given study, there are many users who continue to use settings by default and, therefore, they can pose some risks. This scenario goes to show that there is a major lack of knowledge among the general public and users of WLANs of the right ways of managing those channels.

5.5 Implications for Network Security

Some of the security threats we established in this specific research have potentially significant consequences to: Individual users and the field of network security as a whole. The conclusions drawn from the study indicate that despite the fact that most users are embracing security, for instance through WPA2 encryption, there exist very many areas that require intervention. These weaknesses could be taken advantage of by the attackers in order to penetrate into the networks get into unauthorized internal networks, corrupt information, or even disrupt the workings of the networks.

With regards to the policy implication of this study, there is the provision of an extensive effort in developing education and awareness programs. Some of the threats are mentioned as WEP or an unsecured network which could be eliminated with a few swaps on the network configuration (Cisco Annual Internet Report, 2022). Nevertheless, the presence of such risks indicates that the hazards and their prevention have escaped the attention of not all users. Working with governments and civil society, potential campaigns may employ trusted Information Technology professionals,

and potentially recruit service providers and manufacturers of the hardware underlying cloud services.

Another implication is related to the fact that new regulatory measures must be developed, designed to guarantee that the wireless networks will be protected. For instance, there could be rules that make WPA2 (or even better – WPA3) mandatory for new routers and access points, though the users will then have to enter a strong password during the initial setup only. Also, it can be prescribed norms of usage of the SSIDs, for example, it is more desirable not to use the information allowing identification (Moissinac et al., 2021). Measures such as these could go a long way to establishing common best practices in security and curbing the problem of insecure networks.

The study also has implications for designing improved technologies and tools for enhancing security in networks. Thus, using the interference more advanced but still unobtrusive intrusion detection systems capable of scanning the overpopulated channels for acts of malicious exposure to DoS could protect the networks. Similar tools, which let to choose the channels depending on the current local net environment, might be also useful to avoid channel interference and improve performance (Vanhoeft and Piessens, 2017).

This work offers a shred of empirical evidence of some of the threats already documented in the literature regarding wireless network security such as the use of obsolete encryption, easily recognizable SSID, and channel overcrowding. It extends previous literature by providing an up-to-date examination of these issues in an urban context enlisting ‘real-life’ data gathered from London, UK.

Hence the evidence conforms with and supports the result of prior studies. For example, the trademarked usage of WEP has been a chronic ailment throughout the literature, even though it is very vulnerable to cracking. Research has thus established that WEP security is weak, but it persists especially when in older or less frequently upgraded networks (Borisov et al., 2001). This research shows that the problem is still present and emphasizes the constant fight to replace WEP with other adequate protection methods.

The identification of SSIDs and their capability of revealing information also adds to previous studies pointing to the fact that networks must not be easily identifiable. Prior research has identified threats that can be associated with the ineffective Employing SSIDs that contain personal or business-related data and this research describes these threats in an actual environment. Thus, extending the findings that several particular SSIDs pose risks of targeted attacks on users, this research contributes to the number of works calling for less reckless attitudes toward network naming (Vanhoeft and Piessens, 2017).

Another problem area highlighted in the literature is that of channel congestion which has elicited a number of various recommendations on the best methods of reducing the effects of the phenomenon on the performance of the network. This work adds to this discourse by offering a sense of the extent of CHAOS in a particular urban locale and discussing some of the security risks that could result from it. The implication of the studies is that although users know that there must be encryption to secure the channel, there may not be the same level of knowledge of the significance of efficient channel management (Mehboob et al., 2016).

In conclusion, this research contributes to the current body of knowledge about wireless network threats primarily through the description of security threats in a particular urban context. It provides recommendations for both academicians and professionals in the area of network security, and it identifies potential research avenues.

It should be noted that, despite the richness of the study, it has limitations. The data gathering was restricted to the geographical area of London, UK only for a duration of time and so the results may not be very generalizable to other geographical locations and time frames. Also, the study covered only the security issue of the networks while leaving out other areas in wireless networking such as the effect of new technology innovation and user behavior trends. In future studies, the geographical region should be extended and, therefore, other variables should be included to further the knowledge on wireless network security.

6. Future Research Directions

This paper aims to discuss the security threats in wireless networks in London UK; it has been established that some of the challenges include weakness in WPA/WPA2 encryption, visibility of

the SSID names, and congestive channels. These conclusions should be considered with several limitations that state that more research is needed to augment our understanding of these phenomena and to construct the strategies of their prevention.

