Hindawi
Mobile Information Systems
Volume 2023, Article ID 9863675, 1 page
https://doi.org/10.1155/2023/9863675

Retraction

Retracted: Assessment and Test-Case Study of Wi-Fi Security through the Wardriving Technique

Mobile Information Systems

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] V. O. Etta, A. Sari, A. L. Imoize, P. K. Shukla, and M. Alhassan, "Assessment and Test-Case Study of Wi-Fi Security through the Wardriving Technique," *Mobile Information Systems*, vol. 2022, Article ID 7936236, 21 pages, 2022.

Hindawi
Mobile Information Systems
Volume 2022, Article ID 7936236, 21 pages
https://doi.org/10.1155/2022/7936236

Research Article

Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique

Victor Ojong Etta,[1] **Arif Sari**,[1] **Agbotiname Lucky Imoize**,[2,3] **Piyush Kumar Shukla**,[4] **and Musah Alhassan**[5]

[1]*Department of Management Information Systems, Girne American University, Karmi, Northern Cyprus, Turkey*
[2]*Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka 100213, Lagos, Nigeria*
[3]*Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, Bochum 44801, Germany*
[4]*Department of Computer Science & Engineering, UIT, RGPV, Bhopal 462033, MP, India*
[5]*Electrical Engineering Department, University of Development Studies, School of Engineering, Nyankpala Campus, Tamale, Ghana*

Correspondence should be addressed to Musah Alhassan; musahalhassan@uds.edu.gh

Received 16 May 2022; Accepted 17 June 2022; Published 30 June 2022

Academic Editor: Amit Gupta

This study aims to investigate Wireless Local Area Network (WLAN) within the context of its applicability as a 21st-century business tool and its survivability in a security threat-infested cyber landscape. WLAN security leverages the Wardriving technique deployed within geolocation to scan for WLAN density and explore the associated security mechanisms. Specifically, the study adopts two approaches; the first part reviews relevant research articles in electronic libraries and databases on WLAN security based on wardriving techniques. The other part comprises a measurement campaign conducted in a mid-sized city in North Cyprus. The field measurement aims to underscore the claims from the literature to find out how the security encryption technologies are used. In particular, the goal is to determine the availability of WLAN infrastructure and monitor how the security measures are implemented in Northern Cyprus. The main objective is to determine the security state of WLAN in Cyprus and examine how it can be generalized for related environments. In order to completely grasp the research issue posed in this study, data analyses from several perspectives are analyzed and examined critically. The wardriving approach has been used in this work to crawl wider regions for examination. This study was conducted with security findings drawn only from publicly accessible information emitted by each investigated wireless access point. The channel usage, Service Set IDentifier (SSID) security, the Encryption type (Open, WEP, WPA, WPA2, WPA3, and Mixed mode), WPS usage statistics, geographical locations, detailed security statistics described in Wigle CSV format, and vendor statistics are highlighted. Generally, results indicate that 21,345 WLANs were detected. From the detected WLANs, 23 (0.1 percent) used WEP encryption, 18 (0.08 percent) used WPA-TKIP encryption, 5,359 (25.1 percent) were unencrypted, and a clear majority of 9,139 (42.82 percent) used the more secure WPA2 encryption, while 13 networks (0.06 percent) used the latest WPA3 encryption technique. The results imply that WLAN security in Cyprus can be said to be moderate. Thus, this study adds to the expanding corpus of research on WLAN security and Wardriving to all parties in the wireless security ecosystem. The current study examines WLAN operations in North Cyprus while pointing to future research directions on Wireless LAN security mechanisms. Overall, the dataset from the wardriving experiment is novel and would serve future research exploration in the wireless security systems domain.

1. Introduction

Wireless LANs have recently been widely used in commercial organizations, airlines, hospitals, schools, and residences. However, considerable WLAN is used in Small Offices and Homes (SOHO). Wireless Local Area Networks, or Wi-Fi, are the primary Internet connection for individuals and organizations. The 1997 release of IEEE 802.11 WLAN standards contributed to the increase in popularity of WLAN to become the ubiquitous connectivity solution for many users globally [1]. Its low latency, high transmission speed, low cost, and high stability are critical to its popularity. WLAN will reach more than $3.47 trillion in 2023 [2]. The present spike in WLAN-enabled smart homes and Internet of Things (IoT) devices is expected to increase WLAN equipment to 17 billion by 2030, as 5 billion devices were anticipated in 2019 [3]. Mobility, scalability, flexibility, cost-effectiveness, simplicity of deployment, and other considerations contribute to WLAN spread. However, one of its major drawbacks is that from inception, security was not a consideration in its design, and owing to its broadcast nature, it is susceptible to security attacks. So, despite WLAN's popularity, its technology makes it unsafe because WLANs transmit radio signals for clients to receive. Unauthorized users sometimes position stations to listen for covert criminal activities. Whether at home or the workplace, understanding wireless connectivity and the risks and vulnerabilities involved with its use are crucial concerns for end users. Although some Wi-Fi security mechanisms established to protect wireless LAN had been in line with IEEE 802.11 standard, these security mechanisms were intended to secure WLAN through authentication and encryption [1]. They include WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2, and WPA 3. Some factors that influence the security of Wi-Fi wireless networks include standards, conventions, and good practices [4]. In general, WLANs are vulnerable to both passive to active attacks.

A comparative analysis of the wide application of wireless network communication and the inherent security implication does not seem to deter the high acceptability rate and adoption of wireless network communication by individual users, small businesses, and the enterprise group. In small businesses, WLANs boost productivity and enhance information sharing. The ease of access to documents is untethered. Employees can move around and always have access to the tools they need to conduct their duties. Wireless network communication benefits include increased mobility, collaboration, responsiveness, information access, network growth, and guest access. They now exist in Smartphones, Tablets/Pads, Palmtops, Smart televisions, wireless routers etc., which are used as intermediate and endpoints in wireless networks. Wireless LAN can be said to be the main hub of business communication in everyday life. The growing popularity of the Internet of Things (IoT) in smart homes and cities is built around Wireless LAN or the other [5].

There is a concentration of WLAN adoption in urban and/or business districts relative to the rural area. A simple survey shows that the urban human population, small businesses, and Corporations are found in urban districts, which explains the dense nature of WLAN technology [6]. Another factor contributing to the popular use of Wi-Fi networks is its portability and mobility, low cost, and ease of deployment. Wi-Fi technologies are said to be insecure, and this stems from the broadcast nature and low-security considerations on intermediate and endpoint devices [7]. For this, techniques such as Wardriving or Access Point mapping were developed to study the security mechanisms to demonstrate privacy vulnerabilities while educating the growing population of users on which security mechanisms to adopt to mitigate attacks.

1.1. Wardriving. The term Wardriving describes the technique used for searching and mapping WLAN signals within a particular location or district. Wardriving is generally defined as moving around (not necessarily in an automobile) a designated geographical area and scanning to enumerate wireless access points and their operational state in real time. The statistics reveal the security posture of these types of networks [8]. Wardriving is often a passive experiment that targets publicly available information from each wireless access point [9]. It typically requires a laptop or an Android device (smart phone or Tablet). A USB-powered WNIC and a GPS receiver make the laptop a more effective tool because of its higher processing power. It is now possible to deploy freely available open-source and Wigle software and Android hardware devices to perform wardriving.

1.2. Legality of Wardriving. Wardriving is not hacking, illegal or damaging activity to assessed wireless network devices or their owners, despite its name seeming illegality. According to Wargames (1983), the term "Wardialing" was developed when a computer was used to call a series of numbers to locate other computers having networking capacity [10]. Depending on the equipment and the objective of the survey, wireless network scanning can be active or passive. The active scanning approach requires the wireless scanning device to connect with the devices that are being scanned. This can be accomplished by transmitting and collecting probe request frames from adjacent WLAN devices. It is like wardialing, where the devices are plotted based on the responses.

Wardriving is sometimes misunderstood as a form of hacking due to its deceptive name. Contrarily, Wardriving is a widely accepted tool used by professionals and amateurs in information security. Wardriving can become criminal if used to violate a wireless network's security. This may involve scanning susceptible WLAN networks to acquire unauthorized access. Because of misunderstandings and possible misuse of Wardriving, it is critical to understand the legal and regulatory limits. There appears to be a great deal of ambiguity in determining what constitutes authorized and unauthorized access for the Open WLAN networks [11, 12]. Unauthorized Wi-Fi access (or piggybacking) raises fresh and contentious legal challenges. Regulating open WLAN access is currently uneven and confusing in many areas. This

leaves roaming Wi-Fi users unsure of their legal standing while connecting to an unknown open network [13].

1.3. Common Security Threats to WLAN. Confidentiality, Integrity, and Availability (CIA triangle) are the most important assets in computer networks and resources. The CIA triad is a concept that serves as the foundation for establishing an organization's security systems and policies. When the CIA criteria are satisfied, an organization's security profile becomes stronger and better suited to address the threat occurrences. The CIA triad offers a detailed high-level checklist for assessing security processes and equipment. An effective system meets all three components, whereas an information security system that lacks any of the three characteristics of the CIA triangle is inadequate and vulnerable to threats and assaults. A threat is a prospective security breach that has the potential to take advantage of a system or asset vulnerability. Whether passive or active, an attack is an intentional unauthorized action against a system or its asset.

Wireless local area networks (LANs) are prone to security breaches. In 2018, a data security breach affected two-thirds of small and medium-sized businesses (SMBs). The average attack cost on these companies was over $3 million, owing to protracted system failures (40 percent of servers were down for more than 8 hours), which increased the average cost to over $3 million. [14] Wireless network attacks may occur from misconfigurations or incomplete configurations. These include Denial of Service, Resources hijack, Backdoor intrusion; the passive gathering of sensitive data through eavesdropping within range of an access point, Rogue (or Unauthorized/Ad Hoc) Access Points: that deceive devices into connecting; attacks by impersonating legitimate access points to convince authorized users to sign-on, hacking Lost or Stolen Wireless Devices: getting past the password, freeloading: stealing a connection or stealing files. Figure 1 summarises wireless network attacks and threats that network administrators and users contend with maintaining safe network infrastructures.

1.4. Motivation. The significance of wireless network security assessment stems from the necessity to address the issues, ascertain the key sources of security flaws, and devise methods to mitigate them.

The primary motivation:

(i) To better understand the ubiquitous and pervasive nature and the exponential growth of WLAN devices, intensified by the advancements in wireless technology, declining cost and simplicity in deployment.

(ii) Despite extensive research on WLAN security challenges spanning about 20 years, there are still a plethora of security challenges in Wi-Fi networks.

(iii) There is a need to understudy the vulnerabilities and cyber-attacks associated with WLAN and how to mitigate them or minimize their impact.

(iv) The fast growth of IoT enabling technologies has exacerbated the dependency on WLAN as an underlying hub; thus, security concerns are becoming increasingly significant and capturing public attention.

(v) A wide range of Wi-Fi-based Internet of Things applications are available, from smart homes to smart cities, but security problems exist.

(vi) WLAN security has remained elusive, necessitating on-the-move (OTM) WLAN scanning to successfully infer the condition of WLAN in any given location.

(vii) Despite the widespread availability of wireless connectivity, most wireless users are either unaware or unable to deal with wireless security issues. Consequently, we now have the most serious security vulnerability to hit computers in decades.

The significance of wireless network security evaluation stems from the necessity to address the issue to ascertain the key sources of security flaws and devise methods of mitigating them. Therefore, pursuing research in WLAN based on wardriving techniques will enhance the knowledge of the underlying security mechanisms and users' behaviour towards a resilient WLAN and open a new gateway for future research endeavours.

1.5. Contribution. The main contributions of the paper are outlined as follows.

(i) We carried out extensive reviews of research articles on WLAN security based on wardriving techniques by searching relevant literature in electronic libraries and databases.

(ii) We conducted a measurement campaign in a mid-sized city in North Cyprus to underscore the claims from literature, intending to find out how security encryption technologies are used.

(iii) We determined the availability of WLAN infrastructure and monitored how security measures were implemented in Cyprus.

(iv) We investigate a Wireless Local Area Network (WLAN) within the context of its applicability as a 21st-century business tool and its survivability in a security threat-infested cyber landscape.

(v) We examined WLAN operations in North Cyprus while pointing to future research directions on Wireless LAN security mechanisms.

