An Investigation into How Smartphones Can Be Secured Against MiTM Attacks: Financial Sector

David Steiner-Otoo and Hamid Jahankhani

Abstract MiTM attack aims to violate data in transmission through the air medium in a wireless network; MITM exploits compromise data confidentiality and integrity and are conceivably the most productive types of cyberattacks utilised today. The increasing use of personal devices like smartphones connecting to the internet via Wi-Fi has made wireless attacks on users more crucial. The cyber adversary becomes a "middleman" between two targets to intercept private communication, decrypt traffic, and exploit valuable information like bank details and credit cards. The new WPA3 protocol security features such as 256-bit encryption, OWE (Opportunistic Wireless Encryption), Simultaneous Authentication of Equals (SAE), and disallowing outdated legacy protocols provides risk mitigation against attacks. However, vulnerabilities in WPA3 have been reported whereby a device can be downgraded from WPA3 to WPA2, which opens the system up for DoS and MiTM attacks. This research investigates Wi-Fi-based exploits against the ecosystem of smartphones in the financial sector. Aircrack-ng and Ettercap are open-source tools accessible through the Kali Linux framework. These tools are utilised to demonstrate simulated DoS and MiTM attacks to explain the reported WPA3 vulnerabilities.

Keywords 802.11i · Blockchain · COVID-19 · Encryption · WPA2 · WPA3 · Kali linux · Penetration testing · Self-sovereign identity · Wi-Fi · Wi-Fi 6 · Wi-Fi 7 · WLAN

1 Introduction

Wi-Fi stands for Wireless Fidelity with the generic name of IEEE 802.11, and suffixes are added to represent improved versions of Wi-Fi. Recently launched Wi-Fi 6 (and Wi-Fi 6E) or 802.11ax is the current release, and Wi-Fi 7 or labelled 802.11be is

D. Steiner-Otoo
Northumbria University London, London, UK

H. Jahankhani (✉)
Northumbria University London Campus, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Other Emerging Technologies for Digital Business Strategies*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-98225-6_7

projected to be released in 2024 [1]. Wi-Fi is a necessity today and in finance, and the technology extends to robotics, the Internet of Things—IoT, and the Internet of Everything—IoE [2]. The global economic value generated using Wi-Fi is estimated to grow from $3.3 trillion to $4.9 trillion in 2025, while mobile data is anticipated to rise from approximately 51 billion Gigabytes in 2020 to 226 billion Gigabytes in 2026 on a month-to-month basis [3]. However, there is a growing concern about wireless security vulnerabilities.

Man-in-The-Middle or MiTM (sometimes abbreviated in the literature as MIM, MiM, MITMA) attacks have different names such as machine-in-the-middle [4], monkey-in-the-middle [5], person-in-the-middle [6], or Man-in-the-PC/Phone (MITPC/Phone attack [7]. MiTM exploits aim to violate confidentiality and integrity of data in transmission through a wireless (Wi-Fi network, mitm exploits are conceivably the most productive types of cyberattacks utilised today [8].

The importance of smartphones in daily life, including financial transactions, social media and culture, cannot be understated. Smartphone usage permeates and impacts every demography in Great Britain and globally. However, users have limited knowledge in mitigating risk against hackers, while application developers do not always consider and implement the appropriate security checks during development.

2 Literature Review

The genesis of banking and financial institutions can be traced as far back to ancient civilisation in Kemet (in northern Africa, present-day Egypt) before 4000 BCE, which has some of the "oldest recorded civilisation" that in turn influenced the advancement of later societies and cultures in ancient Asia, Greece, and the Roman Empire [9]. In evaluating the evolution of money and monetary institutions, religion and finance have a direct correlation and significance, the early banks started "in the temples consecrated to the ancient gods" [10]. As was in ancient civilisations, and followed by the Romans, the religious temples such as the temple of Jerusalem and Apollo at Delphi, worship edifices functioned as the first banks or financial institutions (Innes 1913, cited in [11]. Labate [10] describes the early temples as the initial repositories (i.e., banks) where money and treasures of wealthy Romans were deposited in the basements of numerous temples. The temples were involved in banking activities like lending based on their good names and reputation, the priests acted as modern-day banking officers who monitored deposits and loans. The temples were secure because the buildings were regularly inhabited by faithful worshipers and ecclesiastics and constantly guarded by soldiers [10]. This can be analogised as the equivalent of modern-day financial institutions' cybersecurity tools and techniques to secure against theft, financial loss and data attacks. In essence, the priests acted as the temple/bank's Chief Financial Officer (CFO) and Chief Technology Officer (CTO), the patrolling soldiers were the firewalls and intrusion detections systems, while the devout worshipers unknowingly acted as the early form of threat intelligence gatherers—all being risk mitigations against attacks.

Financial institutions have evolved over the centuries from the traditional to contemporary FINTECHs, together with technological advances. Data, an intangible commodity, comes into the equation, so security becomes imperative and more challenging to achieve nearly 100%. At the core of most digital transactions is the reliance on protection to mitigate against cyberattacks such as man-in-the-middle exploits. Thakor [12] describes Fintech as "the use of technology to provide new and improved financial services". This includes innovations in payment services in cryptocurrencies and the role played by Blockchain-assisted intelligent contracts. The goal of financial innovations integrated with technological advances is to lower financial services costs or risks, improve digital security for the consumer, and improve social welfare [13]. The most significant disruption and innovation by Fintech are with cryptocurrency payment systems like Bitcoin, which are digital and virtual currencies stored in electronic/digital wallets in cyberspace that allows peer-to-peer transactions independent of traditional financial banks. Cryptocurrency transactions rely on decentralised control, security and verification methods based on cryptography-based distributed digital ledger technology, the Blockchain, that supplants the conventional banks [12].

2.1 MiTM Attacks

Man-in-The-Middle exploits is a significant security concern whereby threat actors target data in transmission between two legitimate endpoints to compromise the data integrity and confidentiality [14]. The malicious third party can intercept, read, modify or control the communication traffic. MiTM attacks require a communication channel, the popularly used are radio frequency and Wi-Fi, Bluetooth, GSM (Global System for Mobiles), NFC or Near Field Communication [15]. Mobile devices are prone to such attacks [16] when in the process of securing connectivity with an access point or a server. The review of existing literature shows an abundance of research journals on MiTM attacks in healthcare services, transportation, and retail sectors, but a limited number of articles in the financial industry. Financial institutions hold a large quantum of sensitive data, when exposed, this can cause harm to the UK and global economic security and personal interests [17]. Financial institutions are compelled and legally obligated to report security and data breaches to the ICO [18] to satisfy relevant legislations—data protection regulations (GDPR) and the Data Protection Act (2018) [19]. According to the UK's Financial Conduct Authority, FCA [20], cyberattacks against banks in Britain have risen from five in 2014 to forty-nine in 2017. However, banks are reluctant to report such attacks for fear of bad publicity and punishment from regulators. According to Carnegie [21], in January 2021, American Express and the Reserve Bank of New Zealand suffered a cybersecurity attack resulting in a data breach, in March 2021, Wall Street was targeted in New Capital Call cyber fraud scheme, also in March 2021, the American insurance company CNA was hit by a cyberattack. The limited number of MiTM attack research papers in the financial sector is mainly because research experiments

must be conducted in laboratories, which are often not ideal environments and not representative of fully functioning financial institutions.

2.2 *Security Vulnerabilities and Attacks in Mobile Banking and Trading Apps*

A study by Zheng et al. [22] analysed security vulnerabilities in Android OS based mission-critical smartphone apps such as mobile trading and banking apps. The study examined application repackaging attacks whereby a legitimate Android app is reverse-engineered, malicious program codes inserted and rebuilt as a new application. The study found that ineffective security mitigation measures were the main reasons malicious repackaged apps are easily uploaded in Android markets like Google Play, Amazon Appstore, and other app markets. A report by Ciscomag [23] suggested that more than 50% of mobile banking apps were vulnerable to data theft and fraud because of "inadequate security layers". Android OS is an open-source model, making malicious tools and applications easier access to data and information on users' smartphone apps. The authors found that anti-malware tools use signature-based or static analysis methods which evade obfuscation, allowing hackers to adapt by using metamorphism and polymorphism to evade anti-malware countermeasures. Due to inadequate security, 76% of banking apps have vulnerabilities that can be hacked without accessing the physical device, and 33% can be attacked without having administrative privileges [24]. The authors proposed user education as an essential step to protect mobile banking apps against hackers. However, users are more interested in the app functionality and user experience (UI) and do not see themselves as security experts. Another attack prevention approach was using a trusted agency guaranteeing the developer identity and genuineness of the application by inserting "an assurance signature" into the application package so that users can make better-informed decisions when installing apps on their smartphones.

X-Force Exchange by IBM [25] is a cloud-based TI open-source platform that allows users to quickly research current global security threats, share and act on threat intelligence supported by human and ML generated intelligence. More mature and advanced threat intelligence tools are currently available on the market, such as Kaspersky [26] Lab, which collects data from worldwide sources to give in-depth insights into cyber threats targeting financial institutions and revealing potential evidence of cyberattacks [27]. Insights' External Threat Protection (ETP) analysed vulnerability that is "engineered to discover, examine and mitigate cyber risks" and patch critical vulnerabilities [28]. However, TI has limitations due to the overwhelming quantity of available data, the challenges security teams face in identifying the most relevant data, and difficulty making valuable use of them. In some instances, the available intelligence (i.e., data) is out of date. The timeliness of data is essential in understanding strategies, tactics, and motivation of threat actors to protect against intrusive attacks and zero-day exploits. According to OWASP [29], the top ten mobile

risks are improper platform usage, insecure data storage, insecure communication, insecure authentication, insufficient cryptography, insecure authorisation, client code quality, code tampering, reverse engineering, and extraneous functionality.

2.3 Android and iOS—Security Compromise Issues and Analysis

Authors Garg and Baliyan [30] conducted a study on Android and iOS to ascertain security vulnerabilities between the two OSs. This comparative qualitative study included an analysis of the security model, system architecture, encryption mechanism, and app permissions. It listed the most common flaws in both platforms and presented a vulnerabilities assessment of the two OSs. The journal discussed malware attacks on Android and iOS and suggested future research and app development to prevent growing cyberattacks on the platforms. MiTM, DoS/DDoS, SYN flooding attacks are the most common attacks. The authors collected data from CVEDetails, a security vulnerability data source containing listings of publicly reported computer security vulnerabilities and the severity of flaws [31]. However, the US Department of Homeland Security (DHS) and CISA (cisa.gov, n.d.) maintain and sponsor a separate computer vulnerabilities database known as NVD, which also allows searches by but not limited to OS, vulnerability type, product name, severity, and impact. Although both CVE and NVD databases are synchronised, the authors could have missed high other risk vulnerabilities reported in NVD but not available in CVE during their study, hence limiting the study's accuracy. The study showed that the overall number of vulnerabilities in both platforms decreased between 2017 and 2019 because of improved detection rates due to the use of ML and DL algorithms. However, there were 61% more vulnerabilities with Android compared to 39% of iOS platforms.

2.4 Cyberattacks During COVID-19 Pandemic

Cyberattacks during the SARS-CoV-2 or COVID-19 [32] pandemic period in 2020 saw a considerable surge in attacks against financial institutions, individuals, and organisations.