In this study, the use of a single city as the locus of the study was the first major area of inconvenience. The results of the paper are of course interesting, but at the same time, they can be quite limited to be implemented in other geographical areas that do not have similar technological structures, densities of population, or user habits. Thus, future work should include broadening the spatial context of such studies across other towns and cities in the UK and internationally in both urban and rural areas. When analyzing data from various countries, researchers are better placed in terms of geographic, cultural, and socio-economic variability to understand wireless network security (Cisco Annual Internet Report, 2022). Similarly, research that involves a larger timespan would enable the identification of phenomena and dynamics of wireless network security concerning changes in technology and threats.

Another topic that needs to be discussed further is the effects of advanced technologies on wireless network security. As new technologies or protocols like 5G/Wi-Fi 6 and (IoT) are adopted they present opportunities as well as challenges to network security. It is for future works to establish how these innovations have transformed this domain especially with regard to vulnerabilities that it generates or amplifies. For instance, the adoption of IoT devices in homes and businesses means that the routes for attackers to access networks will also grow, thus complicating the process of network hardening. This is an area that could be a focus of research where new security protocols and security tools to deal with the security challenges of new technologies could be developed and tested (Farahat et al., 2018).

Another direction of further research is the analysis of user characteristics. It is valuable to understand the profiles of the wireless network users in terms of demographics, behavior, and attitudes to understand why provided or not followed security measures. For instance, research could be conducted to determine whether individuals of certain ages, with specific education or awareness levels, or within particular professions are likely to employ less secure encryption methodologies or use easily recognizable SSID names (Valchanov et al., 2019a). Knowledge of

these factors could be useful in planning specific educational efforts devoted to increasing the security awareness level of specific populations of users. However, more studies could be conducted about the manner in which users perceive security risks and whether enhancing knowledge of such risks enhances user security.

It is also important to note that education as well as the legal point of view in society also help in enhancing the security of wireless networks. Subsequent studies should focus on examining the efficiency of the existing educational programs that are currently implemented to address the issues of network security threats and of improving the proper behavior. Research could be conducted on these initiatives according to their ability to modify the behavior of users in a positive way, namely regarding the encryption types used and the SSID names chosen. Furthermore, studies could be made to give more understanding of how laws can be used to regulate compliance with network security policies. For example, research can evaluate the efficiency of rules to apply WPA2 or WPA3 encryption on all new routers and access points, or recommendations not to use specific SSIDs. Such comparison helps the researchers to determine the best practices in increasing network security on the macro level based on education and legislation ([Buttyán and Hubaux, 2009](#)).

Future studies should also explore the findings of this study in more detail, focusing on the areas as we defined them; Encryption upgrades: SSID naming Channel selection optimization, and periodic security checks.

6.1 Upgrade Encryption

Identified in this study, most networks in London remain with either use WEP or open that are easily subject to attacks. Further studies should be conducted on how to persuade users to use more secure encryption mechanisms, for instance, WPA2 and WPA3. It could also matter to determine the operations that could be of most benefit in facilitating this change (Moissinac et al., 2021). For example, studies may investigate the effects of pop-ups or banners by ISPs or hardware makers asking users about outdated security standards and explaining how to update them. Moreover, research may quantify the effectiveness of such upgrades in relationship to network security, by studying the decrease in a number of successful cyber-attacks, and an upgrade in data security.

6.2 Change SSID Naming Conventions

Specifically, this paper has established that the use of identifiable SSIDs enhances the risk of security by increasing the vulnerability of the networks to actuate attacks. Future research should focus on the effect of different SSID names on the security of the networks. For instance, research could be conducted where the results would weigh the level of security on the network that is associated with generic SSID and that other network with identifiable or descriptive SSIDs (Ghering, 2016). Researchers could also use questionnaires to find out more about the specific users and the extent to which, they are willing to come up with safer SSID practices and how they make these decisions. This study might be useful in creating a protocol that would set recommendations as well as awareness programs to persuade users to avoid the use of easily discernible SSIDs and subsequently lower their vulnerability to cyber-attacks.

6.3 Optimize Channel Selection

This study pointed out channel congestion as a real problem, especially for the multitudes of networks that exist in areas of high population density where they use the same default channels. Future research should be directed towards the concept validation of Dynamic CSC and identification of the procedures for dynamically selecting and managing the radio channel. It could encompass the development of programs or other mechanisms that can independently decide on the alternatives of channels that are least used at any end time based on analyses carried out on actual interference on the network (Buttyán and Hubaux, 2009).

Also, more studies could be pursued as to how these tools could optimize the network and its security in a high wireless traffic environment. Research could also go further in attempting to locate these tools within the present network management systems to enhance their usability among the network managers.