1.6. Paper Organization. The structure of this work is as follows. The first Section gives the background information on wireless local area network, its growth and ubiquity, security issues and encryption protocols, common security threats, wardriving, the legality of Wardriving, and the research motivation. Section 2 summarises related literature. In Section 3, we cover the research methodology. Similarly, in Section 4, we address notes on the selected studies. In

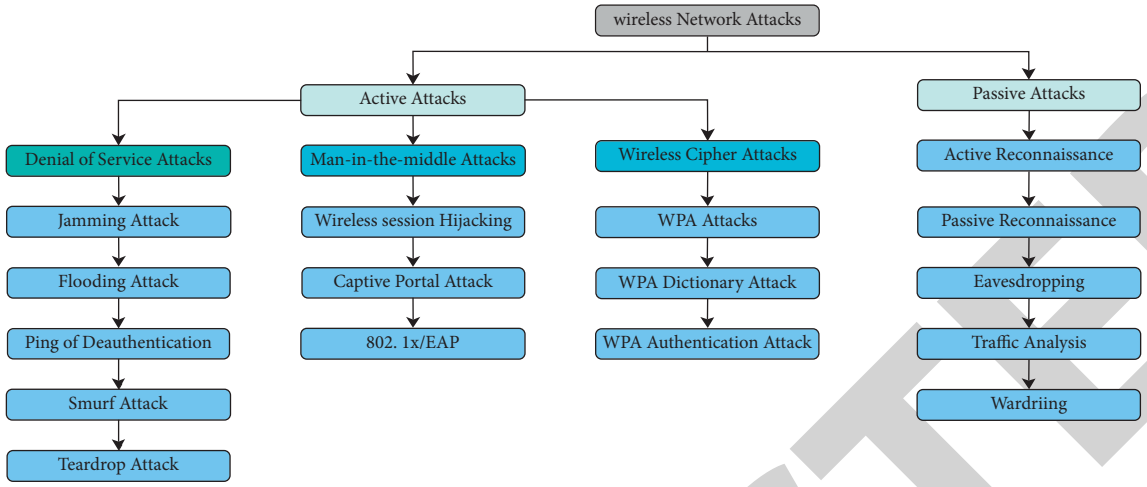

Figure 1: Common WLAN threats and attacks.

Section 5, we perform a test case scenario of the wardriving technique in Girne, a mid-size city in Cyprus, to underscore the rich literature on the subject, and present the limitations of the survey and survey results. Finally, Section 6 concludes the survey.

2. Related Work

Several research works have been carried out in Wireless network communication in general and wireless network security in particular. The next section of this review addresses the articles based on the title of this paper. It is hoped that at the end of the review, concrete recommendations on wireless security infrastructure in different scenarios attract appropriate security approaches for wireless infrastructure while pointing to future research directions in Wireless LAN security. Wardriving, a term coined by Shipley (2000) after an 18-month study of WLAN, was presented at the DefCon conference of 2001 [15]. He referred to wardriving as "driving around and looking for wireless networks" [16]. Webb [17], Yek [18] and Lin, Sathu, and Joyce [19] conducted surveys of WLAN networks in Australia and New Zealand in 2003. According to these early surveys, regular consumers were not yet aware of the benefits of encryption. They found that only 40% of studied WLAN networks use encryption. However, with the growth in density of WLAN, the proportion of encrypted networks fell, according to Webb and Yek. Because WLAN technology was new to the consumer market in the early 2000s, users may have been unfamiliar with it. WLAN standard was only finalized in 1997 by IEEE 802.11, while Apple was the first manufacturer to deliver built-in WLAN networking for laptop computers in 1999 [20]. Hence user experience was at its prime.

The authors of the work reported in [21] used data from 2003, 2007, and 2010 to investigate the progress of WLAN availability and security in Auckland, New Zealand. The findings from the study indicate a 406 percent increase in total WLAN adoption from 2003 to 2010. Additionally, the authors demonstrate a 48 percent rise in the adoption of encryption protocols since 2003, to 88 percent of all observed networks in 2010. In 2015, the authors of the work [22] surveyed WLAN users in the Auckland neighbourhood. The authors reported a 1600 percent rise in overall WLAN deployment, observing an increase from 236 to 4077 unique networks. According to the data presented by the authors, encryption protocol utilization grew to 100% in 2015, compared to 40% in 2003. The data revealed that 71% of the investigated networks applied the WPA2 encryption technique.

In New Zealand, a comparable increase in WLAN security and density was reported by [23, 24]. According to Nisbet's results, the evolution of Wi-Fi security in four distinct sites around New Zealand using survey data from 2004 to 2011 depicted that WLAN deployment rose by 2600 percent in one investigated location. WLAN deployment surged by more than 700 percent in another assessed location during the same period. In 2013, encryption protocol adoption varied significantly amongst the investigated areas, ranging from 77 percent to over 97 percent. Related studies reported by [25, 26] are highlighted in this paper.

Recent Wi-Fi network survey research in Europe has focused on the Balkans. The work reported in [27] evaluated the prevalence and security of WLANs in Budapest and Belgrade. Approximately 90% of examined networks use some version of WPA encryption in both locations, leaving less than 10% of networks unprotected and less than 2% using WEP encryption. The works [28, 29] provide similar findings. Leca's research gathered data from over 100,000 wireless networks located throughout Romania. 86 percent of the 100,000 networks were encrypted with WPA2, 5% with WPA-TKIP, and 3% with WEP, leaving the other 6% unprotected. Over 11,000 WLAN networks in the Bulgarian city of Varna were investigated by Valchanov et al., who observed encryption usage rates almost identical to those reported by Leca.

In the work of Valchanov et al. [9], the authors researched wireless security in Varna city, Bulgaria, through a wardriving method using Raspberry Pi. The results were compared with previous research conducted in 2008. The analysis of the Wi-Fi security posture of Varna showed that

there had been a significant improvement from previous research. They recommended that only WPA2 or higher security protocols be used. Where there is a need for older devices, separate and limited networks can be used to support WPA/WPA2 mixed mode, and WPS settings should be disabled from all access points. For future work, they suggested more research on 802.11ac and 802.11ah networks in the greater Varna area [9].

A review by Sebbar et al. [25] performed a Wi-Fi network measurement campaign in Rabat, Morocco, through Wardriving. They covered about 10,000 WLANs comprising both for private and business use. They reported that 77% of the networks used WPA or WPA2 security protocols and balanced the use of nonoverlapping channels (1, 6, and 11) to avoid interference. They concluded that WLAN security in Morocco is comparable to what exists in the developed countries. They, however, noted that the results of their research might not be generalized to other cities for reasons such as socio-economic and educational differences in Morocco [25].

The wardriving technique was useful in mapping Wi-Fi networks with given landscapes and gathering data on devices used for criminal activities such as terrorism. In passive mode, information from digital devices can be easily collected. [26] opined that such gathered data can be used by law enforcement agents to track the criminals. In the evaluation of Wi-Fi security in one of Malaysia's major cities, conducted by [27], where passive data traffic of private homes, coffee shops, and companies were collected and analyzed using KAli Linux operating system tools to create awareness of the lapses in their wireless network environment; the result of the evaluation shows the lack of security awareness among people thus exposing them to threats such as Spoofing, Tampering, Repudiation, Information disclosure Denial of Service, and Elevation of privileges (STRIDE). The experiment results show that no fewer than 9 out of 1,282 access points were found to disable broadcasting their Service Set IDs (SSID) or names of the access points. The study also found that 19.73% (253 AP) do not use encryption. In other words, they are open access points. The result also shows that 16.77% (215 AP) implemented WEP encryption protocol while 63.7% (814 AP) implemented WPA/WPA2 encryption [27]. They recommended enforcing strict regulations on public places that use wireless access points and embarked on a campaign advert on YouTube to create awareness of the implication of operating an unsecured wireless network.

In the work of [28], the author focused on the ease of compromising Wireless networks as a result of unprotected devices revealed high positives. He maintains that finding open wireless networks was commonplace in Eger. However, his research shows that vulnerability in wireless networks is attributive to those user groups that are less familiar with the use of the Internet. Another susceptible user group is the *Z* generation (anyone born from 1997 onward). Generation *Z* has been dubbed "digital natives" who share Internet access on the open network [28]. The researcher concluded that the users are ignorant of possible threats through some IT devices. He further recommended that strong passwords be used as an additional layer of defence mechanism from attacks when sharing Internet or data traffic.

The study of [29], argues that a false sense of security by Access point administrators is responsible for the neglect of adopting the needed encryption protocols for the security of Wi-Fi networks. The researchers suggest implementing a simple program to determine the security state of the Wi-Fi network and its conformity with the current Wi-Fi security best practices. In conclusion, the authors admit that the poor Wi-Fi security is a growing concern for private and business use needing urgent attention. They urge relevant authorities to mandate effective Wi-Fi security measures and compliance.

A study by [30] in selected cities in Lebanon aimed at raising awareness of the inherent threats and their impact on WLANs using the wardriving techniques. The main contributions of the study were raising awareness of flaws and vulnerabilities of existing Wi-Fi networks, the severity of Wi-Fi network attacks, and steps on how to improve Wi-Fi security procedures [30]. The authors observed that people are unaware of the Wi-Fi attacks and threats they are susceptible to from the study. They recommended that there is a need to conduct security awareness campaigns through conferences and workshops to educate users on the different Wi-Fi attacks, their severity, the threats they portend, and measures to alleviate attacks. In the same vein, the work [31] maintains that developing educational programs that inform the average consumer of inherent threats and the methods for securing wireless networks is a necessary tool to be explored.

The submission of [32] proposing wardriving as a system that can assist in collecting Statistical data of WLANs and their security status in a mapped geographical area suggests that the application can be used to study security trends and threats, misuse, and exploitation of Wi-Fi infrastructure. Although Wardriving is often regarded as a controversial practice, they added that it has helped raise awareness of the significance of WLAN security. It can be argued that some key objectives of their study were to increase the efficiency of Wardriving and awareness of WLAN network security, as well as to create a technique of quickly capturing and storing statistical and location information of WLAN networks within predetermined zones.

In dealing with the problem of "digital inclusion in the Ecuadorian Amazon," which was exacerbated by the pandemic, wireless access point mapping (WAP) or Wardriving was employed to map and analyze data correlating it with geoinformation to observe its potential and limitations as a method for indirect data collection [33]. They argued that Wireless access points correlate weakly but positively with nightlight, young population, accessibility to economic centres, and negatively with slope [33]. The researcher concluded that Wardriving offers interesting opportunities for mapping social data and an indirect data collection method. They submitted that Wardriving offers new opportunities to explore the vast variability of existing sensors and supply data needs for different scientific disciplines.

The objective of the work in [34] is to provide a technique for collecting, analyzing, and storing WLAN survey

data that is efficient, scalable, and easily accessible. This was accomplished using wardriving with publicly available open-source software and commercially available hardware. Despite its threatening nickname, they asserted that Wardriving is neither unlawful, malicious, nor detrimental to the surveyed wireless network devices or their owners. They suggested that future studies will improve the accuracy of surveyed results by investigating newer Wireless Interface Cards (WNICs) and various antenna types. Additionally, the method for data analysis must be enhanced as, over time, the amount of WLAN data increments. They stated that future work should focus on improving data storage, sampling techniques, and increasing sample size covering a larger WLAN networking landscape for a more extensive investigation.

The work reported in [35] posits that only a little research exists on statistical issues with wardriving data, despite several published works in the literature using this approach. The authors sampled publicly collected wardriving data and compared it with a predictive model for Wi-Fi access points to buttress this point. The outcome shows several statistical issues which future wardriving researchers must account for, which include "selection bias," "sample representativeness," and the "modifiable areal unit problem." Their methods include opportunistic Wardriving, using the Wigle app on an Android Google Pixel 4 to develop a self-collected geolocated Wi-Fi AP dataset as a predictive model for Wi-Fi density using national statistics and comparative evaluation of the different quantitative datasets on Wi-Fi Apps. By taking account of these factors, we hope that future wardriving exercises will be able to provide more rigorous and robust statistical assessments of Wi-Fi APs. The work of [36] deals with WLAN security technologies and their potential for integrity, availability, and confidentiality. It provides a thorough analysis of most WLAN packet data services and technologies.

The research purpose of [37] is to design a method for surveying wireless local area networks, assess the present state of WLAN security, and ascertain the extent to which the outdated encryption technologies are still utilized in Finland. The method of WLAN surveying should be efficient, scalable, and easily replicable. Additionally, it should ascertain the current condition of WLAN security in Finland through observation of WLAN security practices. By using the wardriving technique, a passive wireless network scanning was used to gather information about nearby wireless networks by listening for messages broadcast by wireless network devices. The author concluded that scanning WLANs using the wardriving technique accomplished the research's objective. However, he emphasized the importance of refining the wardriving process in a future study by enhancing surveying software, hardware, and methods and scaling up the research to broader locations. Additionally, the author recommends using a separate WLAN adapter for the 2.4 and 5 GHz bands and equipping the adapters with more powerful antennae.

An analysis of Wi-Fi network security based on publicly available datasets was performed through an experimental survey covering several networks across four countries on three continents [38]. The study revealed the consistent use of outdated, vulnerable security settings, the adoption of modern protocols, the increased presence of mesh networks as part of smart city infrastructure, and the frequency spectrum. It also provided a clearer view of Wi-Fi network security in the real world. As a contribution to the research community, tools used for mining security statistics and all anonymized datasets were made available to would-be researchers in the domain.

Wi-Fi network security status of occupants in coffee houses in Libya is the work of [39]. The objective of the study was to evaluate security vulnerabilities in the use of WLAN by the population. Data was acquired through wardriving techniques from different populated locales. The analyzed data provided insights on wireless security awareness among the public. Their result showed that the security status in the public WLAN needs improvement, hence the need to implement sophisticated passwords and configure the encryption to WPA2.