2.4.1 Analysis of Cyberattacks During Pandemic

Lallie et al. [33] used mixed methods to present a timeline of events and analysis into the SARS-CoV-2 pandemic in the context of cyberattacks and cybercrimes that has witnessed a massive surge [34] compared to previous periods. The authors highlight cyberattacks types and persistency experienced in the UK and worldwide from

the onset of the global pandemic in 2020, which witnessed increased cybersecurity challenges ever recorded by citizenry and industry [35]. Hiscox [36] contends that cybercrime is growing in severity and frequency primarily due to inherent risks in centralised identity systems. This review focuses on the different types of cyber-attacks occurring during the pandemic and the impact on people. However, the review will not dwell on the timeline aspects of the attacks due to the unreliability of the timelines, limitations, and inaccuracies because the URLs on which they were reported could have been updated multiple times. The analysis of the cyberattacks was examined in the context of global and UK specific events and attacks to show how threat actors had developed advanced and sophisticated modii Operandi in the cyberattack offensive during the pandemic. During the rapid spread of COVID-19 worldwide in 2020, a significant increase in cyberattacks and cybercrime campaigns was perpetuated in the technology-driven society. Some attacks were indiscriminate, and others targeted. Coronavirus-themed scams that impersonated public authorities, fraud—especially financial fraud, and offering COVID-19 cures were reported. The COVID-19 pandemic cybercrime landscape included DDoS, ransomware, phishing, data harvesting malware like banking Trojans, and malicious domains. Statista3 [37] reported that the malware "Dridex" was the most prevalent banking trojan accounting for 26% of trojans during 2020.

The authors found that the most significant cybersecurity scams targeted the public at large, and millions of ordinary individuals were forced to work from home and suffer from raised anxiety and stress levels, and financial worries. Cybercriminals exploited the people's fears and uncertainty that had come about due to the "unstable social and economic situation" because of COVID-19 [38]. Furthermore, experiences of people working en-masse from home revealed the lack of preparation by both software vendors in terms of their product security. Organisations rapidly deployed remote networks and systems, enabling staff to perform tasks from home without the necessary attention to security vulnerabilities when VPNs could have been deployed, for example. January to April 2020 saw 907,000 spam messages, 737 malware exploits, and 48,000 malicious URLs related to COVID-19 reported by just one Interpol private sector partner. However, Interpol [38] contends that the most significant shift in cybercrime from small businesses and individuals has been an attack on critical national infrastructures like healthcare services [39], requiring new levels of oversight and security [40]. Unlike traditional attacks, advanced persistent threat (APT) groups build highly customised malware that is very targeted to increase the chances of success and achieve maximum impact [41], which were responsible for major critical infrastructure cyber exploits.

The UK NCSC, USA NSA, and Canada's CSE attributed the APT APT29, also called Cozy Bear or the Dukes, to the Russian Intelligence Services cyber espionage group, which targeted COVID-19 vaccine developments [42]. Lallie et al. use the UK's CPS categorisation of cybercrime guidelines, categorising cybercrime into two categories, namely, "cyber-dependent" and "cyber-enabled" crimes Cyber-enabled crimes include financial fraud, phishing, pharming, and extortion. In contrast, a cyber-dependent crime includes denial of service, hacking, and malware [43]. Definitions

of cyber-enabled and cyber-dependent crimes, including cybersecurity by default, are provided in the footnote.

In taking the UK as a case study to analyse the pandemic related cyber-crimes, the authors demonstrated direct correlations, meaning the association between news and policy announcements (such as the UK government hardship fund announcement in 24/03/2020 supporting the citizenry and economy) and associated cybercrime campaigns. The authors reported that by the 7th of May 2020, an excess of 160,000 suspect emails was reported to the NCSC [44], and £4.6 m was lost to coronavirus related scams affecting 11,260 victims of smishing or phishing campaigns. The 43 different types of cyberattacks investigated were categorised,86% involved phishing/smishing attacks; malware accounted for 65%; financial fraud was 34%; extortion was 15%, and pharming accounted for 13%.

COVID-19 and related cybercrimes impacted individuals' data and assets, the workforce. It presented challenges to information governance and regulatory compliance, social-economic structures, and how people communicated and lived[1].

Securing the individual's personal and sensitive information became a severe problem, such as the theft of a person's digital identity through the hacking and unauthorised access to PII or personally identifiable information (including name, national insurance number, and credit card details) via MiTM exploits, data breaches, and identity theft. According to the GDPR law (ICO n.d.), personal data breaches include unauthorised access to personal data transmitted. User's sensitive digital identity and information reside with service providers and centralised systems, and in most cases, users lack control over their digital identity and data flow [45]. The use of AI technology solutions and Self-Sovereign Identity (SSI) identity management system (IDM) offers a decentralised digital identity approach, a better security solution, and is more likely to enable the user to take back control of their digital identity and footprint. This reduces the risk of data breaches during data in transmission MiTM attacks while not depending on one trusted third party or external sources.

2.4.2 Cybersecurity Attack Vectors, Methods and Technics During Pandemic

Susukailo et al. [46] use qualitative analysis to describe cyberattack vectors, methods, and technics deployed by hackers during the global pandemic in 2020. It identifies the most frequent targets for hackers and the tactics used during cyberattacks. The authors review the cyber security challenges, possible countermeasures to improve the security situation, and cyber security controls to mitigate risk against the attack vectors analysed. The author contends that financial gain (arising from the COVID-19 financial crises) is the ultimate motivation of hackers, which is a necessary aspect

[1] Cyber-dependent crime is an offence, "*that can only be committed using a computer, computer networks or other form of information communications technology (ICT)*". Cyber-enabled crimes *are, "traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT)" (McGuire and Dowling 2013).*

of the attack vectors. Attack vectors were categorised into three groups: (i) social engineering attacks, (ii) interruption of critical business functions attacks, and (iii) critical infrastructure attacks. This review looks at the aspects of vulnerabilities involving social engineering. Social engineering exploits were the most prevalent attack vector, which preyed on an individual's compassion or fear and the need to find information online or in newspapers to protect themselves against the coronavirus. Hackers created numerous fake charitable websites deceiving people to earn money or infecting their computers with malware. Azourlt (also known as Puff-Stealer and Rultazo) was a common and popular stealer-type malware, used fake coronavirus phishing emails and online maps to steal the victims banking information, including credit card details and passwords, as well as cryptocurrency [47]. The Azourlt malware's delivery mode was through MS Office document, made simple by the hackers manipulating people's fears.

By opening the file, the malware exploited the CVE-2017–11882 MS Office Equation Editor vulnerability to download the malicious executable; the malicious executable file proceeds to make computer registry changes to run when the system starts. At system startup, the malware launches itself and steals personal data, and the malware deletes itself after a 3-s timeout. Social engineering techniques included the creation of fake online shops to sell COVID-19 related medical supplies and medicines with the sole purpose of attackers being financial gain. Susukailo et al. argue that the primary control to apply to deter social engineering attacks is information assurance strategies such as end-user training or awareness sessions with examples containing fake pandemic online resources. A secondary control against such attacks argued by the authors is the enablement of email malware scannings and phishing detection modules such as those found in Office 365 [48], G Suite (Google.com n.d.), and VirusTotal (Virustotal.com n.d.) browser extension.

2.5 Blockchain Technology

Fartitchou et al. [49] define blockchain (BC) as "a decentralised distributed database technology secured by means of cryptographic algorithms", the append-only ledger database cannot be altered. The BC works in a P2P (Peer-to-Peer) system, with each node in the blockchain system having a duplicate of the blockchain. Additionally, records of transactions and timestamps are made simultaneously and distributed and do not involve a "trusted" 3rd party entity or jurisdiction (Singh et al. 2019, cited in [49]). The security and performance behind BC are due to the cryptographic algorithms like RSA, Rivest-Shamir-Adleman, [50] and ECDSA (Elliptic Curve Digital Signature Algorithm) (Johnson et al. 2001, cited in [49]), and proof-work (PoW) and proof-of-state (PoS) consensus protocols. Notwithstanding advanced and integrated security mechanisms, BC technology has weaknesses and have "certain vulnerabilities" to attacks [49]. According to Orcutt [51], hackers have stolen about $2 billion work of cryptocurrencies from trading platforms since 2017, for example,

$1.1 million was taken from Ethereum Classic and $450 million bitcoins stolen from MtGox [49].

2.5.1 Blockchain and Self-Sovereign Identity Systems to Address Cyberattacks

Researchers Bandara et al. [52] proposed a blockchain and SSI based digital identity platform called "Casper" to address inherent problems with centralised identity systems such as cyberattacks and data breaches. However, a single definition of digital identity presents complexities in proving who the person says they are in the digital realm. It also offers legal, social and economic issues that have yet to be standardised or established and opens up favourable opportunities for a hacker to impersonate the individual [53]. Bitcoin has influenced the SSI evolution due to its underlying Distributed Ledger Technology (Dunphy and Petitcolas 2018, cited in, [54]). The majority of current identity platforms utilise centralised data storage architecture such as central servers and cloud storage, which have intrinsic security, data privacy, and user control issues. Stockburger et al. [55] contend that data is unprotected and insecure without digital identity. Casper integrates blockchain and SSI-based approaches and is an Android and iOS based mobile identity wallet app. The actual user/customer identities were contained in the individual's smartphone wallet app.

The proof of the user identities is contained in a blockchain-based decentralised storage system as SSI proof. SSI negates the requirement for central trusted authority [56]. The Casper platform's SSI-based system gives a Zero Knowledge Proof (ZKP) mechanism in verifying the identity information. The Casper platform is adaptable and can be used in banking, healthcare, government agencies, and businesses. Casper is intended to ensure security, decentralised and ZKP verifiable identity by utilising blockchain and SSI-based approaches. Zero-knowledge proof is a complex protocol incorporating encryption techniques. The prover convinces the other party, the verifier, of the truthfulness of an assertion or statement without the disclosure of other specifics than the statement itself [57].

For methodology, the researchers' use case for the Casper project was the implementation of an inter-bank Know Your Customer (KYC) for banking clientele. Customer identity or decentralised identity (DID) was embedded in the QR code of the mobile wallet. For the Casper project, all the user's personal data was stored in the user's mobile device hardware based on the SSI model; cryptographic DID proofs and other information were stored in blockchain storage. The researchers demonstrated that customers could prove their identity and be able to share their data with other banks, organisations, hospitals, and other entities when they used the mobile wallet. Furthermore, other entities were able to verify customers' identities using ZKP and to verify credentials; the researchers provided a mobile and web-based app for admin staff such as bank officers and healthcare service admins. The researchers' findings proved that the use of blockchain and SSI enabled DID systems coupled with iOS/Android mobile identity wallet (to capture and verify user's identity proofs)

addressed the threats and challenges in centralised identity systems. It also offered greater data privacy, confidentiality, integrity, and authentication while providing authorisation features. Even though blockchain technology seems ideal concerning SSI, Bokkem et al. [54] argue that there are limitations, for example, when the users lose the private/public key pair, the identity proofing process needs to start from the beginning to re-establish their digital identity.

2.5.2 Hyperledger Framework—MiTM Exploits in a Blockchain-Based Identity System

Bhattacharya et al. [58] examined scenarios whereby Personally Identifiable Information (PII) or personal data can be disclosed through credential exchanges between SSIs, risking MiTM exploits in a blockchain-based identity system like Hyperledger Indy. Hyperledger Indy is part of the Hyperledger framework (including Hyperledger Fabric, Cello, Iroha, Explorer and Composer), comprising open-source tools involving different organisations to build robust business-driven blockchain-based enterprise solutions [59]. The authors analysed the risk of MiTM attack that could takeover between two unknown peers DID connections in the initial setup process. An essential aspect of SSI systems is the unique relationships among peers in which an identity holder can form a relationship with another identity holder. Therefore, unless the two peers can satisfy each other about the authenticity of the peer ID connection, each party must verify the other when a new connection is established by using "verifiable credentials" (Deventer et al. 2020, cited in [58]). However, if a hacker can proxy a request/response between the two entities, then the authentication process between the entities fails.