6.4 Regular Audits

These can be defined as systematic inspections of the security status in network systems in order to have the Networks safe and efficient. In future studies, there is much to discover about the idea of developing and implementing the best practice of the audit wherever it is in its development

stage from concept to tangible tools and frameworks. For instance, research could focus on when and how often such audits are required in order to properly address security risks for dissimilar forms of a network (Moissinac et al., 2021).

Further, it is also possible to investigate the outcomes of systematic audits for network security and performance in the context of decreasing the rate of successful attacks and enhancing data protection. When the best practices in audits are discovered it will be easier for the network administrators to escalate the security standards, while practicing efficient practices.

Besides such particular fields of study, further research should embrace the general impact on wireless network security at the societal level. With today and the future world becoming one big computer system where all aspects right from personal calls to business deals and even execution of some critical activities being carried out through wireless networks, it can be seen how crucial it has become to secure these networks (Vanhoef and Piessens, 2017). Research should hence be carried out to discover topmost important features including novel techniques of strengthening the security of wireless networks now and in the future.

Overall, this study has offered important findings on the security threats of wireless networks in London, United Kingdom; however, it has also pointed out forthcoming research that might be required to comprehensively look at these problems. It is suggested that for future research, more work should be done based on the limitations of this study, the influence of technological advancements on wireless networks, characterizations of users, performance of educational activities, and legal bills on the developments of enhanced and secured wireless networks (Farahat et al., 2018).

Moreover, by directing their efforts to certain aspects of WLAN, for instance, encryption improvements, naming scheme for SSID, channel selection, as well as periodic reviews, scholars can assist in designing real-world measures that will make the networks safer and shield the users from the ever-evolving threats.

7. Conclusion:

This paper is regarding research concentration on the threat and vulnerability in the open data source of wireless networks with emphasis on Wi-Fi networks in London United Kingdom. This work involves the analysis of data that is gathered from WiGLE. detail exposed a number of networks that signaled that an urban environment could have several privacy and security threats (Borisov et al., 2001). This eliminated the skepticism I had at the beginning and proved the fact that detailed Wireless Network information is very much available on WiGLE. info such as SSIDs, BSSIDs, encryption types, GPS coordinates, and timestamps can all be captured in an IEEE 802.11. The gathered data offers a rather detailed insight into the state of the wireless networks available in London city; however, it also questions the users' privacy and security. The amount of the analyzed networks using poor or old encryption, for example, WEP or no encryption at all, was worryingly high (Ghering, 2016). This has placed these networks at a high risk of being penetrated and susceptible to data breaches by attackers since the latter can easily capitalize on the weaknesses of these protocols. Examining the results yielded by the analysis, the researchers observed a plethora of SSIDs that included potentially sensitive information such as names, businesses, or locations. This exposure makes it possible to monitor and fingerprint people and companies based on their Wi-Fi utilization and this could lead to invasion of privacy.

As seen from the networking mapping and visualization of data from the networks, there is some dependency between the network configuration and the security measures put in place. The networks that dominated commercial areas had been found to use much stronger encryption protocols than those used in residential areas. This probably calls for awareness creation and possibly the formulation of policies that would enhance security on all types of networks (Mehboob et al., 2016). The study reaffirmed that attackers may leverage the data from public Wi-Fi to execute different network attacks like the DoS attacks, MitM attacks, as well as Evil Twin attacks. The increased availability of such network information facilitates the work of the attackers in that they can easily spot vulnerable networks to attack. Based on the analysis of the research, it is revealed that settings such as London can be at risk owing to the high density of wireless networks. This concentration of networks offers the attacker a large variation to choose from and enhances the possibility of hitting a major target (Zhang et al., 2003).

Also, the study showed that some networks have SSIDs that bear family or company names, or “The Ivy Mayfair Public” or “The Ivy Mayfair Private.” Such easy-to-detect SSID tags endanger the identity or location of the network owner, often leading to cyberattacks. When the SSIDs are easily recognizable, it becomes easier for physically threatening individuals to target the network or for replacers to launch well-planned cyber-attacks. These findings tally with the literature review concerning the perils of utilizing identified names SSIDs and extend the prior research work concerning the application of more generalized and less specific SSIDs to boost security measures.

Congestion of channels was another main concern found in the study, where most networks take default channels including channel 6. This accumulation of networks to a particular channel result in interference; the interference affects the quality of the network and makes the network vulnerable to attacks such as the denial of service (DoS). The results conform to the prior studies made related to the channel congestion effects and further raise the requirement for channel management. Maximum utilization of the channels and the use of channels with less traffic can improve the nodes’ performance and security.