The legal and security framework of Wardriving is the focus of [40]. It has been argued that wardriving is a form of hacking as opposed to an ethical approach to enhance WLAN security. These authors suggest that a technical and legal policy framework for Wardriving be formulated to guide scientists, managers, technologists, and the government. To substantiate the call, the researchers developed a preliminary and novel Mobile Enterprise Security and Legal (MESL) Framework. The study reported in [41] performed through field evaluation of WLANs showed that a high percentage of WLANs are not secured in Jordan. The researcher proposed changing WLAN default settings and well-crafted password Service Set Identifier (SSID) masking as some measures aimed at improving the security of the wireless network by the users.

Another susceptibility in WLAN is observed in its deployment in the Internet of things [42]. The study shows that WLAN technologies for the Internet of Things (IoT), such as IEEE 802.11ah, are vulnerable to major security risks due to their limited computational and memory capabilities, thus limiting the implementation of durable intrusion defence and security protocols. They opined that security administrators must conduct regular and extensive vulnerability evaluations of IoT devices to address this issue.

Wireless networks have grown in popularity as a means of Internet connection in Bangladesh. There is, however, a dearth of statistics on the inherent vulnerability and harm that underlie the use of WLAN. Hossain et al. [43] describe a pilot study in a university context in which they examined the current scenario regarding its vulnerability to malicious attacks. They demonstrated that a substantial number of wireless access points can be exploited and that users can be exploited with evil twin attacks using custom-built portable wireless penetration testing equipment. They maintained that the routers configured in their default state are easy targets for attack; and that the users' lack of awareness drives them to visit vulnerable websites. As a result, public awareness can help mitigate network threats. The users in the examined areas mostly use social media sites over public Wi-Fi and may fall prey to social engineering if unaware.

Based on the study, individuals with technical competence are more concerned with the safety.

This study conducted by the authors in [44] assesses the security of wireless networks in Nuku'alofa's CBD with considerable results. They maintained that Wireless networks had grown rapidly since their inception, maintaining that wireless equipment's security protocols have achieved a robust level. However, security is still an issue, and this study seeks to address security concerns with these questions: How has wireless network growth and security fared? And how can there be an improvement in wireless network security in Tonga. The Nuku'alofa wardrive results clearly showed the number of commercial and home networks. The study is designed using an exploratory research approach. The data revealed a considerable increase in WLAN usage when the fibre optic network was implemented. However, this study concludes that Nuku'alofa WLAN security is still evolving.

The high points of WLANs include speed, range, usefulness, and ease of use, and security is a big concern [45]. The work in [46] in their research aims to highlight the security and privacy concerns of Internet users in Malaysia by exposing the vulnerabilities of Kampung Wi-Fi networks, wardriving with open-source software. The work in [47] addresses the primary risks to WLAN security and some of the various solutions for blocking or limiting illegal access. They submit that WLAN's security strategy must consider the number of possible clients, the value of the data, the likelihood of attacks, and the cost of protective measures as a holistic approach to the WLAN security. The evaluation of WLAN density within a geographical location is a critical step in developing realistic models for the deployment structure of a security framework to mitigate attacks [48]. Such densities are often obtained by large-scale wardriving-like measuring campaigns using off-the-shelf devices as a security approach to WLAN.

The work of [49] examined a database of over 5 million wireless access points obtained by Skyhook Wireless through Wardriving. The result of the analyzed data shows that default naming was a common practice. They also discovered that AP data could provide fertile ground for understanding the intended use of Wi-Fi access points when combined with the location information. It was also observed that analysis and mining of this massive and expanding repository of AP data have the potential to deliver significant technical, social, economic, and security benefits. Additionally, the work demonstrates how geographic information may be used to better understand the overall wireless infrastructure by examining network features such as access point density, demographic biases, and signal propagation behaviour [49].

Data acquired by wardriving in Leeds, UK, revealed a statistically significant influence on Wi-Fi security by ISPs and substantial disparities between several distinct Internet Service Providers (ISPs). Although WEP is a cryptographically flawed encryption mechanism, some networks were discovered to be using it, and identifiable ISPs gave these routers. They are in a position to maintain track of out-of-date routers. The researchers feel that this emphasizes the need for router upgrades and have several recommendations for ISPs, router manufacturers, and end users. The duty-of-care issue was raised: ISPs are held liable for their customers' Wi-Fi security when they provide routers with wireless access points. ISPs frequently advertise that they provide secure networks, and home users are unlikely to reconfigure their routers [50].

The work presented in [51] focuses on mechanisms for cost-effectively collecting data from several devices for developing social, economic, and security architectures. At a relatively low cost, data collected by opportunistic Wardriving can provide current Wi-Fi deployment data in communities around the Philippines. Much information on APs may be acquired, including encryption, providers, kinds, and even density. The data collected may be used to guide a variety of decisions on Internet accessibility and other related helpful initiatives.

Constant access to the Internet is now a daily routine. The covid19 scare exacerbated the use of WLAN for the Internet in virtually all aspects of human endeavours, especially in education, governance, entertainment, etc. Despite these, security concerns are not emphasized with deserving urgency and seriousness. A degraded and obsolete WEP protocol is still in use. The work in [52] focused their study on the WEP protocol in a sector of the city of Bogota, Columbia. The authors observed that using cheap WLAN devices from Oriental companies dominates the IT market. These low-cost devices operate under low-security standards. The authors submitted that there was a need for improved security culture in WLANs.

The studies of [53] reveal that many residences are installing wireless access points without considering their security. It is expected that more digital crime cases will be launched as a result of this. It also looks into forensic technologies monitoring war drivers. Open and unauthorized APs may be set up as honeypots. A wireless honeypot can disclose important information regarding infrastructure assaults, such as attack frequency, attacker's skill, plan, and methodology [54]. Researchers have adopted several techniques to arrive at research goals in dealing with WLAN security, as stipulated in Table 1.

3. Research Method

Our comprehensive evaluation of the literature was prompted by [73]. A systematic literature evaluation was conducted to thoroughly and concretely address the specified concerns. A thorough analysis was conducted based on collected research, and the most pertinent studies addressing the specified issues were reported. The entire purpose of this review is to assemble the most relevant materials from primary sources. These publications were analyzed and assessed to obtain the most accurate findings. The primary goal of a systematic review is to design an unbiased technique [74]. We made the same efforts to eliminate any element of bias to achieve objectivity. As seen in Figure 2, our review design comprises a sequence of phases. The sequential processes in the review methodology are as follows: establishing research questions, developing a strategy for search, documenting the strategy, establishing criteria for inclusion and exclusion, criteria for quality assessment, and

Table 1: Related work categorization by techniques.

Year	Ref. no.	Research method/ technique	Domain	Description
2021	[55]	Security model	Wireless network	Analyses a new physical layer security strategy to improve wireless communication security against eavesdroppers
2020	[56]	Security model	Wi-fi network security	Proposes a model for small and medium-sized businesses by identifying and analyzing security measures in businesses
2018	[57]	Empirical analysis	Wireless network	Employs empirical data to map wi-fi hotspots in metropolitan areas to operationalize the virtual component of urban vibrancy
2019	[58]	Survey	Wi-fi security	Describes the fundamentals of wi-fi security problems to raise awareness
2014	[59]	Experimental procedure	Network security	Uses a correlation coefficient-based learning method to find problems in WLAN
2014	[60]	Review	Wi-fi security	Considers the remote security threats to current wireless systems and standards, including WEP, WPA, and WPA 2. (WPA2).
2021	[4]	Review	Wi-fi security	Enables visualizing the numerous factors required in wi-fi wireless network security
2018	[51]	Wardriving	Wi-fi	Assists in comprehending a low-cost technique for acquiring information about wi-fi distribution in a variety of locations
2021	[61]	Wardriving	Wi-fi security	Proposes a standalone python-based programme for assessing the vulnerability of wardriving-captured access points (APs)
2021	[62]	Penetration testing	Wi-fi security	Presents a kAli linux-based wi-fi penetration testing technique
2021	[63]	Wardriving	Wi-fi security	Analyses the results of evaluating the security of a wireless network on raspberry pi running kAli linux
2021	[36]	Survey	Wi-fi security	Examines the possibilities for integrity, availability, and confidentiality and also analyses most WLAN packet services and technologies, revealing safety
2020	[64]	War-flying	Cyber security	Designs a system for using a drone to capture and map unauthorized 2.4 GHz and 5 GHz wireless network access points in mission-critical infrastructure, then converting the data to a map view
2019	[65]	Survey	Network security	Highlights the prospective risk and forms of network security attacks, as well as shedding light on existing preventative approaches and making realistic ideas for their enhancement
2019	[66]	Wardriving	Wi-fi security	Provides a method for identifying rouge access points based on a set of static properties chosen from a well-conducted experiment on real-world locations
2018	[67]	Multi-parameter framework	WLAN security	Improves rouge access point detection in WLAN by using a multi-parameter-based approach
2021	[68]	War flying	WLAN security	Evaluate wireless networks drone system (warflying) that detects and analyses information such as access point locations, MAC, authentication, power, privacy, and encryption settings
2020	[69]	Survey	Wi-fi network security	Examines wireless technologies and the security vulnerabilities that these technologies offer to larger communication networks
2017	[70]	Survey	Wi-fi security	Focuses on developing solutions for mitigating cyber-attacks and examines the hazards associated with utilizing wireless devices to offer Internet service in open access zones
2021	[71]	Review	Wireless network security	Explores the worldwide implications of growing wireless network technologies and cyber security concerns and suggests some recommended remedies
2021	[72]	Wi-fi protocol model	Wi-fi security	Provides a model for detecting wi-fi protocol attacks with low false positives and varied low rates of false negatives for various attacks
2021	[61]	Analysis tool	Wireless access point security	A python language-based tool is proposed and implemented as a standalone tool for assessing an access Point's vulnerability

quantitative meta-data analysis. The stages are explained in further detail in the next section.

This effort aims to find, assess, and synthesize significant academic material on WLAN security utilizing Wardriving methodologies. Despite the topic's real-world relevance, there is a shortage of academic research, particularly on a widely agreed-upon, comprehensive definition of wardriving WLANs to determine their security posture. This problem makes it difficult for academics and organizations to locate pertinent literature, impeding study and innovation in this sector. We intend to offer a guided tour of the available literature and build a shared ground truth. We also adhere to Tranfield et al.'s [75]. The three-stage approach is based on well-established criteria [76, 77]. Their review methodology details the research topics, sources of information, search criteria, and pertinent keywords. Following the initial collection of articles, we use established criteria for inclusion and exclusion to trim down publications in terms of quantity and improve the quality of the literature chosen for future assessment.

3.1. Research Questions. The literature evaluation aims to develop questions that potentially include security and offer

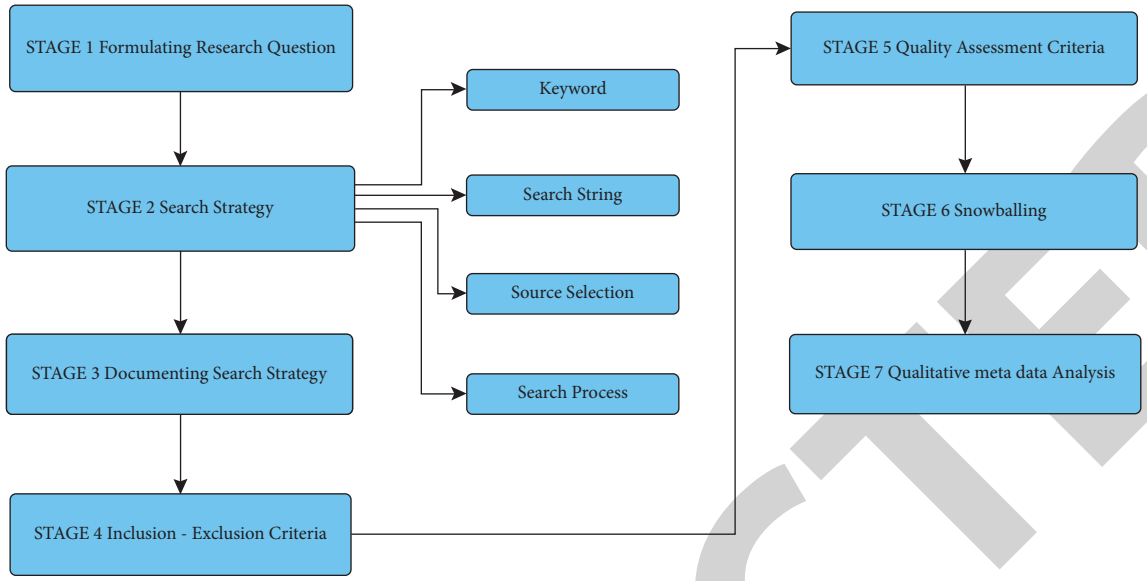

Figure 2: Systematic literature review model.

Table 2: Research questions.