Bhattacharya et al. proposed a mechanism to detect and mitigate the risk of MiTM attacks between peer SSIs. This involved an agency of self-signing features utilising the sender's private key peer ID, which will guarantee that the party generating the message and delivering it is the actual sender; and the use of unique DIDs and keys, which can only be resolved by the two parties in the relationship with each other. A mismatching signature alerts the receiving party that the message was not originating from the original transmitter. At this point, any peer connection is terminated to stop PII and data breaches. Additionally, Bhattacharya et al. proposed a quantitative model that computes a reputation score for credential issuers, enabling a quantitative confidence level value for the issuer. This aids in eliminating privacy and security concerns when there is a communication with a new peer that presents verifiable credentials that the issuer issued. The limitation of this study is that there was no comparison with other SSI ecosystems; it would have been worthwhile to present comparative analysis, however brief, with at least one other SSI system to ascertain how MiTM risk mitigations are handled. Furthermore, the authors did not propose best practices on building trust between DIDs, also did not suggest what minimum data would be required to complete a task to prevent the accumulation of private data by an attacker or even by legitimate parties.

2.6 *Using Artificial Intelligence Mitigation Predicated ML Techniques Against Attacks*

Zhang et al. [60] investigated and analysed DDoS attack detection and prevention using artificial intelligence mitigation predicated ML techniques. This work presented a detailed survey on the current advancements in detecting attacks using machine learning algorithms (Random Forest tree) plus Naïve Bayes. It provided recommendations on AL methods to be utilised to detect and prevent DDoS attacks. Typically, AI techniques include ML, natural language processing, and speech recognition [61]. The authors contend that the average size of packets, pack size variance, number of packets, number of bytes, bit rate, packet rate, and time interval are features that can be used in detecting DDoS attacks. However, Anandshree et al. [62] have argued that detecting DDoS attacks are complex because legitimate data packets are not distinguishable from illegitimate packets. And Yuan et al. [63] have suggested that AI/ML defences are more advantageous as countermeasures against DDoS attacks than other antidotes such as Blockchain risk mitigation techniques.

Zhang et al. use of AI techniques offer substantially higher accuracy in identifying and averting DDoS attacks. Applying Naïve Bayes in ML classifications provides about 97% accuracy. Adding a Random Forest tree or Gaussian Naïve Bayes with the data obtained produces at least 99% accuracy in detecting DDoS attacks. Substantially, automatically detecting packets from DDoS exploits becomes the primary mechanism for risk mitigations. Verisign [64] DDoS trends claim that:

- The top three industries targeted were the financial industry, IT Services/SAAS/Cloud, and the Telecom sectors.
- The financial sector represented 57% of mitigation activity, the highest routinely targeted industry; IT Services/SAAS/Cloud experienced 26% had the second-highest amount of DDoS attack; the Telecom sector represented 17% of mitigation activity.
- 58% of DDoS attacks mitigated by Verisign used at least two different attack types.
- User Datagram Protocol (UDP) floods accounted for 50% of DDoS exploits.
- The second highest frequent attack vector or 26%, were TCP-based attacks in the quarter.

Support Vector Machine (SVM) and Artificial Neuron Network are other ML algorithms applied to the DDoS defence anomaly detection phase. The authors recommend using Naïve Bayes and random forest trees to be used in classifying regular traffic and pernicious traffic for better performance. Furthermore, the authors recommend combining ML algorithms to detect DDoS exploits; these have a "better accuracy and performance".

2.7 *New Security Features in Wi-Fi 6 WPA3 and Enhanced WPA2 Security*

The enhanced security in WPA2 and the adoption of new security features in Wi-Fi 6 and WPA3 (Wi-Fi Protected Access 3) (Wi-Fi [65] introduced in June 2018 has been mandated for use in devices connecting to wireless networks to make data in transmission security more robust. The goal of WPA3 certification is securing home Wi-Fi networks, whilst enterprise wireless networks use EAP-pwd to authenticate users. Both the WPA3 certification and EAP-pwd use the Dragonfly handshake to give forward secrecy and protection against dictionary attacks [66]. The new WPA3 protocol could be a significant disruptor in MiTM attacks.

University of Leuven, Belgium, KU Leuven, researcher Vanhoef [67], discovered the KRACK or **K**ey **R**einstallation **A**tta**ck**s vulnerability in the WPA2 protocol. KRACK attack exploits the 4-way handshake protocol used in the WPA2 cryptographic mechanism when a device such as a smartphone is joining a wireless network. Threat actors can steal victims' data such as login credentials and credit card information when in transmission over WI-FI networks using the KRACK exploit. WPA3 aims to improve cyber security in the networks. Table 1 shows Common Vulnerability and Exposures (CVEs) attacks identified through specific instantiations of KRACK attacks; each CVE ID illustrates a specific WPA2 KRACK vulnerability.

The new announcements are: (i) new security specifications in the WPA3 protocol and (ii) enhancements to WPA2 security specifications.

2.7.1 WPA2 Enhancements

WPA2 enhancements include:

Table 1 CVEs identified through KRACK vulnerabilities

- CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
- CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
- CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Source Vanhoef [67]

1.6.2.1 Improved authentication, configuration requirements, and encryption.
1.6.2.2 Mandatory use of PMF—Protected Management Frames.

- Management frames are used in initiating and terminating Wi-Fi connectivity, management frames transmitted are not encrypted, and its integrity is not verified without PMF
- With PMF, network management traffic integrity is ensured
- Protects against (i) eavesdropping (ii) replay (iii) forging od management action frames
- Protects against DoS/DDoS traffic-based attacks that use de-authentication and disassociation frames to remove a client from a network whereby the client is forced to authenticate again, a tactic used in MiTM attacks such as smartphones.

2.7.2 WPA3 Wi-Fi Security Features

WPA3 augmentations provide:

2.6.3.1 more robust encryption with mandated 256-bit encryption, compliance with CNSA approved cypher suite requirements [68]. The overall effect is to enable 192-bit encryption security for Wi-Fi networks.

2.6.3.2 new OWE (Opportunistic Wireless Encryption) protects against eavesdropping; this replaces open, unencrypted networks and allows hackers to read and modify users' traffic. OWE enables individualised user encryption on public networks such as airports and cafes to defend against brute force or dictionary password attacks on networks relying on password-based authentication.

2.6.3.3 SAE or Simultaneous Authentication of Equals is the new powerful password-based authentication method replacing PSK (Pre-Shared Key) mode, which is susceptible to passive and active brute force attacks. SAE limits the number of guesses an attacker makes – this currently stands at a "rate of 4000,000 possible passwords per second". SAE adds to the user experience, which does not change [68].

2.6.3.4 Device Provisioning Protocol (DPP), a mechanism in provisioning IoT appliances with limited or no user interface in a trusted network.

2.6.3.5 will disallow outdated legacy protocols.

2.7.3 Reported WPA3 Vulnerabilities

Notwithstanding the improved security features in the new WPA3 protocol, it is not perfect; recently, some vulnerabilities have been reported:

- Denial of Service/MiTM attack
  - Fragmentation and Aggregation attack

- Downgrading Attack
  - Exploits backward compatibility
  - Exploits dragonfly handshake
- Side-Channel Attacks
  - Timing-based
  - Cache-based

3 Methodologies and Frameworks

Due to the increase in cyberattacks and the requirement for security appraisal and risk mitigation strategies, a few methodologies and frameworks have been developed to aid in a structured approach to cybersecurity research. These include NIST 800–115, OSSTM, PTES, OWASP, and MSF. The following frameworks are adaptations from research by Shanley [69].

The NIST SP 800–115 document is a technical guide to information security testing and is adaptable for assessment; the guide aids entities/organisations to develop their own information security (IS) methodology. It was developed for US federal government agencies; however, it is freely available for use by the private sector [70]. Unlike OSSTMM, NIST SP 800–115 does not focus on penetration testing alone but as part of a general process that focuses on the identification of vulnerabilities through repeatable, detailed planning and execution assessments, followed by conducting analysis. Like OSSTMM, NIST SP 800–115 does not suggest tools for cybersecurity tests, although it lists some tools that can be used, and assumes that the security professional has the requisite skills and knowledge to conduct penetration tests.

OSSTM is a security approach utilised in evaluating operational security and analysis. It is an open-source license and an audit methodology designed to be a "consistent and repeatable measurement of security at the operational level" developed by ISECOM [71]. Tests are partitioned into five channels: these channels test (i) data/information controls, (ii) mobile devices, wireless devices, and physical security access controls, (iii) human interactions and personal security awareness levels, (iv) social engineering and fraud control levels (v) telecommunications and computer networks, (vi) physical security access, and (vii) buildings and perimeters [72]. OSSTMM is for penetration testing to satisfy regulatory requirements [73]. OSSTMM recommends best practices, guidelines, and trust metrics for assessing risks and attack surfaces, it does not recommend what tools to use because it assumes that security professionals will have adequate knowledge of techniques and tools to perform the tasks in the modules [71].

Penetration Testing Execution Standard (PTES) is a penetration testing standard providing guidelines for the entire scope of pen testing activities in seven main sections covering (i) "pre-engagement interactions, (ii) intelligence gathering,

(iii) threat modelling, (iv) vulnerability assessment, (V) exploitation, (vi) post-exploitation, and (vii) reporting" [74]. Faircloth [75] suggests that pen testing of wireless networks includes the same methodologies used in testing individual systems. Like the Open Web Application Security Project, OWASP, PTES is a community standard, which aims to improve web applications via the provision of tools, guidelines, and reports [76]. PTES does not give technical guidelines on the process of conducting a pen test. Instead, the process is described at a conceptual level. The PTES standard has technical guidelines which include specifications of specific tools and instructions on how to use them [75]. Like OSSTM, PTES assumes that the security professional will have some knowledge of techniques and tools of pen-testing. However, unlike OSSTM and NIST SP 800–115, PTES attempts to remedy the shortcomings by providing methods, guidelines, tools, and techniques in a single document.

The Open Web Application Security Project (OWASP) Foundation (OWASP n.d.) is an international technical not-for-profit organisation aiming to improve security in software focusing on research, testing, tools and resources, methodologies, education, and training. OWASO research updates information on the latest prevalent vulnerabilities for web applications [77]. The OWASP Testing Guide or OTG is a framework for web applications, software development security, web application security testing methodology, which explains "how to test for evidence of vulnerabilities within the application due to deficiencies with identified security controls", and reporting (OWASP n.d.). The OTG offers a web application testing methodology more focused on security relating to the software development stages instead of identifying vulnerabilities after the software is developed and released to the public. Testing includes white box and black box testing. The OTG is divided into three main sections (i) the OWASP testing framework, (ii) web application security testing introduction and objectives and (iii) reporting, with each section having further detailed sub-divisions. The Application Threat Modelling is provided by the OWASP guide, which is used in application testing security flaws during the design of the application (OWASP1 n.d.). OWASP WebGoat is an insecure J2EE application developed to educate pen testers on web application security [78]. OTG is mainly suited for web applications only. Unlike OSSTMM, OTG has a strong focus on the security of web applications during the Software Development Life Cycle (SDLC) with recommended tools for the security professional. The OWASP To 10 is a security risk awareness document and a de facto industry application security standard. Furthermore, in testing application technical security controls, the OWASO's ASVS or Application Security Verification Standard is the standard applied (OWASP2 n.d.).