The significance of these findings is great for the significance of wireless network security. They emphasize that such issues as ineffective encryption and insecure networks remain actual and stress that the main problem is the lack of understanding of the population of modern requirements for secure networks among many operators. Also highlighted is the role of non-identifiable SSIDs in minimizing security threats resulting in the proposal of public awareness and best practice guidelines that could help publish non-identifiable SSIDs (Zhang et al., 2003). In addition to the choice of channels the problem of channel congestion is brought up and some guidelines on how to counteract it are given, including the usage of such dynamic systems of channel selection to avoid interference and achieve better performance.

The following is a guideline for future studies: Thereafter, it should consider ways through which the users of WEP or unsecured networks can be persuaded to shift to the use of WPA2 or WPA3. This research could assess several awareness campaigns and interventions geared toward increasing the shift toward modern encryption standards (Vanhoef et al., 2016). Second, outcomes

of particular naming protocols investigated in relation to security and user behavior should concern the creation of secure SSID practices guidelines and should also investigate how effective these guidelines are in preventing identified targeted attacks. Third, future research needs to focus on the dynamic channel selection and channel control decision where researchers should extend their work by proposing and testing channel optimization tools (Butty'An and Hubaux, 2009). Last of all, there should be further research on how to properly and frequently conduct security audits as well as their influence on the stability and security of the network; here the emphasis should be on the regular and broad audit frameworks and instruments.

All in all, the findings of this dissertation hold a plethora of data that can be used to understand the level of security threat in wireless networks in London. The study agreed that these are considerable threats; they include the use of older encryption, such as WEP, the use of obsolete SSIDs, and congestion of channels (Vanhoeft et al., 2016). These findings conform with previous studies and stress the further need for enhancing security measures and the general public's security literacy. With regards to these issues and with reference to recommended areas for future study, the stakeholders can improve the security of the wireless networks as well as safeguard against emerging threats.

8. References

1. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends [WWW Document], 2016. . IEEE Journals & Magazine | IEEE Xplore. URL <https://ieeexplore.ieee.org/abstract/document/7467419>
2. Adewuyi, N.A., Oladele, N.A.A., Enyiorji, N.P.U., Ajayi, N.O.O., Tsambatare, N.T.E., Oloke, N.K., Abijo, N.I., 2024. The convergence of cybersecurity, Internet of Things (IoT), and data analytics: Safeguarding smart ecosystems. *World Journal of Advanced Research and Reviews* 23, 379–394. <https://doi.org/10.30574/wjarr.2024.23.1.1993>
3. Agarkar, P.T., Chawan, M.D., Karule, P.T., Hajare, P.R., 2020. A Comprehensive Survey on Routing Schemes and Challenges in Wireless Sensor Networks (WSN). *International*

Journal of Computer Networks and Applications 7, 193.

<https://doi.org/10.22247/ijcna/2020/205320>

4. Alblwi, S., n.d. A Survey on Wireless Security Protocol WPA2 - ProQuest [WWW Document]. URL
<https://search.proquest.com/openview/51c0ac6dabb1cdd2dbeda43c194f0a56/1?pq-origsite=gscholar&cbl=1976342>
5. Architectural Wireless Networks Solutions and Security Issues, 2021. , Lecture notes in networks and systems. <https://doi.org/10.1007/978-981-16-0386-0>
6. Biswas, R.N., Mitra, S.K., Naskar, M.K., 2019. Preserving Security of Mobile Anchors Against Physical Layer Attacks, in: Advances in Information Security, Privacy, and Ethics Book Series. pp. 211–243. <https://doi.org/10.4018/978-1-5225-5742-5.ch008>
7. Boutet, A., Cunche, M., 2021. Privacy protection for Wi-Fi location positioning systems. Journal of Information Security and Applications 58, 102635.
<https://doi.org/10.1016/j.jisa.2020.102635>
8. Butty'An, L., Hubaux, J.-P., 2009. Security and Cooperation in Wireless Networks Additional Problems.
9. Cisco Annual Internet Report (2022). <https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html>.
10. Cyber Security Issues and Challenges for Smart Cities: A survey [WWW Document], 2019. . IEEE Conference Publication | IEEE Xplore. URL
https://ieeexplore.ieee.org/abstract/document/9024768?casa_token=NiIEJKIujAAAAA A:UhEwlv74gmYE1j6rxOfc_3RPEBYJ3D04lzbUBGwt7Hqs3b3LM6FLhYcIggTZT8vnyYIQX6wisso
11. DDoS in the IoT: Mirai and Other Botnets [WWW Document], 2017. . IEEE Journals & Magazine | IEEE Xplore. URL
https://ieeexplore.ieee.org/abstract/document/7971869?casa_token=iJyXReY9lGQAAA AA:- Oqga2hZH12QPbPk8LIaXweKHLlcn2dM5B8ykc7RCpVXs76SuE4CZoz7UGMmOJ7 iTbv9a5nFew