Research questions	Motivation
(1). What are the security challenges associated with wireless local area network (WLAN)?	The focus is on how to gain deep insight into the security challenges and concerns of WLAN
(2). How is the wardriving method considered a technique for evaluating WLAN security?	This question aims to provide the security posture of WLAN of a location using wardriving techniques
(3). How do the present security measures and mechanisms improve security in WLAN infrastructures?	A comparative analysis of WLAN security mechanisms and their impact
(4). What are other measures deployed to enhance WLAN security?	The main focus is to outline other security measures to enhance WLAN security

tangible solutions to those concerns. The study's research topics sparked discussions on possible privacy and security safeguards for WLAN analysis employing Wardriving. Four research questions were created, and our collected studies were used to address them in this research study. Table 2 provides a detailed explanation of the questions posed in this study.

3.2. Search Strategy. We focused on appropriately organizing our search technique using identification, screening, and the Prisma protocol approach [78]. The first stage in the protocol was to use keywords to create a search string. To find articles, keywords alone are insufficient; they must be concatenated in various ways to generate a string containing the names of many journals and digital libraries [79]. The work in [80] was the source of our search approach. The search technique consisted of four steps: keyword identification, search string, source selection, and search execution.

3.3. Defining Keywords. In order to obtain the most relevant results from articles, keywords were specified for a particular query [81]. Table 3 provides a list of all the different terms that have been used for searching. The primary topic's search string was created by combining the keywords from each inquiry. Additionally, formulated questions were searched using keywords to get information about the subject.

3.4. Search String Strategy. A search string was built using precise query terms. This was confirmed by computer security and wireless networking specialists. The search query was tested on many search engines and adjusted until it yielded the most relevant results. The model presented by [82] was adopted to create search strings.

(a) Major words derived from subject and research questions

(b) Identifying alternate spellings or synonyms for main nouns

(c) Identifying relevant keywords

(d) By using the Boolean operator OR to find the synonyms or other spellings

(e) The relationship between main phrases and the Boolean AND operator

Consequent to the above method, the following search strings were generated.

("Security Protection" OR "Safety") AND ("Wi-Fi Network" OR "WLAN") AND ("Wardriving" OR "OTM

Table 3: Research Questions associated with keywords.

Research question	Keywords
RQ1. What security issues exist in wireless local area network (WLAN)?	"Security challenges" OR "security problems" AND "wireless local area network" OR "WLAN" OR "wi-fi"
RQ2. How is the wardriving method considered a technique for evaluating WLAN security?	"Wireless local area network" OR "WLAN" OR "wi-fi" AND "security mechanisms" OR" security protocols" OR "security measures" AND "wardriving" OR "warwalking"
RQ3. How do the present security measures and mechanisms improve security in WLAN infrastructures? What are the shortcomings of wardriving?	"Security procedures" OR" security techniques" OR "security model" AND "wireless local area network" OR "WLAN" OR "wi-fi" AND "wardriving" OR "warwalking" AND "shortcomings" OR "limitations"
RQ4. What are other measures deployed to enhance WLAN security, such as hard and soft wares?	"Hardware" AND "softwares" AND "wardriving" OR "warwalking" AND "wireless local area network" OR "WLAN" OR "wi-fi"

Table 4: Data sources.

Data Source	Website address
Scopus	Scopus-advanced search | signed in
IEEE	IEEE xplore: advanced search
Hindawi	Search | hindawi
Web of science	Advanced search-web of science core collection

Table 5: Inclusion and exclusion details.

Name of journal	Inclusion	Exclusion	Total
Hindawi	1,483	6,296	7,779
Scopus	32	1,147	1179
IEEE	103	46,613	46,716
Web of science	9	23,179	23,188s

Scanning") AND ("Assessment" OR "Evaluation" OR "Analysis").

A systematic pilot search was performed to provide the best possible results and to fine-tune the search technique. Our search phrase is divided into two sections: the first Section discusses WLAN security, while the second Section discusses the Wardriving technique.

3.5. Sources Selection. In order to gather data, the following libraries and databases were utilized. Many areas of our topic are covered in these libraries, making them the most useful. These libraries' search engines are better ideal for automated searches since they are user-friendly and powerful [83]. Table 4 contains a list of these databases and libraries.

3.6. Search Process. Our search took place from December 2021 to January 2022. Primary studies were found using automated and manual searches. According to [82], automatic research is superior to manual research. However, a manual search was conducted to ensure the search string was correct. The search string was used on all databases specified in Table 4. This search generated 7,779 results on Hindawi, 1,179 results from Scopus, 46,716 results from IEEE Xplore, and 23,188 results from the Web of Science.

3.7. Search Strategy Documentation. The documentation of our search approach was influenced by [84]. This phase involved the creation of a paper outlining our search approach in detail. The number of included and excluded papers was carefully documented, and the details are presented in Table 5. Additionally, data regarding the search method used to retrieve records based on the given search phrase were recorded, such as the search date, the name of the online library, and the number of items retrieved. This stage generates a report including all pertinent information regarding the search method. With the documentation provided, it is easier to evaluate a search and maintain tabs on the progress of that search.

3.8. The Criteria for Inclusion and Exclusion of Articles. Table 6 explains the specifics of the criteria for Eligibility and Non-Eligibility of articles. The articles included in the study were evaluated using the following inclusion and exclusion criteria. Duplicate papers were deleted in the first attempt, and articles were then evaluated against the stated keywords and study objectives. The articles that were dropped did not give thorough replies to the questions. Then, using inclusion-exclusion criteria, each paper was evaluated based on its title, abstract, and entire text. Studies were chosen for inclusion from peer-reviewed journals. When many versions of the same document exist, the most recent, complete, and an updated copy is chosen for inclusion, and the others are eliminated. Conflict analysis was used to eliminate bias at every level of the selection process.

3.9. Criteria for Quality Assessment. For every research, the quality evaluation criteria are critical. Following the study selection, we used quality evaluation in our research. The goal of this approach is to enhance the selection criteria. The quality assessment questions (QAs) checklist was developed. Each publication was verified against the checklist to pick the most related research, the majority of which would answer our RQs. The work presented in [85] served as the foundation for the quality evaluation approach. "Yes" was allotted to an article that met the quality assessment checklist and a "No" if it did not meet all of the quality evaluation criteria. Some research articles were discovered that only partially answered the QA questions. To that end, each research article was awarded a score or value based on how well it answered the quality assessment questions. For each question, the options are "Yes," "No," and "Partial," with

Table 6: The criteria for inclusion and exclusion of articles.

Included articles
Included were English-language research articles
Original articles were selected
Range of research papers in years from 2010 to 2022
Excluded articles
Non-English research articles are excluded
Articles that did not address or capture the research questions were excluded
Duplicate articles were not counted

scoring set at 1, 0, and 0.5, respectively. There are only three possible answers. Each manuscript was assessed against the QA questions, and a quality total was computed for each research paper at the conclusion. Table 7 contains a checklist of quality evaluation questions. The initial stage was to establish QA questions, and then a scale was created to award ranks to the papers based on the QA questions checklist. The aggregate value (AV) was calculated by adding all weights granted based on QA questions. An AV of at least 2.5 was required for an article to be accepted for publication, and the work was rejected if it was below 2.5. Figure 3 illustrates the process of quality evaluation.

3.10. Snowballing. Snowballing is crucial for research since it leads to additional investigation [82]. Both forms of snowballing, forward and backwards snowballing, were used in our study to get the most relevant results.

3.11. Analysis of Quantitative Meta-Data. Our evaluation is contingent upon the analysis of quantitative meta-data since it provides statistical data analysis from research papers. Additionally, literature on quantitative meta-analysis frequently advocates developing criteria for studying quality when making inclusion decisions [86]. In order to completely grasp our research issue, this study analyses data from several perspectives.

4. Research Questions on the Selected Studies

This Section answers the research questions in depth to achieve the goals of the research questions.

4.1. Rq1: What Are Security Challenges Associated with WLAN? WLANs use radio waves to transmit and receive data. WLANs are subject to illegal interception, eavesdropping, hacking, and various other cyber security threats because of the lack of a physical barrier.

The following are the three most prevalent WLAN security threats:

(1) Denial of service attack, in which an intruder floods the network with messages, causing network resources to become unavailable.

(2) Spoofing and session hijacking - when an attacker assumes the identity of a legitimate user to obtain access to network data and resources.

Table 7: Quality assessment questions.

Question ID	Quality assessment question
QA1	Are the research's goals and objectives properly stated?
QA2	Is the security of WLAN using wardriving stated?
QA3	Are any solutions provided for the formulated RQs
QA4	Does it answer to the security of WLAN in the light of wardriving?
QA5	Did the security techniques related to WLAN and wardriving contribute to this work?

(3) Eavesdropping is when data is intercepted while sent over a secure network by an unauthorized third party.

WLAN hardware employs a variety of security techniques, including:

(1) Service Set Identifiers (SSIDs) block devices from connecting to access points unless they use the right identification.

(2) Media Access Control (MAC) restricts access to access points by employing addresses assigned to each device.

(3) WEP-WPA Encryption – These ensure that only devices with the right key can interact with access points. These security standards differ in the level of protection based on the authentication mechanism and encryption techniques used [87].

Basic WLAN characteristics cannot ensure security even when all of these security measures are implemented. Furthermore, security features on WLAN devices are frequently turned off. If the default stage is not modified, no security is provided.

4.2. Rq2: How Is the Wardriving Method Considered a Technique for Evaluating WLAN Security? Wardriving is a passive wireless network scanning technique intended to acquire statistical data about wireless networks to help mobile computing and network security [35].

On the other hand, Wardriving is going about a given geographical region and scanning wireless network devices [88]. Today, Wardriving includes Bluetooth and ZigBee, widely used in IoT and smart devices. Warwalking, warbiking, and warflying with drones are examples of network scanning [8].

A survey system and process are the two components that constitute an effective wardriving exercise. The system is commonly built around open-source operating systems (Linux and Android). Others are open-source applications and commercially available hardware, while the survey is conducted using the passive scanning approach.

The network SSIDs, the Wireless Access Points (WAP), MAC, Manufacturers' names, Utilized channel, Encryption technique used, and the projected network location may all be derived from the gathered data. With this information, it

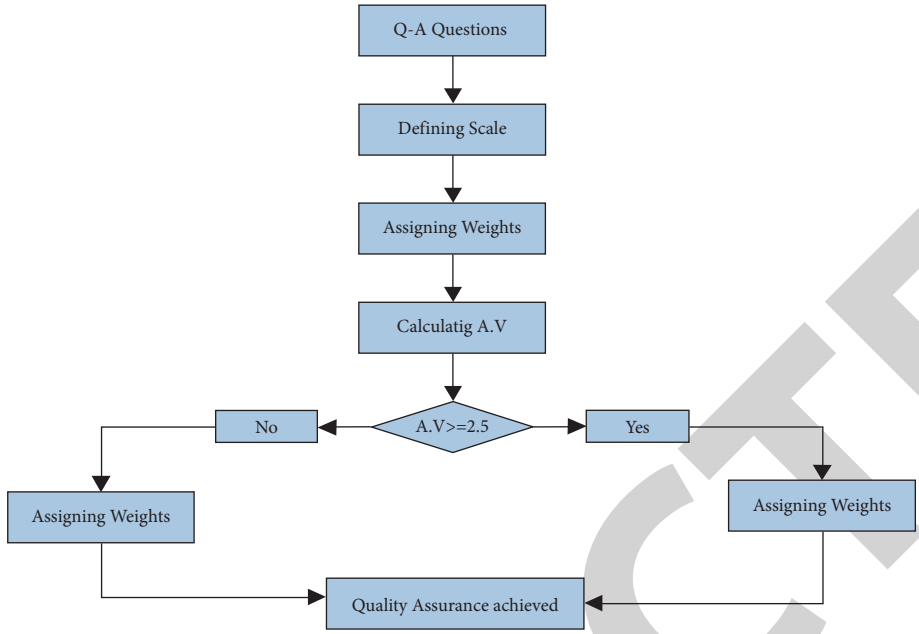

Figure 3: Flow chart of quality assessment.

is possible to establish the current condition of WLAN security in a region being studied.

4.3. Rq3: How Do the Present Security Measures and Mechanisms Improve Security in WLAN Infrastructures? What Are the Shortcomings of Wardriving?

(a) Default Passwords Modification: Preconfigured default administrator passwords are standard on most network equipment, including wireless access points. Because of their simplicity, these default passwords offer just a minimal level of protection. Changing the default password on a computer can make it more secure [89]. Passwords should be complex and changed frequently to protect WLAN data.

(b) Limited Access to Network Resources: Allow only authorized users to connect to a network. A media access control (MAC) address is assigned to each piece of network hardware. Unauthorized users may be restricted access to network resources [90]. The "guest" account, a common feature found on many wireless routers, is a restrictive option when activated. This feature allows visitors Wi-Fi access on a second wireless channel with a different password while keeping the primary credentials private.

(c) Data protection by encryption: By encrypting wireless data, anyone who has access to the network will be unable to access it. A variety of encryption techniques can provide this security. The Wi-Fi Protected Access (WPA), WPA2, and WPA3 protocols encrypt data sent between wireless routers and devices [91]. WPA3 is the most secure encryption available right now. Although WPA and WPA2 are still available, it is recommended that the equipment that supports WPA3 is used, as utilizing the previous protocols may expose the network to exploitation.