Metasploit Framework (MSF) is the world-leading pent testing solution; it is a modular penetration testing platform that enables testers to "write, test, and execute exploit code" written in Ruby programming language. Metasploit can be run as a stand-alone or from Kali Linus. MSF is a multitude of tools providing the environs for pen-testing and vulnerabilities development. It consists of multiple tools for enumerating networks, investigating security vulnerabilities, attack executions, and detecting evasion (Rapid7 n.d.). Metasploit was initially developed in 2003 as an open-source

license by HD More. It was acquired in 2009 by Rapid7 company providing vulnerability management solutions, and it oversees development and funding [79]. The elements of MSF that can be leveraged are the virtual or isolated working environment, MSF ability to launch exploits, its database, and the Meterpreter payload. The exploit database is a repository storing all attacks that MSF can launch. Once an exploit is selected and brought to the foreground, it can be customised and then launched, the attack result is displaced when an attack is completed.

Metasploit Framework is run manually in the command-line for developers and security researchers. It is used extensively in pen testing with exploits of more than 1650 and with features such as import of network scan. In contrast, MSF Pro is a commercial version with advanced features such as a web interface, automation, integration via remote APIs, network discovery, and website application evaluations for OWASP vulnerabilities—and much more (Rapid71 n.d.).

The primary modules in MSF are stored under directory: /usr/share/metasploit-framework/modules/[80]:

(a) Exploit—modules that use payloads
(b) Auxiliary—modules include port scanners, sniffers, fuzzers, etc.
(c) Payloads—consists of code that runs remotely
(d) Encoders—ensure that payloads make it to the destination intact
(e) Nops—keeps payload size consistent across exploit attempts.

Armitage is a Java-based GUI for MSF and is accessible by multiple parties for collaboration within a pen testing team [81]. Unlike NIST 800–115, OSSTMM, PTES, and OWASP, MSF provides a suite of tools to provide practical pen testing solutions for which security professionals can take advantage.

The main advantage of MSF is its modularity that allows combinations of exploits with any payload; this acts as a motivation for pen testers and exploits coders. A significant disadvantage and limitation of MSF are that most of the exploit in the MSF system is Windows platform-based, probably because many applications have been developed for the Windows operating system, which is prevalent globally.

Kali Linux framework is a leading open-source and advanced penetration testing software; it is used for advanced information security tasks, ethical hacking, uncovering vulnerabilities, assessing network security, reverse engineering, and computer forensics; it is Debian-based Linux distribution (Kali.org n.d.). Penetration testing can be defined as "the operational process of analysing or evaluating the security of a computer system or network" (Arkin et al. 2005, cited in [82]. Kali contains over 600 tools and is used by ethical hackers to test their security skills. This includes the Aircrack-ng suite of tools used for demonstrating attack scenarios in this project. The pen testing conducted throughout this project is termed ethical or white-hat hacking; this is legal [83].

3.1 Research Design

The research design will attempt to answer the research questions and be presented in three phases. Securing communications (i.e., data) is critical in WLANs as data is communicated through the air medium.

Phase 1 will review the downgrade of WPA3 to WPA 2, leading to DoS/DDoS and MiTM attacks.

Phase 2 will demonstrate a DoS/DDoS attack on a private smartphone through Aircrack-ng; this is a penetration testing technique. Bacudio et al. [84] contend that pen testing is a sequence of events conducted to "identify and exploit security vulnerabilities", this confirms the ineffectiveness and effectiveness of implemented measures regarding security.

Phase 3 will extend upon Phase 2 and demonstrate an Ettercap-based MiTM attack via ARP Poisoning; this is also pen-testing.

The materials utilised in this project consists of the following:

- MacBook Pro (Retina, 13-inch)
  - Processor—2.6 GHz Dual-Core Intel Core i5
  - Memory—8 GB 1600 MHz DDR3
- Wireless Adapter Card: ALFA NETWORK (AWUS036NHA)
  - Monitor/injection mode support
  - 802.11b/g/n protocols support
  - Supports 150Mbps 2.4 GHz wireless access
- Wireless router
- Oracle VM VirtualBox (n.d.) (virtual environment).

3.2 Data Analysis

Data analysis will comprise interpreting the outcome obtained from the pen testing outlined in the research design, how this relates to WPA3 newly discovered vulnerabilities and degradation to WPA2, and the consequences thereof.

A few researchers, such as Vanhoef and Ronen [85], have performed systematic analysis into the recently released and enhanced security in the WPA3 protocol. The researchers found severe vulnerabilities, including downgrade, denial of service, MiTM and side-channel attacks on WPA3.

3.3 MiTM Attack Demonstrations

3.3.1 Phase 1: Review of Dragonfly Degradation and "Dragonblood" Exploit

Recent research by Vanhoef and Ronen [66] on the newly launched WPA3 protocol demonstrated security vulnerabilities, which the researchers termed "Dragonblood". The Dragonblood vulnerability directly correlates with the ability to degrade the Dragonfly handshake mechanism of WPA3 to WPA2 and subsequent MiTM attacks. However, the WPA3 Dragonblood vulnerability does not form part of the demonstrations in this project because this was not part of the research proposal. Furthermore, time constraints and availability of WPA3 devices and materials would not have been readily available at the onset of this project. Detailed discussions of the Dragonfly mechanism and related Dragonblood exploit are presented in Chap. 4—Data Analysis and Discussions.

3.3.2 Phase 2: DoS/DDoS Attack on WPA2

This practical will capture a WPA2 4-way handshake between an AP and a client (smartphone) using the Aircrack-ng suite of tools in the Kali framework. An attempt will be made to use brute force in cracking or breaching the password; this will be for pen testing purposes.

3.3.3 Staying Anonymous During Pen-Testing: Spoofing MAC Address

During pen-testing, it is paramount to be anonymous; this can be achieved by changing the MAC address, anonymity avoids detection. The MAC or Media, Access Control address, is unique to every device's NIC or Ethernet network interface card; the MAC address is 48 bits long [86]. Prior to performing the attack scenarios, the MAC address is changed, this is also known as "spoofing" the MAC address. The change is not permanent but temporary and exists in RAM only. GNU MAC Changer or Macchanger is a Kali tool used for MAC address manipulation in network interfaces; the MAC address is randomised, as illustrated in Fig. 1 (Kali.org n.d.). When the MacBook is restarted, the original MAC address is restored.

Alternatively, the MacBook Terminal tool and Linux command can be used to spoof the MAC address as follows:

(i) Obtain the MAC address of the machine with the command:

ifconfig or ifconfig en0 | grep ether

(ii) Generate Hexadecimal MAC number—Fig. 2.
(iii) (a) disconnect from wi-fi then connect to wi-fi but not AP/router.

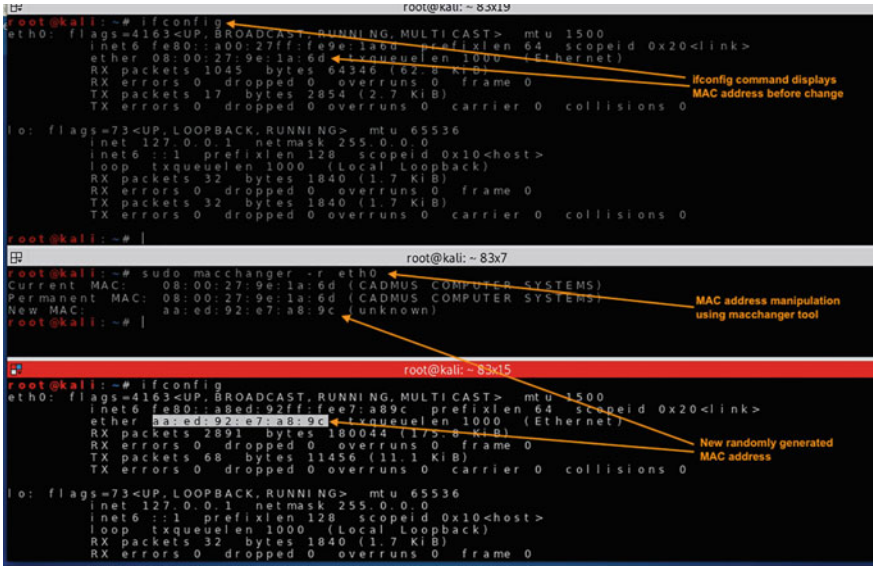

Fig. 1 Changing MAC address with Macchanger Linux command

Fig. 2 An alternative method to generate a random Hexadecimal MAC number

(b) disconnect from VPN.

(iv) Followed by commands:

sudo --login

ifconfig en0 ether 06:28:66:ae:cd:45 ← from new MAC address generated in (ii)

Step 1: Update Kali.

Use the command: *sudo apt update*—Fig. 3.

Then upgrade to the latest Kali version with the command: *sudo apt full-upgrade -y* (Fig. 4).

Fig. 3 Updating Kali in the virtual environment

Fig. 4 Upgrading Kali

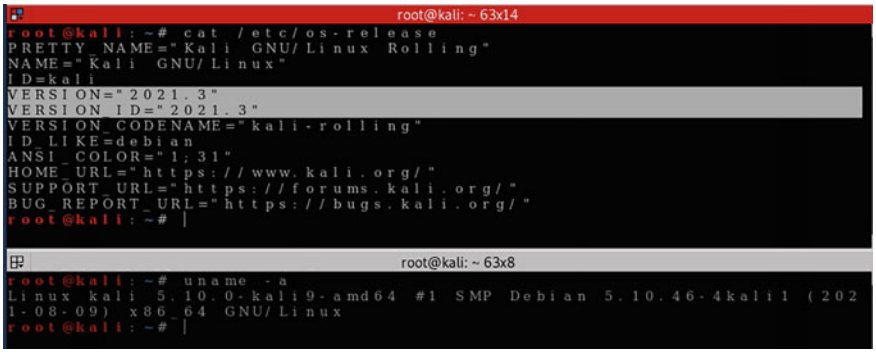

Fig. 5 Kali and Linux versions

Step 2: check for Kali and Linux versions—Fig. 5.
Terminal horizontal split screen shows:

(a) Kali version in use: *cat /etc/os-release.*
(b) Linux version: *uname -a.*

Step 3: the wireless interface details—Fig. 6.

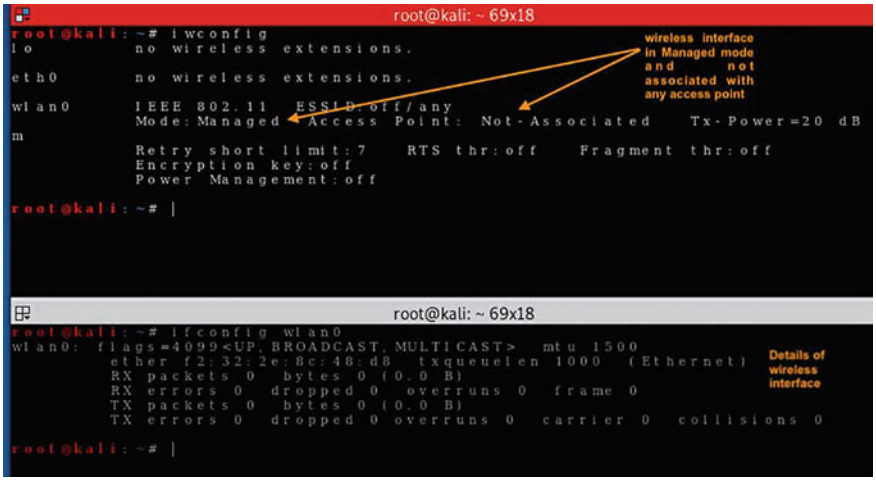

Fig. 6 wireless interface details

Figure 7 screenshot shows the green light of the ALPHA [87] wireless adaptor device, which is switched "on".