12. Farahat, I.S., Tolba, A.S., Elhoseny, M., Eladrosy, W., 2018. Data Security and Challenges in Smart Cities, in: Lecture Notes in Intelligent Transportation and Infrastructure. pp. 117–142. https://doi.org/10.1007/978-3-030-01560-2_6
13. Ghering, M., 2016. Evil Twin vulnerabilities in Wi-Fi networks [WWW Document]. Radboud University. URL http://cs.ru.nl/bachelors-theses/2016/Matthias_Ghering_4395727_Evil_Twin_Vulnerabilities_in_Wi-Fi_Networks.pdf
14. Hacking Exposed Wireless | Guide books, n.d. . Guide Books. <https://doi.org/10.5555/2825917>
15. Jamalipour, A., Bi, Y., 2018. Introduction to Wireless Powered Communication Network, in: Springer eBooks. pp. 1–23. https://doi.org/10.1007/978-3-319-98174-1_1
16. Kifayat, K., Merabti, M., Shi, Q., Llewellyn-Jones, D., 2010. Security in Wireless Sensor Networks, in: Springer eBooks. pp. 513–552. https://doi.org/10.1007/978-3-642-04117-4_26
17. Lockwood, J., Mooney, A., 2017. Computational Thinking in Education: Where does it Fit? A systematic literary review [WWW Document]. arXiv.org. URL <https://arxiv.org/abs/1703.07659>
18. Mallaboyev, N.M., Qosimov, M., Chimberdiyev, S., 2022. INFORMATION SECURITY ISSUES, International Congress on Multidisciplinary Studies in Education and Applied Sciences.
19. Matte, C., 2017. Wi-Fi tracking : Fingerprinting attacks and counter-measures [WWW Document]. URL <https://theses.hal.science/tel-01921596>
20. Mehboob, U., Qadir, J., Ali, S., Vasilakos, A., 2016. Genetic algorithms in wireless networking: techniques, applications, and issues. Soft Computing 20, 2467–2501. <https://doi.org/10.1007/s00500-016-2070-9>
21. Moissinac, K., Ramos, D., Rendon, G., Elleithy, A., 2021. Wireless Encryption and WPA2 Weaknesses. <https://doi.org/10.1109/ccwc51732.2021.9376023>
22. Sen, J., 2013. A Survey on Security and Privacy Protocols for Cognitive Wireless Sensor Networks [WWW Document]. arXiv.org. URL <https://arxiv.org/abs/1308.0682>

23. Toh, C.K., 2020. Security for smart cities. IET Smart Cities 2, 95–104.
<https://doi.org/10.1049/iet-smc.2020.0001>
24. Valchanov, H., Edikyan, J., Aleksieva, V., 2019a. A Study of Wi-Fi Security in City Environment. IOP Conference Series Materials Science and Engineering 618, 012031.
<https://doi.org/10.1088/1757-899x/618/1/012031>
25. Valchanov, H., Edikyan, J., Aleksieva, V., 2019b. A Study of Wi-Fi Security in City Environment. IOP Conference Series Materials Science and Engineering 618, 012031.
<https://doi.org/10.1088/1757-899x/618/1/012031>
26. Vanhoef, M., Matte, C., Cunche, M., Cardoso, L.S., Piessens, F., 2016. Why MAC Address Randomization is not Enough. <https://doi.org/10.1145/2897845.2897883>
27. Vanhoef, M., Piessens, F., 2017. Key Reinstallation Attacks.
<https://doi.org/10.1145/3133956.3134027>
28. Zhang, K., Shen, X., 2015. Security and Privacy for Mobile Healthcare Networks, Wireless networks. <https://doi.org/10.1007/978-3-319-24717-5>
29. Zhang, W., Das, S.K., Liu, Y., 2016. Security in Wireless Sensor Networks: A Survey, in: Auerbach Publications eBooks. pp. 253–288. <https://doi.org/10.1201/b13609-19>
30. Zhang, Y., Lee, W., Huang, Y.-A., 2003. No Title. Wireless Networks 9, 545–556.
<https://doi.org/10.1023/a:1024600519144>