(d) Cloaking Service Set Identifier (SSID): Avoid making the SSID public to prevent unauthorized access to the network. Users may secure their device's SSID on all Wi-Fi routers, making it more difficult for attackers to locate a network [92]. Change SSID to something unique at the very least. When the SSID default option is enabled, a prospective attacker can determine the kind of router and exploit any known vulnerabilities.

4.4. Rq4: What Are Other Measures Deployed to Enhance WLAN Security, Such as Hard and Soft Wares? Other measures that enhance WLAN security include

(1) Setting up a firewall. Consider firewalls on wireless devices (a host-based firewall) and networks (a router- or modem-based firewall); an attacker who gets direct access to the wireless network may bypass the network firewall. On the other hand, a host-based firewall adds another layer of security to a computer's data [93].

(2) Virtual private network (VPN): VPNs can safeguard wireless networks. Most WAPs can pass VPN traffic. Normally, the wireless network is segregated from the rest of the network, and all access is via the VPN server. Ideally, a business should put Access Points with VPN servers on them. An access point with its VPN server can be isolated. This AP connects directly to the WLAN. Only clients using VPN software and the right credentials will be given access.

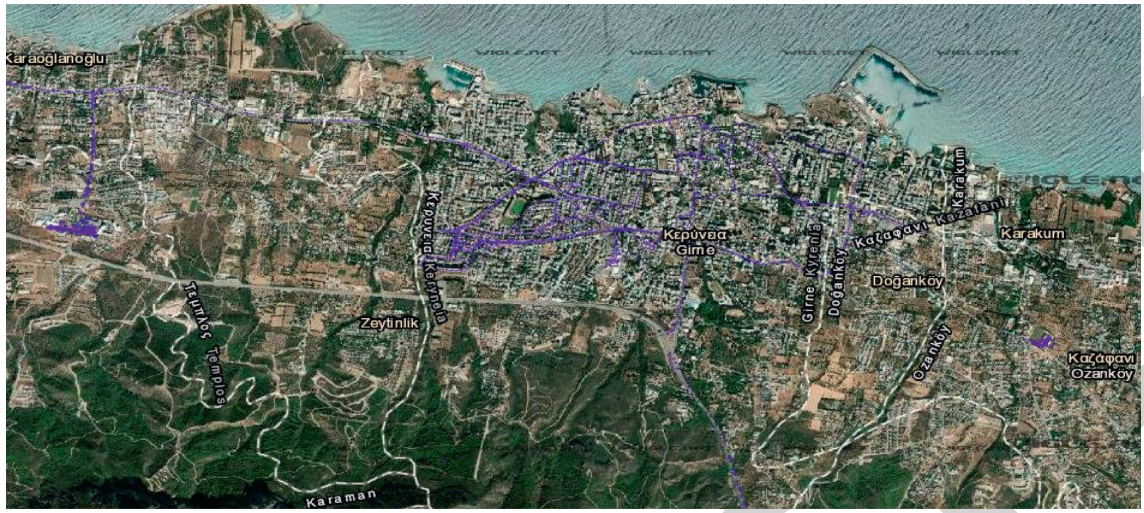

Figure 4: High-density Wi-Fi locations in Girne.

The WLAN connections cannot be sniffed since all traffic is encrypted [94].

(3) Maintaining up-to-date antivirus software and ensuring that Access points or Router firmware are updated are additional measures to protect WLAN [95].

(4) Network file sharing and device file sharing should be disabled. Never enable file sharing on public networks [96].

(5) The Wi-Fi Protected Setup (WPS) encryption simplifies the process of accessing the wireless network by requiring the user to input a PIN or use the Push Button Configuration (PBC), often referred to as Quick Secure Setup (QSS) [97]. Because of the inherent vulnerability of WPS-enabled access points, it is better to disable WPS in preference to WPA2 or the latest security mechanisms.

5. A Test Case Scenario of Wardriving Technique

5.1. Background. In order to underscore the effectiveness of wardriving as a technique for gauging the availability and security status of Wi-Fi networks at given geolocations, a measurement campaign was performed in November and December 2021 and January 2022. The experiment was conducted in designated locations in the mid-sized city of Girne (Kyrenia) in the north of Cyprus. Girne is located in the northern hemisphere at coordinates 35.3416667, 33.3166667. The selected places represent typical WLAN usage locations, namely, Academic, City centre and a major route across the city, as depicted in Figure 4. The analyzed result of the systematic measurement campaign provided an estimate of the density of WLAN and a general overview of its availability while also giving insight into the security mechanisms in use. The survey aims to determine how widespread the usage of antiquated and outdated encryption methods and newer encryption mechanisms are deployed in the area under review. Observing other WLAN security practices also enabled us to determine the present condition of WLAN security in Cyprus. The process is depicted in Figure 5.

5.2. Data Acquisition. The data gathering instrument was the Wireless Geolocation Engine (Wigle) Android application [98], developed for use on smart devices. A Samsung Model SM-N960F device with an internal WNIC and a GPS receiver was used for the survey. This work offers an opportunistic Wardriving approach, which maximizes using already available assets at the lowest potential cost. Wardriving sessions were performed in November, December 2021 and January 2022 around High-density Wi-Fi locations in Girne, as shown in Figure 5.

Before analyzing the findings of the WLAN survey, the obtained data must be processed. Depending on the survey tool, this can be done in numerous ways. For example, the WiGLE programme handles the sample automatically. Wigle outputs the.kml and the.csv file formats (**K**eyhole **M**ark-up **L**anguage and **C**omma **S**eparated **V**alue, respectively). The.kml files can be visualized in Google Earth or Map, as depicted in Figure 5, while the.csv file can be visualized in any spreadsheet application and Pandas data frame, as seen in the spreadsheet in Figure 6.

5.3. Survey Results. It is important to note that the views of [99–103] about various connectivity issues can affect the density and the overall evaluation of a wardriving result based on the variability of several issues highlighted in this paper. The wardriving approach is used in this work to crawl wider regions for examination [104–106]. A passive investigation was conducted, with security findings drawn only from publicly accessible information emitted by each wireless access point [107]. In order to produce statistical reports, data is processed and statistically analyzed. Channel usage, SSID security, the Encryption type (Open, WEP,

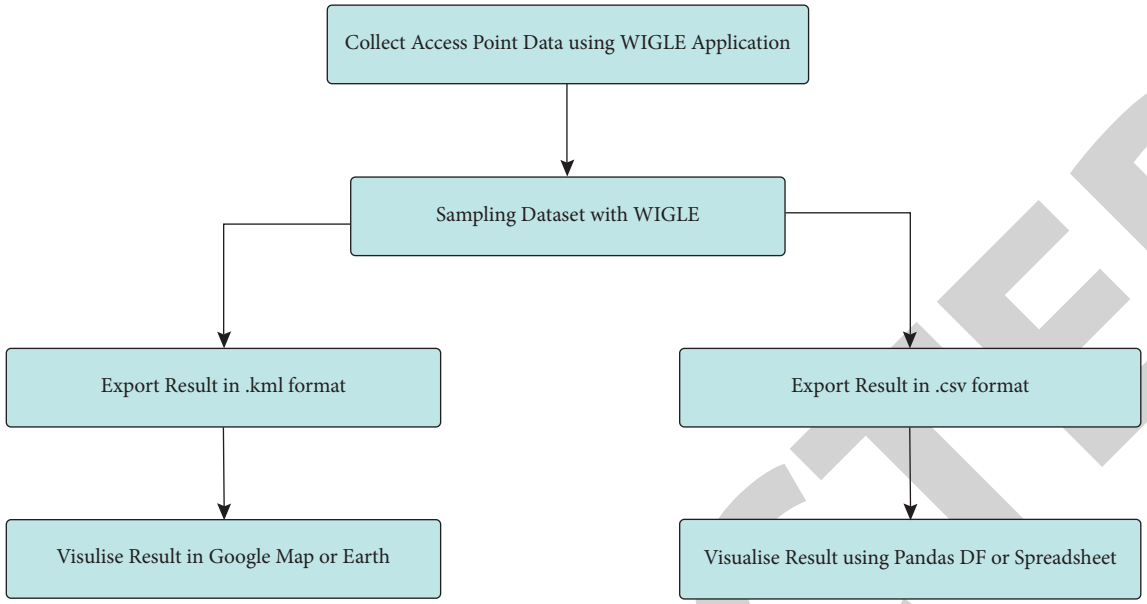

Figure 5: Wardriving process.

	MAC	SSID	LAT	LON	AUTH	DATES	Channel	RSSI	ALT	ACCUR	TYPE
1	a2:6c:ac:2c:2d:ef	GAUWIFI	35.33210517	33.27657948	[ESS][PARTIAL]	2021-11-05 14:1...	1	-74	79.4562	192	WIFI
2	d8:0f:99:15:d5:c8	LAPTOP-8C851...	35.33210517	33.27657948	[WPA2-PSK-CCM...	2021-11-05 14:1...	11	-74	79.4562	192	WIFI
3	50:d4:f7:47:03:f0	BIMAH	35.33210517	33.27657948	[WPA2-PSK-TKIP+...	2021-11-05 14:1...	6	-80	79.4562	192	WIFI
4	34:e8:94:44:dd:6a	KaderFatih	35.33210517	33.27657948	[WPA2-PSK-TKIP+...	2021-11-05 14:1...	11	-91	79.4562	192	WIFI
5	d6:ca:6d:06:28:7b	HIDDEN SSID	35.33197035	33.27668131	[ESS]	2021-11-05 14:1...	161	-86	45.4765	96	WIFI
6	d4:ca:6d:06:28:7b	AyComK39EYH...	35.33197035	33.27668131	[ESS]	2021-11-05 14:1...	161	-87	45.4765	96	WIFI
7	d4:ca:6d:e8:02:45	AyComK39EYH...	35.33197035	33.27668131	[ESS]	2021-11-05 14:1...	132	-87	45.4765	96	WIFI
8	d6:ca:6d:e8:02:45	HIDDEN SSID	35.33197035	33.27668131	[ESS]	2021-11-05 14:1...	132	-89	45.4765	96	WIFI
9	7a:0c:b8:a1:e6:22	LAPTOP-8C851...	35.33195388	33.27669848	[WPA2-PSK-CCM...	2021-11-05 14:1...	11	-56	46.6666	400	WIFI
10	a2:6c:ac:2c:2d:f7	ALJARAH	35.33195388	33.27669848	[WPA2-PSK-CCM...	2021-11-05 14:1...	11	-83	46.6666	400	WIFI
11	4e:5e:0c:31:9f:cd	GAUWIFI	35.33214693	33.27682595	[ESS]	2021-11-05 14:1...	36	-89	66.7206	32	WIFI
12	4c:5e:0c:31:9f:cd	HIDDEN SSID	35.33224929	33.27683628	[ESS]	2021-11-05 14:1...	56	-90	69.073	16	WIFI
13	9a:6e:cf:57:f2:e5	AyComK39EYH...	35.33224929	33.27683628	[ESS]	2021-11-05 14:2...	56	-87	70.2835	16	WIFI
14	fa:f9:07:5f:18:66	iPhone	35.33224929	33.27683628	[WPA2-PSK-CCM...	2021-11-05 14:2...	6	-54	71.1694	12	WIFI
15	98:da:c4:e0:50:e4	GAUWIFI	35.33224271	33.27689317	[ESS][PARTIAL]	2021-11-05 14:2...	1	-61	72.7644	16	WIFI
16	c8:3a:35:57:0d:48	iPhone	35.33234039	33.27694752	[WPA2-PSK-CCM...	2021-11-05 14:2...	6	-90	73.3688	16	WIFI
17	9c:9d:7e:6e:64:8b	iPhone	35.33234943	33.2769431	[WPA2-PSK-CCM...	2021-11-05 14:2...	6	-84	72.765	12	WIFI
18	64:09:ac:e4:77:af	AyComK39EYH...	35.33235503	33.27692364	[ESS]	2021-11-05 14:2...	132	-81	71.4166	16	WIFI
19	d6:ca:6d:ac:8e:a1	HI	35.33235503	33.27692364	[ESS]	2021-11-05 14:2...	132	-81	71.4166	16	WIFI
20	ac:84:c6:15:d6:46	AyComK39EYH...	35.33235503	33.27692364	[ESS]	2021-11-05 14:2...	161	-82	71.4166	16	WIFI
21341	c8:3a:35:2d:b3:d8	Tibet	35.33684667	33.31461584	[WPA-PSK-CC...	2021-11-11 12:1...	6	-81	76.4279	4	WIFI
21342	7a:28:f1:89:7d:20	OLD HOLBORN	35.33684667	33.31461584	[WPA2-PSK-CC...	2021-11-11 12:1...	6	-85	76.4279	4	WIFI
21343	e2:82:70:f9:e8:c3	GAZANATION	35.33684667	33.31461584	[WPA2-PSK-CC...	2021-11-11 12:1...	3	-86	76.4279	4	WIFI
21344	62:bc:4d:0d:56:b5	B?LSEV	35.33684667	33.31461584	[WPA2-PSK-CC...	2021-11-11 12:1...	11	-87	76.4279	4	WIFI
21345	a6:2a:a6:05:ca:52	Boray	35.33684667	33.31461584	[WPA2-PSK-CC...	2021-11-11 12:1...	11	-88	76.4279	4	WIFI

Figure 6: Sample of the captured dataset.