Figure 8: Terminal command: *airmon-ng start wlan0*—command puts the wireless interface in "Monitor" mode for the purpose of packet capture from surrounding APs

Step 4: kill processes that might interfere with Monitor mode—Fig. 9

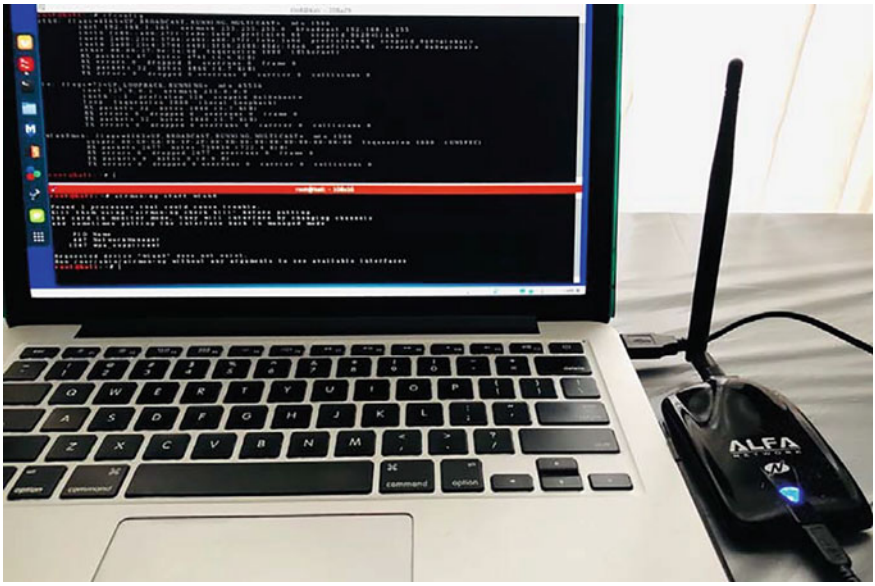

Fig. 7 Wireless adapter WLAN0 set to monitor mode to sniff data packets

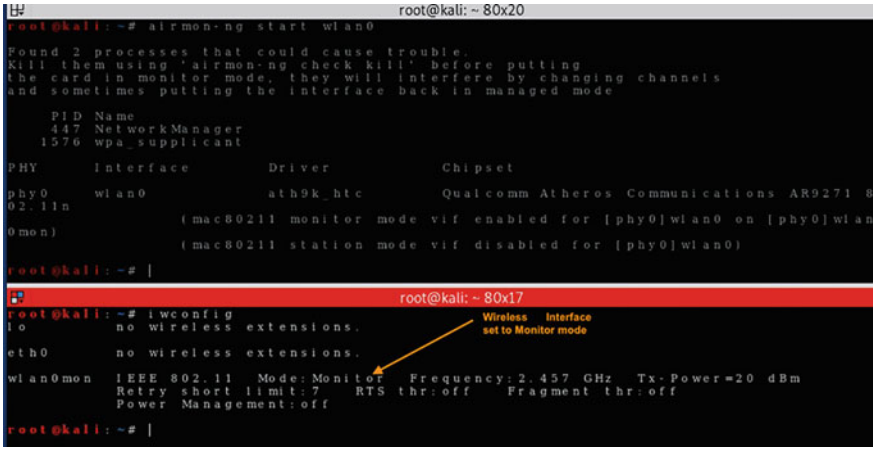

Fig. 8 Wireless interface in monitor mode

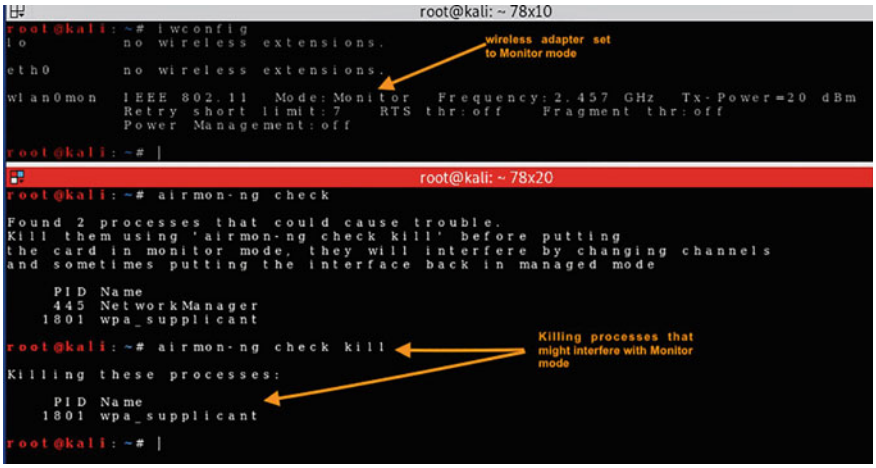

Fig. 9 Processes interfering with monitor mode

Step 5: command *airodump-ng:* capturing/sniffing available networks/APs in the vicinity and grabbing packets using the interface. This process is also called "channel hopping"; by hopping multiple channels to detect APs or routers within range, as shown in Fig. 10.

BSSID is the MAC address of the target network; ESSID is the name of wireless networks within range; PWR is the signal strength; CH is the channel; Beacon is the access point/network broadcasting its presence; ENC is the encryption protocol used by the network, e.g., WPA2; #Data is the number of data packets being sent, and AUTH is the authentication used on the network.

Step 6: targeted sniffing on specific AP of interest (BSSID = 18:82:8C:1D:F4:5B) and writing captured data packets to file named "capture"—Fig. 11.

Command: *airodump-ng -c6 -w capture -d 18:82:8C:1D:F4:5B wlan0mon.*

Step 7: DoS/De-authentication attack on AP and station of interest.

The aim is to detach the station from the AP/router so that in the process of re-association with the AP, the 4-way handshake is captured, as shown in Fig. 12.

Command: *aireplay-ng –deauth 0 -a 1x:82:8x:1D:×4:5B -c 5x:xx:96:Bx:8B:3E wlan0mon.*

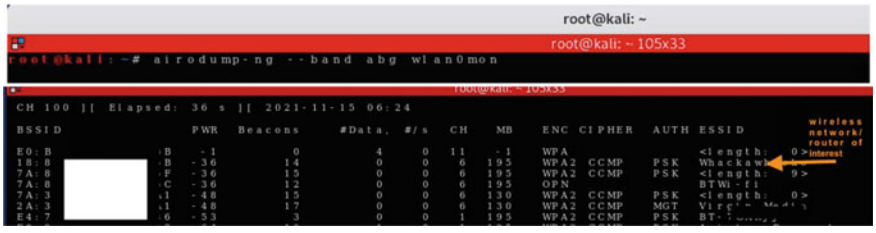

Fig. 10 The screenshot shows AP with details

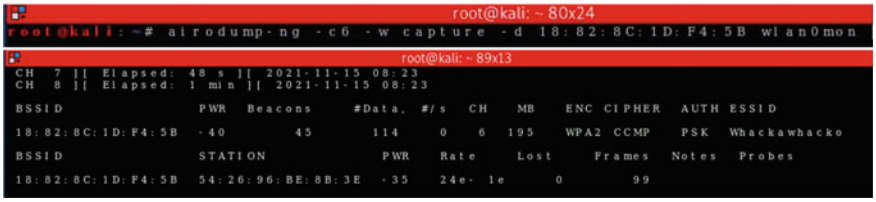

Fig. 11 Packet sniffing on a specified AP and station

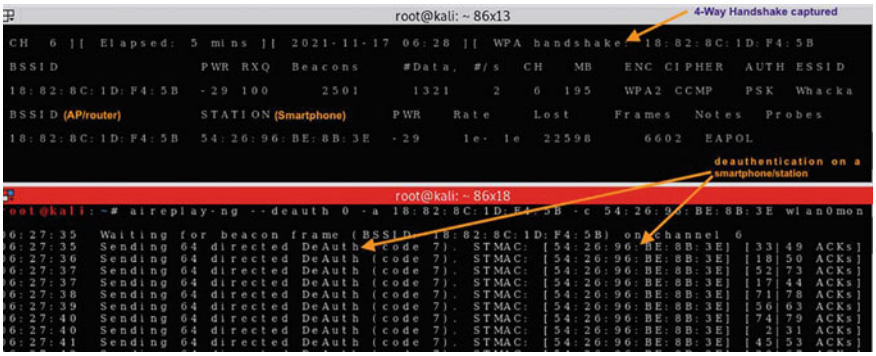

Fig. 12 Deauth attack a station (i.e., smartphone) to capture 4-Way Handshake

Capture file with data—Fig. 13.

Figure 14—stop monitor mode after data capture

A Shell script program simulates a DDoS attack by changing the MAC address and attacking the AP in the program loop (Fig. 15).

Step 8: Start Wireshark analyser to view 4-Way Handshake and other data details.

Step 9: Aircrack-ng—brute force cracking of WPA password (Fig. 16).

Successful cracking of keywords will depend on the password complexity, how comprehensive and extensive the wordlist being used is, and the password not ordinarily found in a dictionary. In this case, the password was not found because it is complex; it is a personalised passphrase comprising of (a) 15 characters long, (b) alphanumeric and (c) special characters.

Fig. 13 Capture file with data

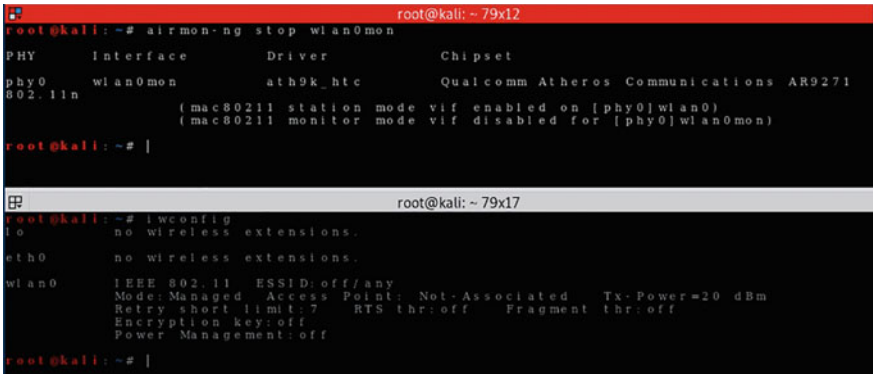

Fig. 14 Stop monitor mode

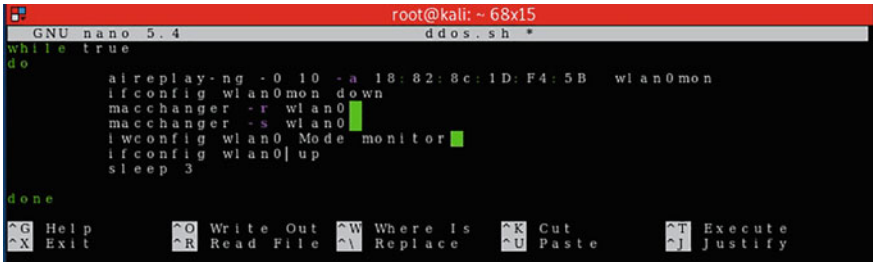

Fig. 15 DDoS shell script program

Fig. 16 Aircrack-ng command to capture password

Figure 17 shows that brute force to crack passwords did not work in this instance.

More advanced and sophisticated tools are available to crack complicated passwords, as shown in Fig. 18. These tools include the GPU Hashcat and Python CUPP tool; both generate brute force attacks. The use of such a sophisticated attack is not within this project's scope.

3.3.4 Phase 3: Ettercap-Based ARP Poisoning MiTM Attack

Ettercap is an open-source tool pre-installed in Kali Linux. In this simulation scenario, address resolution protocol (ARP) poisoning MiTM attack is demonstrated against a Wi-Fi network between a router and a target user, a smartphone. During a regular data transmission over Wi-Fi, messages are routed over the network by associating

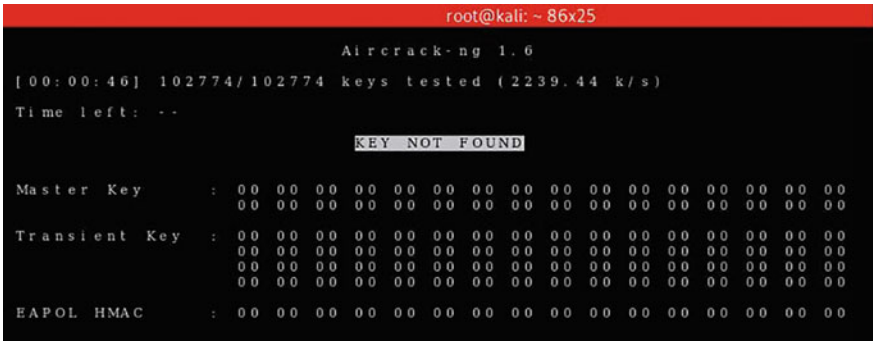

Fig. 17 Password not found in brute force cracking of station/smartphone password

Fig. 18 Strong password

the device MAC address and its IP address; this is done via the ARP. However, this can be "spoofed" to change the data traffic routing whereby messages meant for the target smartphone are transmitted to the hacker instead, allowing the hacker to deny service and man-in-the-middle the smartphone.

Step 1: The Default Gateway (Fig. 19) is determined to be 192.168.1.254 using the command: *netstat -nr.*

St**ep 2**: Enumeration (Fig. 20) to extract machine names and network resources using the command: *nmap -sn.*

The command: *arp-scan -l* can also be used to scan the network for IP addresses with their corresponding MAC address.

Step 3. Ettercap can be run in either command mode or by using the graphical interface. Allow IP forwarding using the command in Fig. 21. Number 1 indicates that ip_forwarding is now enabled.

Step 4. Ettercap MiTM attack in terminal command mode (Fig. 22).

Starting MiTM Ettercap attack manually: *sudo ettercap -T -S -i eth0 -M arp:remote /192.168.1.254// //192.168.1.97//*

Step 5. Ettercap MiTM attack in graphical interface mode (Fig. 23).

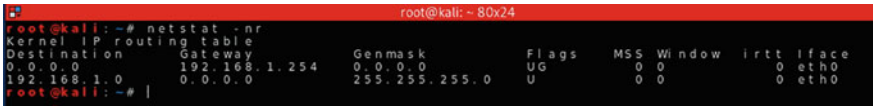

Fig. 19 System default gateway

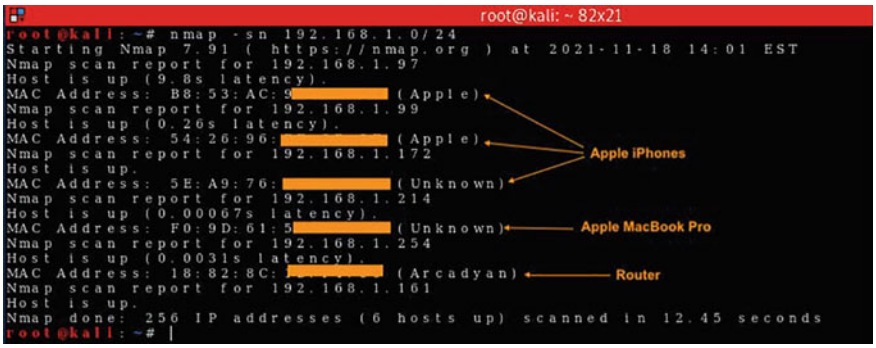

Fig. 20 Enumeration process to extract machine names

Fig. 21 IP forwarding enabled

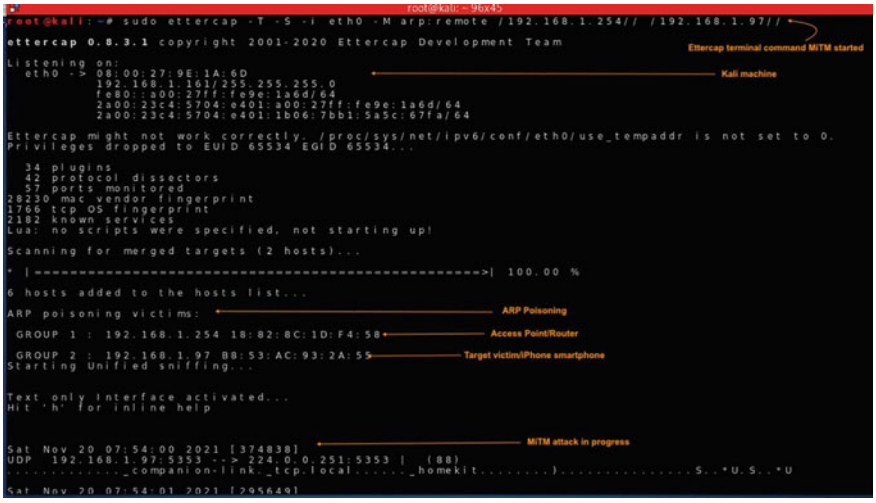

Fig. 22 Ettercap MiTM attack in terminal mode

$$\text{TRGET1} = \text{iPhone (smartphone)}$$
$$\text{TARGET2} = \text{Kali machine}$$

Step 6. MiTM ARP poisoning. in progress—Fig. 24.

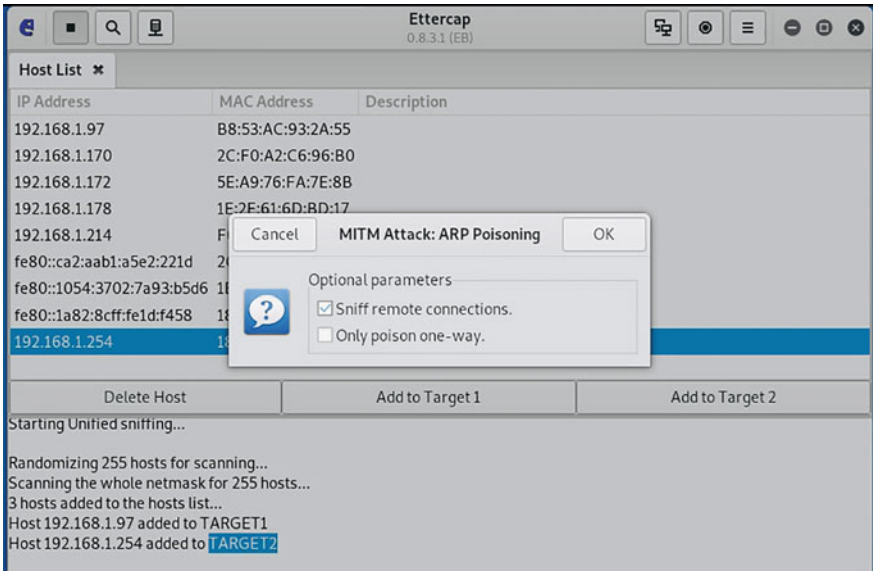

Fig. 23 The selected target for ARP poisoning attack

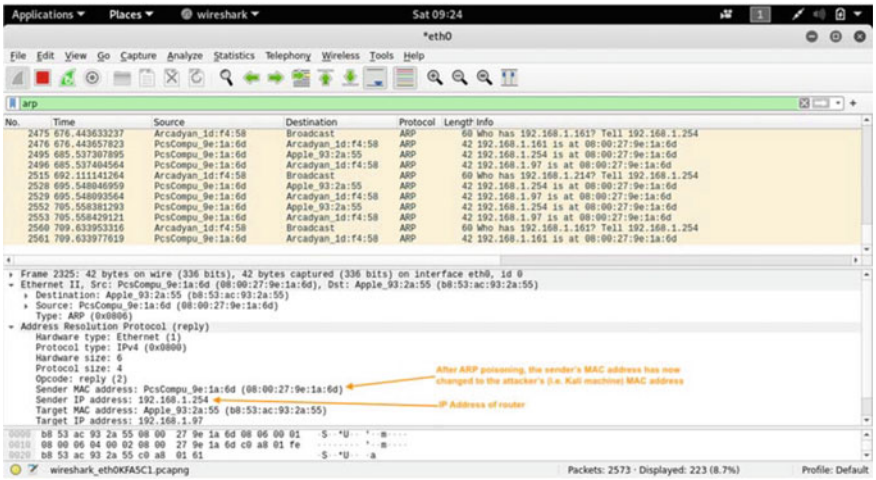

Fig. 24 MiTM ARP poisoning in progress

4 Data Analysis and Discussion

4.1 Explaining the 4-Way Handshake Problem/vulnerability

Understanding the 4-Way Handshake mechanism is critical to the comprehensive appreciation of the WPA3 dragonfly mechanism and the Dragonfly attack, leading to DoS and MiTM attacks. It is commonly known that the 4-way handshake method (as defined in 802.11i) utilised in WPA2-Personal wi-fi networks and applied by all secured Wi-Fi systems in generating a new session key can readily be cracked using a single capture of a data packet as demonstrated in Chap. 3. The weaknesses in the 4-way handshake are demonstratable in the KRACK vulnerability Vanhoef and Piessens [88].

A client such as a smartphone connects to a Wi-Fi network by authentication and association; this is a mutual process. The association stage is a typical connection to Wi-Fi at airports and cafes where no actual authentication occurs; no passwords are needed. This is Open System and Null authentication allowing all clients to authenticate without a password (Wireless [89].

The main elements or keys of interest in the 4-Way handshake are MSK (Master Session Key), PMK (Pairwise Master Key); GMK (Group Master Key); PTK (Pairwise Transit Key); GTK (Group Temporal Key); ANonce, SNonce; and MIC. The actual authentication is conducted during the 4-way handshake and is predicated on the shared secret PMK or Pairwise Master Key. The PMK resides in the client now called the supplicant, and APs now called the authenticator during the handshake. In a personal network, the Pairwise Master Key is generated from a pre-shared password, while for an enterprise, the PMK is generated using 802.1 × authentication. The PTK is generated by combining the PMK, MAC address of the authenticator and supplicant, plus the ANonce (Authenticator Nonce), and SNonce (Supplicant nonce)(Vanhoef and [88].

PTK can be derived as:

$$\text{PTK} = \left(\text{PMK} + \text{MAC}_{(\text{authenticator})} + \text{MAC}_{(\text{supplicant})} + \text{SNonce} + \text{ANonce}\right)$$

When generated, the PTK is divided into three, KCK (Key Confirmation Key), KEK (Key Encryption Key), and TK (Temporal Key). KEK and KCK protect handshake messages, and the TK is utilised in protecting regular data-frames. When WPA2 is used, the 4-way handshake transmits the GTK to the supplicant [88].

In level one, the MSK is generated through 802.1 × and EPA-TLS encryption.

In level two, GMK and PMK keys are generated from the MSK, and PTK and GMK keys are generated from the PMK.

Level three keys are used for data encryption.

After the initial authentication and association, security validation and the 4-way handshake process commence where messages exchanges occur over EAPoL (Extensible Authentication Protocol over LAN).

Message 1 (Fig. 25): The AP sends an EAPOL message containing Anonce, a randomly generated number, to the station to generate the PTK.

Message 2 (Fig. 26): After the creation of the PTK by the station, the station sends out SNonce required by the AP to generate its own PTK for unicast traffic encryption.