Table 8: Summary of encryption type.

Encryption type	Frequency	Percentage
OPEN ACCESS	5,359	25.1
WEP	23	0.1
WPA	18	0.08
WPA + WPA2	6,793	31.83
WPA2	9,139	42.82
WPA3	13	0.06
TOTAL	21,345	99.99

Table 9: Open and hidden SSIDs.

Hidden SSIDs	2,791	13.07%
Open SSIDs	18,554	86.93%

WPA, WPA2, WPA3, and Mixed-mode), WPS usage statistics, geographical locations, detailed security statistics described in Wigle CSV format, and vendor statistics are summarised in the study. In order to compile vendor statistics, the IEEE MAC address allocation lists are used [108].

About 21,345 WLAN networks were gathered with the related data. We can deduce the network SSIDs, manufacturers, MAC addresses, utilized channels, encryption protocols, and projected network location from the collected data. One may assess the area's WLAN security based on the obtained data. This may be done by analyzing the use of

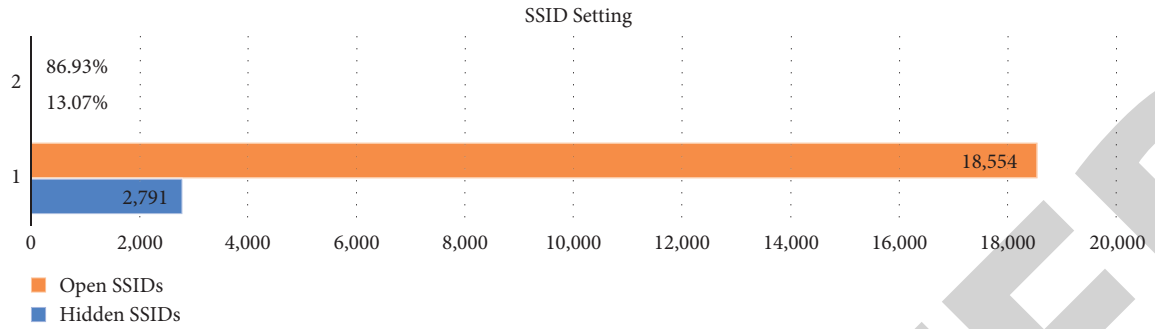

Figure 7: Ssid setting.

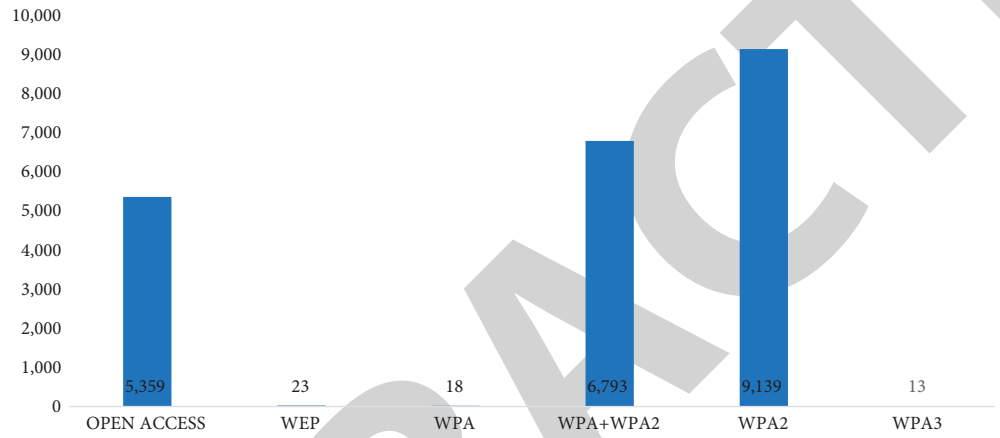

Figure 8: Distribution of encryption types.

encryption protocols and other security procedures like cloaking or changing the network SSID and WPS settings. Figure 6 is a sample of the captured WLAN dataset.

Table 8 provides a summary of the analyzed dataset. Guest networks provided by different companies, schools, and other organized establishments in investigated locations may account for some of the high numbers of open, unencrypted networks (5,359, 25.1%). Twenty-three networks used the deprecated WEP, and 18 still utilized the out-of-date WPA-TKIP encryption standard. WPA + WPA2 (mixed mode) accounted for 31.83% of the total networks. This may largely be attributed to legacy access point devices that need support.

Veiled SSID was only seen on 13.07% of the networks analyzed in this study, while Open SSIDs accounted for 86.93%. For this study, veiled networks are referred to as HIDDEN SSIDs, as shown in Table 9 and Figure 7.

On average, 2.36 percent of the surveyed networks had SSIDs that included the device manufacturer, model, or ISP name in digits and letters. The prominent manufacturer is TP-LINK. 73.11% of the studied wireless networks were found to be using the 2.4 GHz band, according to a study on wireless channel utilization. Most networks used the non-overlapping channels 1, 6, and 11 in the 2.4 GHz range. In the 5 GHz spectrum, most networks are set to use channels 36, 52, and 108. Further statistics show that WPS-enabled APs account for 10,329, while non-WPS-enabled APSs are 11,016 of 21,345 discovered access points, as shown in Table 8 and Figure 8, respectively. Therefore, 11,016 or 51.61% of Wi-Fi networks fall within WEP, WPA, WPA2, WPA3, and Open Access, which are non-WPS enabled. The overall security of the study area is poor, considering that part of the 51.61% still has the deprecated WEP and the fairly secured WPA networks.

Table 10: 2.4GHz nonoverlapping and other channels.

Channels	Count	Percentage
Channel 1	2,671	17.11
Channel 6	3,245	20.79
Channel 11	3,321	21.27
Other 2.4GHZ channels	6,470	40.82
Total	15,607	100

In terms of channel usage, the most discovered networks, 15,607 (73.11%), were found on the 2.4 GHz band, and over 59.17% of networks were set to operate on channels 1, 6, and 11. Table 10 shows the 2.4GHz channel used, and Figure 9 depicts the spread of the nonoverlapping channels in the 2.4GHz band.

The intermediate channels between the nonoverlapping channels in the 2.4GHz band (2, 3, 4, 5, 7, 8, 9, 10, 12, and 13) are not often used. However, when an Access Point is set at AUTO Channel, the device hops across channels using any channel with no interference.

The 5.0GHz had 5,738 (27.89%) networks, with channels 36, 52, 120, and 161 as dominant channels, as depicted in Table 11 and Figure 10.

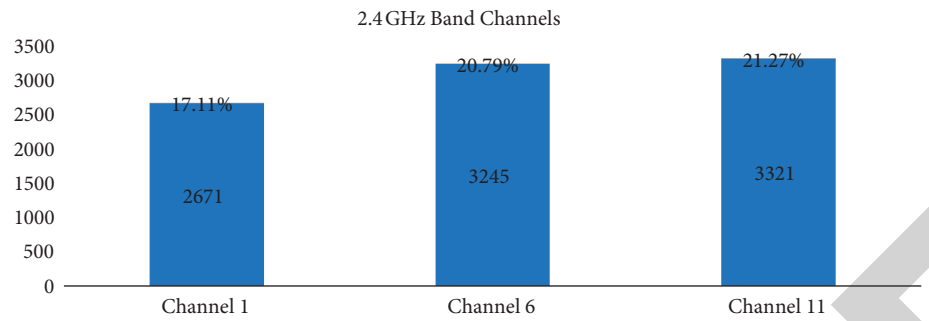

Figure 9: 2.4GHz nonoverlapping channels.

Table 11: 5 GHz prevalent channels.

Channels	Count
Channel 36	629
Channel 52	407
Channel 120	347
Channel 161	364
Other 5 GHz channels	3,991
Total	5,738

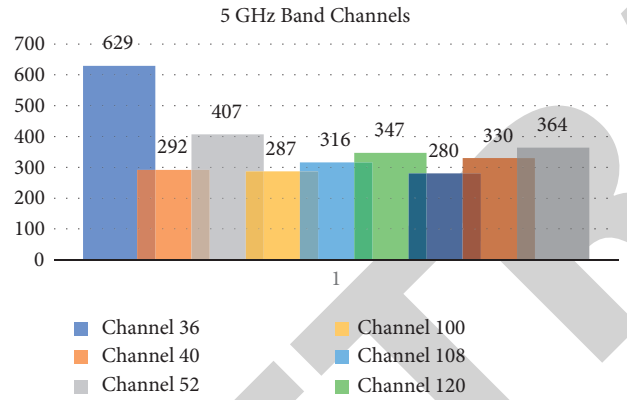

Figure 10: Dominant 5GHz channels.

Table 12: WPS result in the surveyed network.

Security setting	Count	%
WPS-enabled APs	10,329	48.39
Non-enabled WPS APs	11,016	51.61

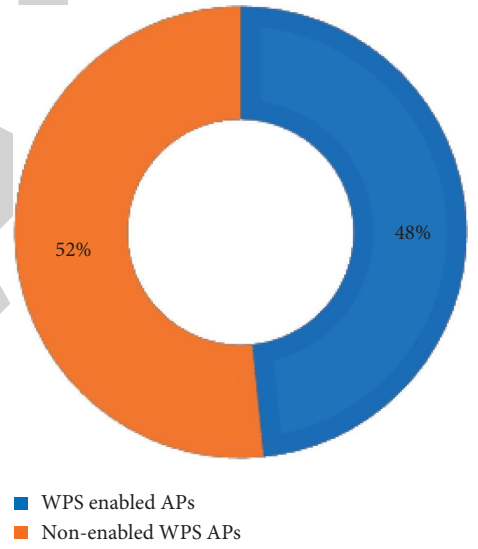

Figure 11: WPS settings in the surveyed network.

WPS is an insecure feature that increases the vulnerability of wireless networks to attack. WPS does nothing more than make it easier for clients to connect to Wi-Fi. It is risky for a function that provides such a minor advantage as the convenience of connecting to be enabled in a secured infrastructure. For secure WLAN, WPS are to be disabled [109].

With WPS-enabled networks constituting 48%, as shown in Table 12 and Figure 11, about half the number of WLANs in the study sample are vulnerable and susceptible to attacks.

5.4. Limitations of the Study. Some identified limitations of this survey are summarised as follows:

In the wardriving toolset, we used an Android smart device with an internal antenna for this study instead of a laptop with a high-power external antenna that would have provided wider coverage within the selected locations.

Wardriving with a car limits scanning only along motorable access paths. Future endeavours should consider war-droning or warflying as a more effective alternative, as a drone will cover wider areas, not limited to motorable roads.

In the wardriving measurement campaign, some captured Wi-Fi networks were not necessarily Home/Office networks; some were Mobile/Ad hoc networks. No known tool can distinguish between Stationary and Mobile/Ad hoc Access Points (MiFi devices). A faulty WLAN density assessment can arise due to two fundamental factors.

(i) The mobility of Ad hoc devices at each experiment will cause a change in a dataset, and the general inference of the statistical evaluation of the measured geolocation is altered.

(ii) On the other hand, Mobile/Ad hoc depends on mobile phone towers' cellular data to provide wireless Internet connectivity. Because of variable connectivity issues, mobile AP devices (MiFi) may be ON and OFF a wardriving radar, resulting in inconsistent results and datasets at each run.

The views expressed in the works [99–103] on various connectivity issues can affect the density and the overall evaluation of a wardriving result based on the variability of the above problems. However, current research endeavour using Artificial Intelligence (AI) and Machine Learning is addressing these issues [110–113]. Last, it is unclear how the proposed scheme would revolutionize some critical aspects of emerging wireless security systems. Therefore, it would be nice to explore how the projected framework would behave in blockchain-based information security systems [114], unified authentication and access control systems [115], radio frequency identification and password-enabled security access system [116], and localization for the jamming attack in wireless sensor networks [117].