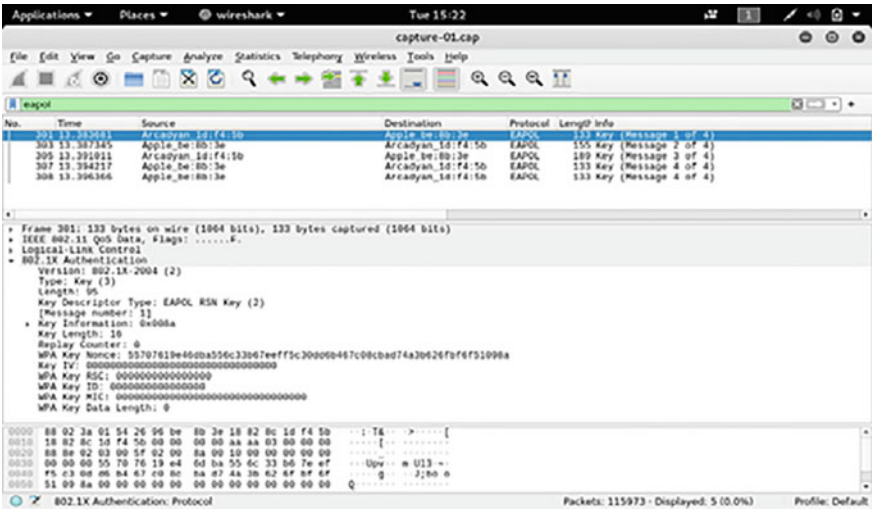

Fig. 25 Wireshark view of message 1 details

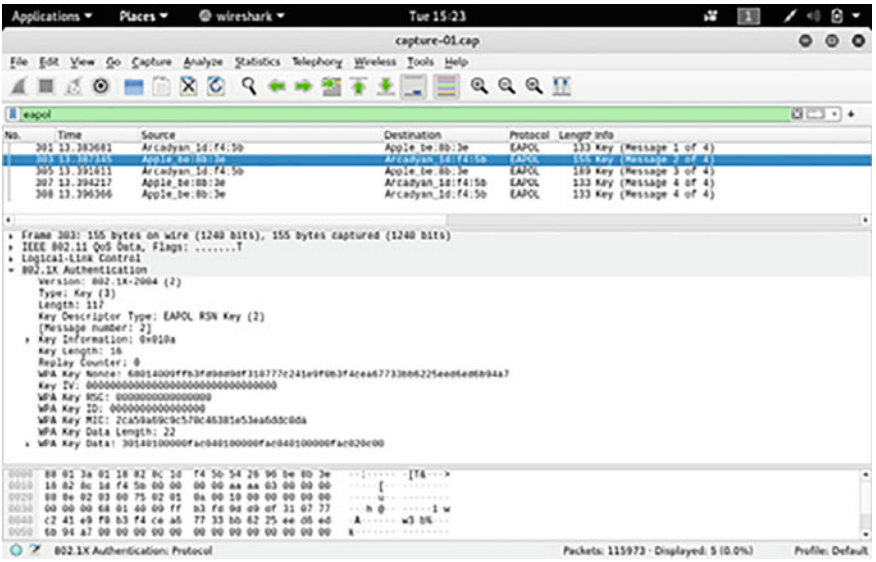

Fig. 26 Wireshark view of message 2 details

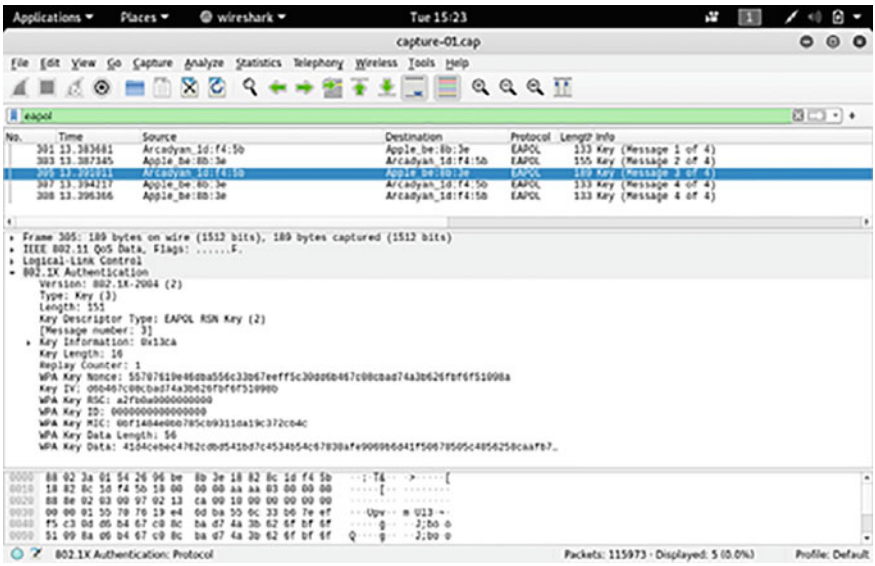

Fig. 27 Wireshark view of message 3 details

In the process, the station sends an EAPOL message containing the message integrity check (MIC) to ensure the AP can check if the message is modified or corrupted.

Message 3 (Fig. 27): AP sends a message to the station containing the GTK.

Message 4 (Fig. 28): Station sends a fourth and final message to AP confirming the installation of keys.

Upon successfully completing the 4-way handshake, the virtual control port is opened to allow the flow of encrypted data, unicast data is encrypted with PTK, and multicast data is encrypted using the GTK.

However, messages can be dropped or lost in transition; the authenticator (AP) retransmits message number 3 if the appropriate acknowledgement response is not received. Potentially, the supplicant may get message number 3 multiple times. Upon receiving message number 3 again, the same session key is reinstalled, thereby resetting the nonce number (the incremental transmit packet number) and the received replay counter used by the data-confidentiality protocol. A hacker can force resets of the nonce by "collecting and replaying retransmissions of message 3". Hence, the protocol in the data confidentiality is violated by forcing nonce reuse in this way. For instance, packets are re-playable, can be decrypted, and or forged [67].

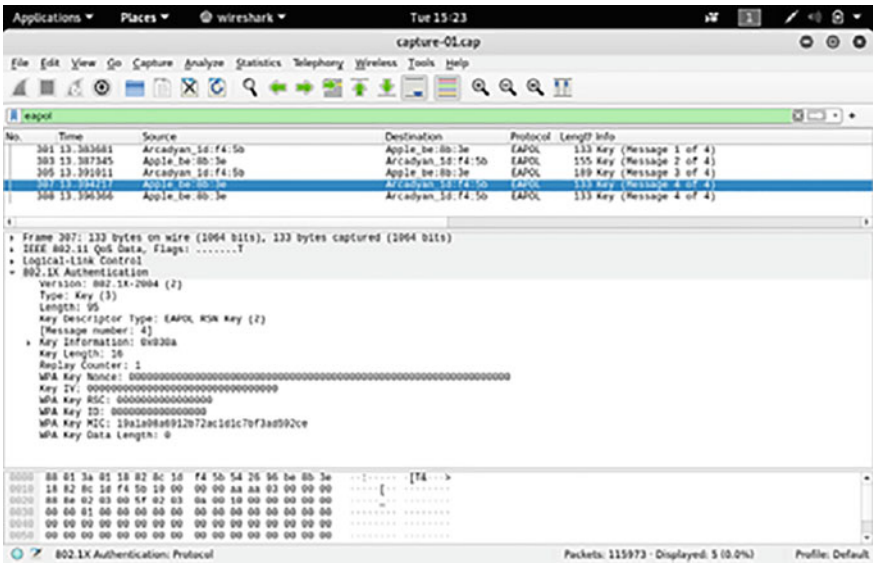

Fig. 28 Wireshark view of message 4 details

4.2 WPA3 Dragonfly Handshake and the Dragonblood Vulnerability

The Dragonfly handshake mechanism and WPA3 design flaws, and the Dragonblood attack are documented by Vanhoef and Ronen [66], the researchers who discovered the vulnerabilities. A complete account of the Dragonfly mechanism and Dragonblood attack is not within the scope of the project proposal. However, this section presents a brief synopsis taken from the research paper by Vanhoef and Ronen [66].

The improved WPA3 Dragonfly-Handshake is intended to make it extremely difficult for hackers to breach the 4-way handshake resistance against offline brute-force dictionary attack; the introduction of WPA3 perfect forward secrecy aids in preventing hackers from decrypting previous traffic following a key breach and thereby making use of Zero-knowledge proofs. The WPA3 vulnerabilities fall into two categories: (i) downgrade attacks against WPA3 enabled devices and (ii) weaknesses in the SAE (Simultaneous Authentication Equals) handshake, also known as the Dragonfly handshake. The adoption of the SAE in WPA3 allows for transition mode connections and compatibility with older devices using WPA2. In this situation, an adversary can modify beacons, making the client think the AP is supporting WPA2 protocol only. By using known WPA2 security attacks like PMKID and KRACK, the attacker can recover the network password. In essence, the hacker forces the device with WPA3 to use WPA2, which negates the KRACK and PMKID countermeasures. This mode of attack is termed the downgrade attack. By this point, the hacker can

adequately capture data to carry out a dictionary attack even though the downgrade attack is detected by the WPA2 4-way handshake.

Further to the SAE compatibility downgrade attacks, another attack against the Dragonfly handshake worth mentioning is the Dragonfly password encoding mechanism side-channel attacks known as the hash-to-curve operation. The hash-to-curve operation has a high overhead, which allows a hacker to exploit the high overhead. This is done by impersonating a client to "impersonate a user and transmit a commit frame, and to deliberately delay the response speed at the access point with subsequent attacks to perform a DOS attack ". The Dragonblood attack is currently the most critical vulnerability in the recently released WPA3 security protocol and requires immediate correction before WPA3 enabled devices become widely available for use.

4.3 Zero-Day Attack

The recently announced Dragonblood attack can be termed a zero-day attack because it is a security vulnerability on the new WPA3 protocol; it will continue to be abused until the vendor patches the exploit [90]. The Window of Vulnerability or WOV is the timeframe the vulnerability is initially made public to the time the security patch is finalised or when the exploitations reduce to insignificance. t_0 equals the time when the first client gets a patch p, t_1 equals the time the last client gets patch p. Given that Δ_{attack} is the time the hacker requires to reverse engineer the patch p and make it a viable exploit, then WOV starts at $t_{0+}\,\Delta_{attack}$ and finishes at t_1 [91].

4.4 Data Analysis and Data Visualization

Data visualisation is visually representing information that communicates information concisely and clearly without being confusing and cluttered; it is a compelling visual to enhance understanding of the phenomenon [92]. Using graphs and charts to illustrate cyberattack patterns and activities instead of reading through several logs, reports and spreadsheets enable the security administrator to pinpoint the severity and scope of cyberattacks expeditiously. Additionally, using DV saves time analysing extensive data and applying faster action [93]. However, using data visualisation highlights the requirement in more robust data governance and data management and the necessity for clear boundaries and data dissemination or transmission, monitoring, and tracking—among individuals with the ability to alter data origination and "write back to the system record through their visual discovery activities" [94]. Practices and privacy attitudes of organisations in the collection of data carry ramifications for data confidentiality, availability, and integrity [95].

The pen testing simulations conducted for this project and the data produced are applicable to the financial services sector. For financial services entities, the CBEST

(Bank of England Penetration Testing Framework) mechanism by The [96] is the primary means to evaluate security safeguards in the financial sector by employing sophisticated threat intelligence coupled with achievable pen-testing simulations. The Annual Cybersecurity Report by Bulletproof [97] suggests that DoS or DDoS attack could cost a lar ge business upwards of $2 million and $120,000 for a small-medium enterprise.