6. Conclusions

The data extracted from WLAN surveys could be used to get insights on WLAN availability, security, and use. The data could subsequently be utilized to provide proposals and procedures to enhance WLAN networking security in a dynamic environment and forecast the future of WLAN security systems. Following the successful survey and data analysis, it can be deduced that the suggested Wardriving technique achieved the stated purpose. It can successfully collect and analyze WLAN security networks with minimal hardware and publicly accessible software. From the 21,345 networks detected, 23 (0.1 percent) used WEP encryption, 18 (0.08 percent) used WPA-TKIP encryption, 5,359 (25.1 percent) were unencrypted, and 9,139 (42.82 percent) used the more secured WPA2 encryption, 13 networks (0.06 percent) used the latest WPA3 encryption technique. From the projected data, it would be rational to infer that WLAN security in North Cyprus is moderate when the encryption mechanisms are considered as the main variable. It is worth mentioning that most unencrypted networks are Open Guest Networks (OGN) supplied by cafés, schools, governments, and other business enterprises. A close examination of the surveyed data reveals that owners of wireless network devices in the tested locations left their wireless networks' factory-set default settings unchanged. About 2.92% of the networks examined utilized recognizable factory-set SSIDs, whereas just 13.07% employed the masked SSIDs. In addition, 15,607 (73.11%) of the studied networks operated on the 2.4 GHz band. Interestingly, 9,237 (59.17%) of the networks operated on channels 1, 6, and 11. Other channels on the 2.4GHz band made up the remaining 6,370 or 40.9%. The 5.0GHz had 5,738 (27.89%) networks, with channels 36, 52, 161, and 120 as dominant. As a result, Wi-Fi access points should have their SSID, channel, and passwords customized from the factory defaults. When devices utilize the default network name (SSID), this may suggest that they also use the default password, which is well known to the suppliers and adversaries. This is a potential point of entry, and in the event that the device's model and manufacturer are revealed in the SSID and default password, an attacker would have all the information needed to initiate an assault on the wireless network. While wireless network scanners can circumvent the benefits of changing the network SSID, the proposed procedures can help keep casual eavesdroppers at bay and give the wireless network an extra layer of protection. In order to undertake further in-depth research on the evolution of the WLAN landscape, wardriving with newer WNICs and high gain types of antennae and improved survey result accuracy is imperative. Finally, the data analysis process must be enhanced since the amount of WLAN data gathered will grow with time, necessitating more efficient data storage and sampling procedures. Along with studying the evolution of the broader WLAN networking landscape, more detailed research on Wardriving ethics will form part of our future work.

List of Abbreviations

AP: Access point
CIA: Confidentiality, integrity, and availability
GPS: Global positioning system
IEEE: Institute of electrical and electronics engineers
IoT: Internet of things
MAC: Media access control
MESL: Mobile enterprise security and legal
ISP: Internet service provider
OTM: On-the-move
PBC: Push button configuration
QA: Quality assessment
QSS: Quick secure setup
SMB: Small and medium-sized businesses
SOHO: Small offices and homes
SSID: Service set identifier
STRIDE: Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privileges
USB: Universal serial bus
VPN: Virtual private network
WEP: Wired equivalent privacy
Wi-Fi: Wireless fidelity
WIGLE: Wireless geolocation engine
WLAN: Wireless local area network
WPA: Wi-Fi protected access
WPS: Wi-Fi protected setup.

Data Availability

The data that support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest related to this work.

Acknowledgments

The work of Agbotiname Lucky Imoize was supported in part by the Nigerian Petroleum Technology Development Fund (PTDF) and German Academic Exchange Service (DAAD) through the Nigerian–German Postgraduate Program, under Grant 57473408.

References

[1] C. Kohlios and T. Hayajneh, *A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3*, pp. 1–28, MDPI, Basel, Switzerland, 2018.

[2] W-F Alliance, "Value of wi-fi," 2022, https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi.

[3] Business Wire, *Smart Home Will Drive Third Wave in Wireless Home Evolution: Strategy Analytics,* 2019, https://www.businesswire.com/news/home/20190807005530/en/Smart-Home-Drive-Wave-Wireless-Home-Evolution.

[4] G. Lorena, B. Cristian, and H. Julio, "Conceptual model of security variables in wi-fi wireless networks: review," in *Proceedings of the ITNG 2021 18th International Conference on Information Technology-New Generations*, AISC, June 2021.

[5] A. Hilal, A. Salman, and S. El-Tawab, "Exploring the use of IoT and WiFi-enabled devices to improve fingerprinting in indoor localization," in *Proceedings of the 2019 IEEE Global Conference on Internet of Things (GCIoT)*, IEEE, Dubai, December 2019.

[6] H. S. Choi, C. Darrell, and M. S. Ko, *Risk Taking Behaviors Using Public Wi-Fi*, Information Systems Frontiers, 2021.

[7] R. Kalniņš, J. Puriņš, and G. Alksnis, "Security evaluation of wireless network access points," *Applied Computer Systems*, vol. 21, no. 1, pp. 38–45, 2017.

[8] C. Hurley, R. Rogers, F. Thornton, and B. Baker, *WarDriving and Wireless Penetration Testing*, Elsevier Science, 2007.

[9] H. Valchanov, J. Edikyan, and V. Aleksieva, "A study of wi-fi security in city environment," in *Proceedings of the IOP Conference Series: Materials Science and Engineering*, IOP, October 2019.

[10] H. Chris, R. Rogers, F. Thornton, and B. Baker, *Wardriving and Wireless Penetration Testing*, Syngress, Rockland, 2007.

[11] P. S. Ryan, "War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics," *Virginia Journal of Law and Technology*, vol. 9, no. 7, pp. 3–57, 2004.

[12] B. D. Kern, "Whacking, joyriding and war-driving: roaming," *Santa Clara Computer and High Technology Law Journal*, vol. 21, no. 1, pp. 101–162, 2004.

[13] C. Meshram, A. Aljaedi, and A. R. Alharbi, "SBOOSP for massive devices in 5G WSNs using conformable chaotic maps," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 4591–4608, 2022.

[14] W. Sean, "Be aware of these 7 common wireless network threats," *Pluralsight,* 2020, https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats.

[15] C. Hurley, Rogers, and Thornton, *WarDriving and Wireless Penetration Testing*, Syngress, 2007.

[16] L. Caviglione, "Wireless wardriving," *Handbook of Research on Wireless Security*, pp. 61–77, 2008.

[17] S. Webb, *Growth in the Deployment and Security of 802.11b Wireless Local Area Networks in Perth, Western Australia*, pp. 48–56, Edith Cowan University, Perth, 2004.

[18] S. Yek, *Wily Attackers Seek Wireless Networks in Perth, Western Australia for Easy Targets*, Edith Cowan University, Perth, Western Australia, 2005.

[19] L. Chih-Ta, S. Hira, and J. Donald, "Wireless network security," *Unitec New Zealand*, pp. 337–339, 2004.

[20] L. Wolter, H. Vic, and G. John, *The Innovation Journey of Wi-Fi: The Road to Global Success*, Cambridge University Press, 2010.

[21] N. I. Sarkar and A. H. Abdullah, "Exploring wireless network security in Auckland City through warwalking field trials," in *Proceedings of the 13th International Conference on Advanced Communication Technology (ICACT2011)*, IEEE, Gangwon, January 2011.

[22] A. Sarrafzadeh and H. Sathu, "Wireless LAN security status changes in Auckland CBD: a case study," in *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research*, IEEE, Madurai, India, December 2016.

[23] A. Nisbet, "A tale of four cities: wireless security & growth in New Zealand," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)*, IEEE, Maui, HI, USA, January 2012.

[24] A. Nisbet, "A 2013 study of wireless network security in New Zealand: are we there yet?" in *Proceedings of the 11th Australian Information Security Management Conference*, Edith Cowan University, Perth, 2013.

[25] A. Sebbar, S. Boulahya, G. Mezzour, and M. Boulmalf, "An empirical study of WIFI security and performance in Morocco -WarDriving in Rabat," in *Proceedings of the 2nd International Conference on Electrical and Information Technologies ICEIT'2016*, IEEE, May 2016.

[26] Z. Akram, M. A. Saeed, and M. Daud, "Wardriving and its application in combating terrorism," in *Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, IEEE, Riyadh, Saudi Arabia, April 2018.

[27] H. A. Noman, S. A. Noman, and Q. Al-Maatouk, "Wireless security in Malaysia: a survey paper," *Journal of Critical Reviews*, vol. 7, no. 4, pp. 301–312, 2020.

[28] M. Maráczi, "Wardriving in eger," in *Proceedings of the IEEE 13th International Symposium on Applied Computational Intelligence and Informatics*, pp. 127–130, IEEE, Timisoara, Romania, May 2019.

[29] P. Bajpal, N. Raj Singh, and P. Singh, "Analysis of current WI-FI security practices via war driving and proposed solution," *International Journal of Advanced Computational Engineering and Networking, ISSN*, vol. 2, no. 7, pp. 45–49, 2014.

[30] E. Nasr, M. Jalloul, J. Bachalaany, and R. Maalouly, "Wi-fi network vulnerability analysis and risk assessment in Lebanon," in *Proceedings of the International Conference of Engineering Risk*, Beirut, May 2019.

[31] C. Priya, S. Umar, and T. Sirisha, "The impact of war driving on wireless networks," *IJCSET*, vol. 3, no. 6, pp. 230–235, 2013.

[32] E. Eldaw, A. M. Zeki, and S. Senan, "Analysis of wardriving activity and WiFi access points," *Communications in Computer and Information Science*, vol. 366, pp. 51–59, 2013.

[33] F. Santos, P. Pesantes, and S. Bonilla-Bedoya, "Exploring wardriving potential in the Ecuadorian Amazon for indirect data collection," in *Proceedings of the 2020 International Symposium on Water, Ecology and Environment - Earth and Environmental Science*, Quito, Ecuador, 2021.

[34] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," *Computer Networks*, vol. 197, p. 108359, 2021.

[35] O. Edward, K. Julius, P. Thibault, and C. Jon, "Wi-fi wardriving studies must account for important statistical issues," *IEEE*, pp. 1–11, 2020.

[36] O. H. Anayo, O. C. kelechi, A. I. Yinka, and E. Godwin, "Security in wireless local area network," *Journal of*

Multidisciplinary Engineering Science and Technology (JMEST), vol. 8, no. 7, pp. 14291–14295, 2021.

[37] S. Lindroos, *Developing a Systematic Process for Mobile Surveying and Analysis of WLAN Security*, UNIVERSITY OF TURKU, Turku, 2020.

[38] S. Domien, R. Aanjhan, and V. Mathy, "Let numbers tell the tale: measuring security trends in wi-fi networks and best practices," in *Proceedings of the Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21)*, ACM, New York, June 2021.

[39] S. Benqdara and A. Mahmoud, "Wireless security in Libya: a survey paper," *International Journal of Computer Applications*, vol. 181, no. 35, pp. 26–31, 2019.

[40] E. Lawrence and J. Lawrence, "Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking," in *Proceedings of the INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: CODING AND COMPUTING*, IEEE, Las Vegas, NV, USA, April 2004.

[41] A. S. Mashhour and Z. Saleh, "Wireless networks security in Jordan: a field study," *International journal of Network Security & Its Applications*, vol. 5, no. 4, pp. 43–52, 2013.

[42] S. Verma, Y. Kawamoto, and N. Kato, "A network-aware internet-wide scan for security maximization of IPv6-enabled WLAN IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8411–8422, 2021.

[43] I. Hossain, M. M. Hasan, S. F. Hasan, and M. R. Karim, "A study of security awareness in Dhaka city using a portable Wi-Fi pentesting device," in *Proceedings of the International Conference on Innovation in Engineering and Technology (ICIET)*, IEEE, Dhaka, Bangladesh, December 2019.

[44] P. R. Lutui, O. Tete'imoana, and G. Maeakafa, "An analysis of personal wireless network security in Tonga: a study of nuku'alofa," in *Proceedings of the 27th International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, Melbourne, VIC, Australia, December 2017.

[45] P. Shinde, A. Karve, and P. Mandaliya, "Wireless security audit & penetration test using Raspberry pi," in *Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET)*, IEEE, Mumbai, India, January 2018.

[46] F. Syahrul, N. Akhyari, and S. Nooraida, "Wireless network attacl: raising the awareness of Kampung wi-fi residents," in *Proceedings of the International Conference on Computer & Information Science (ICCIS)*, Kuala Lumpur, Malaysia, June 2012.

[47] C. Gherghina and G. Petrică, "Wireless LAN security issues (II). Security assurance," *International Journal of Information Security and Cybercrime*, vol. 3, no. 1, pp. 37–46, 2014.

[48] A. Achtzehn, L. Simi´c, M. Petrova, and P. M¨ah¨onen, "IEEE 802.11 wi-fi access point density estimation with capture-recapture models communications (CNC)," in *Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Workshop on Computing and Networking*, IEEE, March 2015.

[49] K. Jones and L. Liu, "What where Wi: an analysis of millions of wi-fi access points," in *Proceedings of the 2007 IEEE International Conference on Portable Information Devices*, Orlando, FL, USA, May 2007.

[50] Z. C. Schreuders and A. M. Bhat, "Not all ISPs equally secure home users: an empirical study comparing wi-fi security provided by UK ISPs," in *Proceedings of the 2013 International Conference on Security and Cryptography (SECRYPT)*, Reykjavik, Iceland, July 2013.

[51] A. Bandong, C. Felizardo, F. Cedric Angelo, and W. M. Tan, "Opportunistic wardriving through neighborhood public utility vehicles as an alternative to crowdsourcing and dedicated wardriving for wireless network data collection," in *Proceedings of the IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, IEEE, Bali, Indonesia, November 2018.

[52] F. Valle and M. Alonso, "Identifi cation of patterns in the use of wired equivalent privacy (wep) as a security protocol in wi-fi networks," *Research Square*, pp. 1–18, 2022.

[53] M. G. Huwida Said and I. A. A. Noora Al Mutawa, "Forensics and war-driving on unsecured wireless network," in *Proceedings of the 6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, United Arab Emirates, December 2011.

[54] K. Vyas, A. Sharma, and D. Songara, "The growing phenomenon of wireless crime forensic a tracing and tracing," *International Journal of Computational Engineering Research*, vol. 2, no. 1, pp. 150–156, 2012.

[55] S. K. M. Ataelmanan and M. A. H. Ali, "Develop an effective security model to protect wireless network," *IJCSNS International Journal of Computer Science and Network Security*, vol. 21, no. 3, pp. 48–54, 2021.

[56] D. Vega, A. Lozano, F. Blanco, and F. Simanca, "Model for the implementation of security in wi-fi networks for SMEs," *Journal of Physics: Conference Series*, vol. 1828, no. 1, p. 012105, 2021.

[57] K. Young-Long, "Seoul's Wi-Fi hotspots: Wi-Fi access points as an indicator of urban vitality," *Computers, Environment and Urban Systems*, pp. 1–12, 2018.

[58] E. Ahmet and K. Mesrure Betül, "Wi-fi security analysis for E&M-Government applications," *International Journal of Multidisciplinary Studies and Innovative Technologies*, vol. 3, no. 2, pp. 86–98, 2019.

[59] P. Kavitha and M. Usha, "Anomaly based intrusion detection in WLAN using discrimination algorithm combined with naïve bayesian classifier," *Journal of Theoretical and Applied Information Technology*, vol. 62, no. 1, pp. 77–84, 2014.

[60] U. Kumar and S. Gambhir, "A literature review of security threats to wireless networks," *International Journal of Future Generation Communication and Networking*, vol. 7, no. 4, pp. 25–34, 2014.

[61] A. M. Thomas, G. A. Kumaran, R. Ramaguru, R. Harish, and K. Praveen, "Evaluation of wireless access point security and best practices for mitigation," in *Proceedings of the 2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, Mysuru, India, December 2021.

[62] H. J. Lu and Y. Yu, "Research on WiFi penetration testing with Kali Linux," *Complexity*, vol. 2021, pp. 1–8, 2021.

[63] D. Delija, Ž. Petrović, G. Sirovatka, and M. Žagar, "An analysis of wireless network security test results provided by Raspberry pi devices on Kali Linux," in *Proceedings of the 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, IEEE, Opatija, Croatia, September 2021.

[64] B. Sándor, "Warflying – 2.4 ghz and 5 ghz wireless network detection by drone in critical infrastructure," *Cybersecurity-Review*, pp. 1–11, 2020.

[65] N. N. Shree, K. Kamesh, S. Vishwa, R. Ravikumar, and R. Hegde, "Security challenges in mobile communication networks," in *Proceedings of the 2019 Third International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, January 2019.

[66] F. Tchakounte, M. Nakoe, B. O. Yenke, and K. P. Udagepola, "Recognizing illegitimate access points based on static features: a case study in a campus wifi network," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 4, pp. 279–291, 2019.

[67] S. B. Vanjale and P. B. Mane, "Multi parameter based robust and efficient Rogue AP detection approach," *Wireless Personal Communications*, vol. 98, no. 1, pp. 139–156, 2018.

[68] M. Taneja, S. Bhiwapurkar, N. Mohanty, and B. Bhattacharyya, "Vulnerability analysis and testing of wireless networks through warstorming," in *Proceedings of the 2021 International Conference on Advances in Computing and Communications (ICACC)*, IEEE, Kochi, Kakkanad, India, October 2021.

[69] J. M. Kizza, "Security in wireless networks and devices texts in Computer Science," in *Guide to Computer Network Security*, pp. 399–428, Springer, 2020.

[70] D. I. Quirumbay, I. A. Coronel, M. M. Bayas et al., "Threats and risks to information security: a practical analysis of free access wireless networks," in *Proceedings of the SPIE 10445, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments*, SPIE, August 2017.

[71] O. J. Adinya, B. I. Ele, and I. O. Obono, "The impact of emerging wireless network system And cybersecurity in a global community," *iJournals: International Journal of Software & Hardware Research in Engineering (IJSHRE)*, vol. 9, no. 3, pp. 53–65, 2021.

[72] P. Satam and S. Hariri, "WIDS: an anomaly based intrusion detection system for wi-fi (IEEE 802.11) protocol," *IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT*, vol. 18, no. 1, pp. 1077–1091, 2021.

[73] B. Liao, Y. Ali, S. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[74] S. Nazir, S. Shahzad, and N. Mukhtar, "Software birthmark design and estimation: a systematic literature review," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3905–3927, 2019.

[75] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," *British Journal of Management*, vol. 14, no. 3, pp. 207–222, 2003.

[76] W. Jane and R. T. Watson, "Analyzing the past to prepare for the future: writing a literature review," *Management Information Systems Research Center, University of*, vol. 26, no. 2, pp. 8–18, 2002.

[77] O. Chitu, "A guide to conducting a standalone systematic literature review," *Communications of the Association for Information Systems*, vol. 37, no. 43, pp. 879–910, 2015.

[78] Prisma, "Prisma TRANSPARENT REPORTING of SYSTEMATIC REVIEWS and META-ANALYSES," 2021, http://prisma-statement.org/PRISMAStatement/FlowDiagram.aspx.

[79] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, 2007.

[80] P. Achimugu, A. Selamat, R. Ibrahim, and M. N. Mahrin, "A systematic literature review of software requirements prioritization research," *Information and Software Technology*, vol. 56, no. 6, pp. 568–585, 2014.

[81] E. M. Grames, A. N. Stillman, M. W. Tingley, and C. S. Elphick, "An automated approach to identifying search terms for systematic reviews using keyword co-occurrence networks," *Methods in Ecology and Evolution*, vol. 10, no. 10, pp. 1645–1654, 2019.

[82] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, ACM, London, England, May 2014.

[83] S. Mahdavi-Hezavehi, V. H. S. Durelli, D. Weyns, and P. Avgeriou, "A systematic literature review on methods that handle multiple quality attributes in architecture-based self-adaptive systems," *Information and Software Technology*, vol. 90, pp. 1–26, 2017.

[84] A. K. Kable, J. Pich, and S. E. Maslin-Prothero, "A structured approach to documenting a search strategy for publication: a 12 step guideline for authors," *Nurse Education Today*, vol. 32, no. 8, pp. 878–886, 2012.

[85] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," Tech, Rep, EBSE–2007–01, Elsevier, pp. 1–57, Durham, UK, 2007.

[86] J. M. Norris and L. Ortega, "Effectiveness of L2 instruction: a research synthesis and quantitative meta-analysis," *Language Learning*, vol. 50, no. 3, pp. 417–528, 2000.

[87] I. Shadeed Al-Mejibli and D. N. Rasheed Alharbe, "Analyzing and evaluating the security standards in wireless network: a review study," *Iraqi Journal for Computers and Informatics*, vol. 46, no. 1, pp. 32–39, 2020.

[88] S. Ekhator, *Evaluating Kismet and NetStumbler as Network Security Tools & Solutions*, Digitala Vetenskapliga Arkivet, M.S. thesis, 2018.

[89] A. A.-G. Hezam and K. Dimitri, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: an IoT perspective," *A Journal of sensor and acuator networks*, vol. 8, no. 22, pp. 1–38, 2019.

[90] J.-K. Kim, W.-J. Lee, C.-B. Chae, and J.-H. Kim, "Performance analysis of fair medium access control protocol for asymmetric full duplex in WLAN," *IEEE Access*, vol. 8, pp. 140546–140557, 2020.

[91] E. Baray and N. K. Ojha, "WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique," in *Proceedings of the Fifth International Conference on Computing Methodologies and Communication*, IEEE, Erode, India, April 2021.

[92] K. Juhász, V. Póser, and M. Kozlovszky, "Wi-Fi vulnerability caused by SSID forgery in the IEEE 802.11 protocol," in *Proceedings of the IEEE 17th World Symposium on Applied Machine Intelligence and Informatics*, IEEE, Herlany, Slovakia, January 2019.

[93] K. S. V. Susmita and D. P. Kailas, "Portable firewall for data security toward secured communication," *East African Scholars Journal of Engineering and Computer Sciences*, vol. 4, pp. 41–45, 2021.

[94] VARinsights, "WLAN security: 802.1x vs. VPNs," 2021, https://www.varinsights.com/doc/wlan-security-8021x-vs-vpns-0001.

[95] J. Jaejin and I. Y. Jung, "Sustainable and practical firmware upgrade for wireless access point using password-based authentication," *Sustainability*, vol. 8, no. 9, pp. 1–17, 2016.

[96] A. Imoize, B. Ben-Adeola, and J. Adebisi, "Development of a multifactor-security-protocol system using ambient noise synthesis," *ICST Transactions on Security and Safety*, vol. 6, no. 22, p. 163979, 2020.

[97] H.-J. Lu and Y. Yu, "Research on WiFi penetration testing with Kali Linux," *Complexity*, vol. 2021, pp. 1–8, 2021.
[98] Wigle, "Wigle.net," 2021, https://wigle.net/.
[99] S. Ojo, M. Akkaya, and J. C. Sopuru, "An ensemble machine learning approach for enhanced path loss predictions for 4G LTE wireless networks," *International Journal of Communication Systems*, vol. 35, no. 7, 2022.
[100] J. Isabona, A. L. Imoize, S. Ojo, C.-C. Lee, and C.-T. Li, "Atmospheric propagation modelling for terrestrial radio frequency communication links in a tropical wet and dry savanna climate," *Information*, vol. 13, no. 3, p. 141, 2022.
[101] J. Isabona, A. L. Imoize, P. Rawat et al., "Realistic prognostic modeling of specific attenuation due to rain at microwave frequency for tropical climate region," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–10, 2022.
[102] S. Ojo, A. Imoize, and D. Alienyi, "Radial basis function neural network path loss prediction model for LTE networks in multitransmitter signal propagation environments," *International Journal of Communication Systems*, vol. 34, no. 3, 2021.
[103] B. Bilgehan and S. Ojo, "Multiplicative based path loss model for wireless channels," *International Journal of Communication Systems*, vol. 17, no. 31, pp. 1–18, 2018.
[104] D. Dalibor, S. Zeljko, J. Stefan, and R. Zoltán, "A method for comparing and analyzing wireless security situations in two capital cities," *Acta Polytechnica Hungarica*, vol. 13, no. 6, pp. 67–86, 2016.
[105] E. Veroni, C. Ntantogian, and C. Xenakis, "A large-scale analysis of Wi-Fi passwords," *Journal of Information Security and Applications*, vol. 67, p. 103190, 2022.
[106] K. Ar Kar, A. Pulin, and C. Brian, "Wi-Pi: a study of WLAN security in Auckland CBD," in *Proceedings of the International Conference Proceeding Series (ICPS)*, Auckland, February 2016.
[107] C. Priya, S. Umar, and T. Sirisha, "The impact of war driving on wireless networks," *International Journal of Computer Science Engineering and Technology*, vol. 3, no. 6, pp. 230–235, 2013.
[108] Wireshark, "OUI lookup tool," 2021, https://www.wireshark.org/tools/oui-lookup.html.
[109] A. Sadeghian, "Analysis of WPS security in wireless access," in *Proceedings of the Advanced Informatics School (AIS) Universiti Teknologi Malaysia*, UTM, Kuala Lumpur, 2014.
[110] S. Lindroos, A. Hakkala, and S. Virtanen, "The COVID-19 pandemic and remote working did not improve WLAN security," *Procedia Computer Science*, vol. 201, pp. 158–165, 2022.
[111] A. Efe and M. B. Kaplan, "Wi-fi security analysis for E&M-Government applications," *International Journal of Multidisciplinary Studies and Innovative Technologies*, vol. 3, no. 2, pp. 86–98, 2019.
[112] A. E. Ibhaze, I. K. Okakwu, A. T. Akinrelere, and A. L. Imoize, "An intelligent dispatch system operating in a partially closed environment," *Network and Communication Technologies*, vol. 4, no. 1, p. 26, 2019.
[113] A. L. Imoize, O. A. Ajibola, T. R. Oyedare, J. O. Ogbebor, and S. O. Ajose, "Development of an energy-efficient wireless sensor network model for perimeter surveillance," *International Journal of Electrical Engineering and Applied Sciences (IJEEAS)*, vol. 4, no. 1, 2021.
[114] U. P. Rao, P. K. Shukla, C. Trivedi, S. Gupta, and Z. S. Shibeshi, Eds., *Blockchain for Information Security and Privacy,* Auerbach Publications, 1st ed edition, 2021.
[115] S. Joshi, S. Stalin, P. K. Shukla et al., "Unified authentication and access control for future mobile communication-based lightweight IoT systems using blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, p. 12, Article ID 8621230, 2021.
[116] A. L. Imoize and O. B. Alabi, "Implementation of a user-friendly radio frequency identification and password-enabled security access system," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 13, no. 2, pp. 23–30, 2021.
[117] Y. Lyu, Y. Mo, S. Yue, and W. Liu, "Improved beetle antennae algorithm based on localization for jamming attack in wireless sensor networks," *IEEE Access*, vol. 10, pp. 13071–13088, 2022.