4.5 Comparative Data Analysis Between MiTM DoS and ARP Poisoning Attacks

Data are analysed using the Wireshark Statistics tools. Figure 29 screenshot gives the DoS scenario capture file data like the file name, length, Hash properties and encapsulation; capture suration (start and end time); hardware; interface type and packet size limit; and capture statistics.

The graph in Fig. 30 (obtained through Wireshark interface, Statistics I/O Graphics function) shows typical DoS traffic generated; the peaks in the graph indicate bursts of traffic in 100 ms time intervals. These were created in Phase 2 practical by generating denial of service attacks in the Kali Linux platform. In this case, numerous significant traffic bursts were generated, indicating the many deauthentication attacks during the

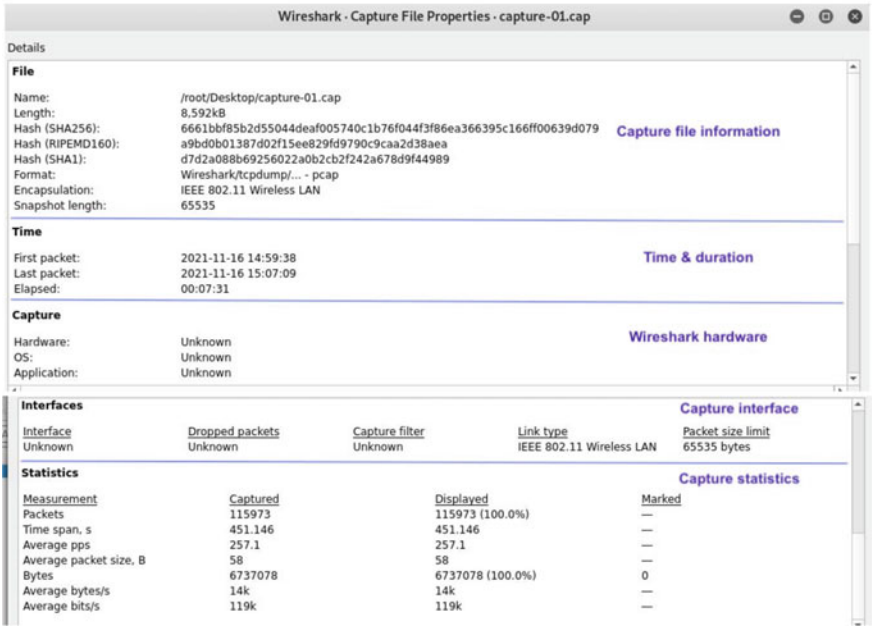

Fig. 29 DoS capture file properties

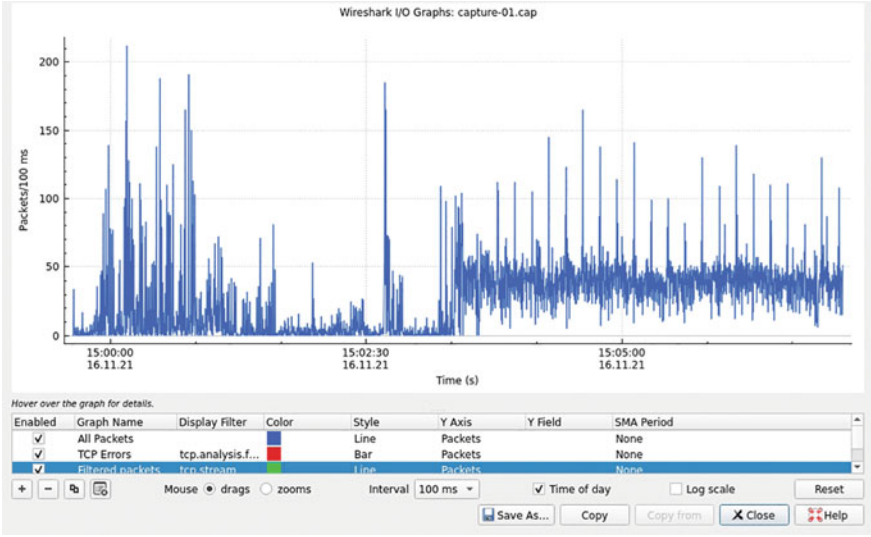

Fig. 30 Wireshark input/output traffic graph during DoS attack

DoS scenario. Cybersecurity professionals can use Wireshark statistics to identify traffic bursts when an attack occurs more quickly. Figure 31 is the shark input/output traffic graph during MiTM ARP poisoning.

Figure 32 is a Wireshark analyser showing the 4-Way Handshake. EAPoL filter is applied to obtain the 4-way handshakes.

Figure 33 is the hierarchy or tree of all captured packets, with each row showing statistical values for each protocol. The first column is the protocol's name, IEEE 802.11 wireless LAN protocol; the second column is %age of protocol packets. The third column is the protocol's total number of packets captured, which in this scenario is 115,973.

Figure 34 is a screenshot indicating a de-authentication packet number 55093 and the relative peak of the graph.

Figure 35 screenshot is the deauthentication details of specific packet number 55093. It gives details such as the wireless LAN protocol (802.11), BSS ID of the AP, and the Apple [98, 99] iPhone under deauthentication attack.

4.6 Security in 802.11ax and 802.11be; 5G and 6G

To what extent the recently released Wi-Fi 6 (and 6E) certification can become a game-changer as a countermeasure against Wi-Fi-based MiTM cyberattacks is too early to determine. Moreover, improvements in Wi-Fi 7 or 802.11be and the standardisation process are already being considered for release in 2024. The new features

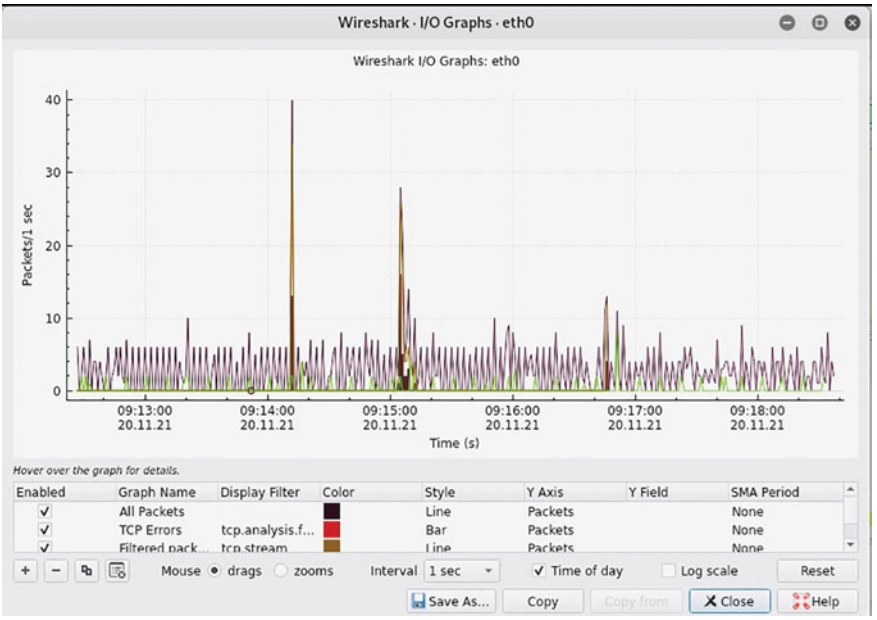

Fig. 31 Wireshark input/output traffic graph during MiTM ARP poisoning

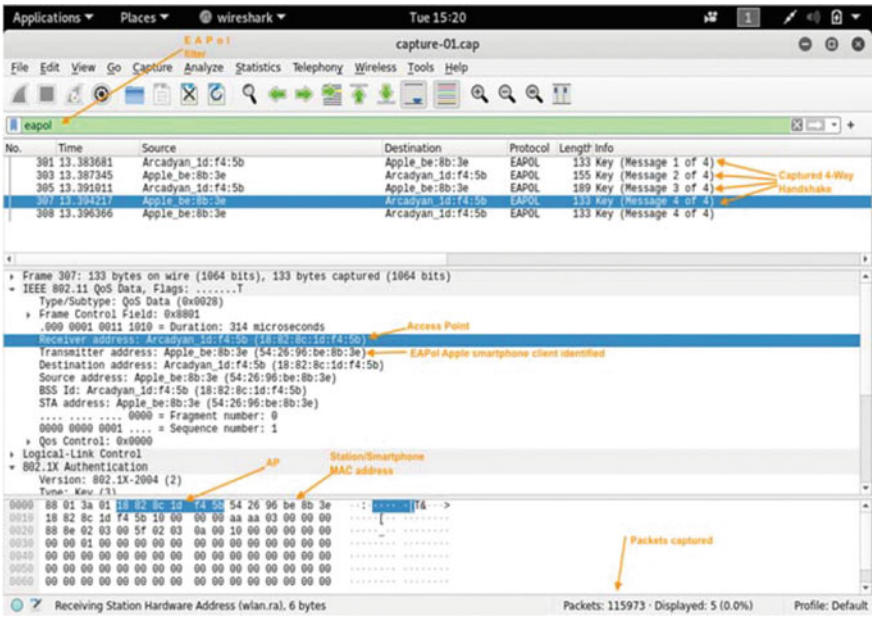

Fig. 32. 4-Way Handshake in Wireshark analyser

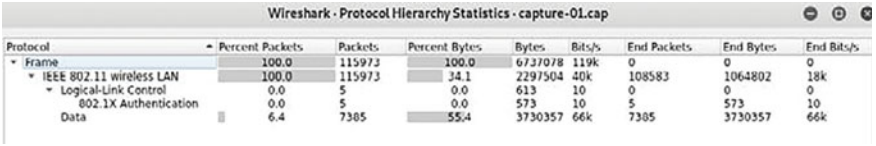

Fig. 33 Protocol hierarchy of captured packets

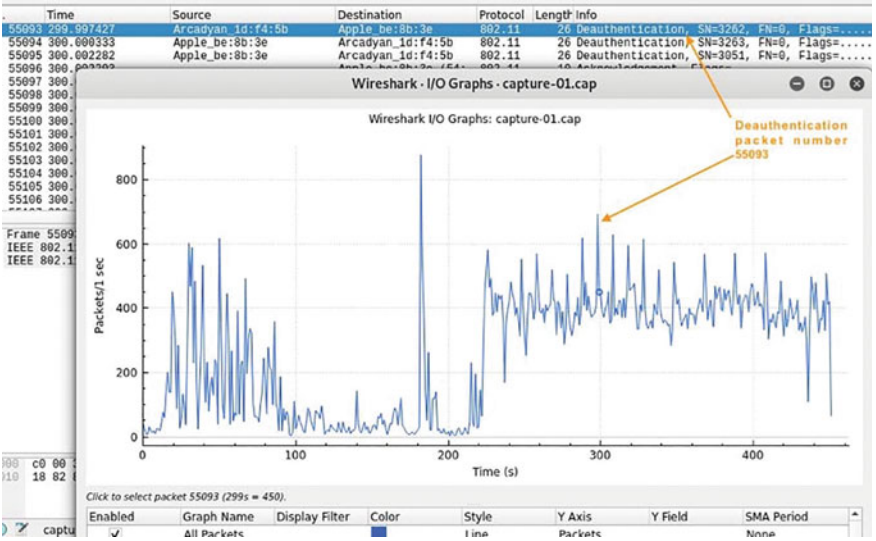

Fig. 34 Specific deauthentication packet

in Wi-Fi 7 aim to revolutionise technologies in areas such as Interactive Robotics, Virtual Reality, and Automated Vehicles. Gulasekaran and Sankaran [100] contend that Wi-Fi 6 principal objective is improved efficiency in the network with multiple access points, different traffic loads and capacity enhancements, and multiple clients. Wi-Fi 6E is the terminology and not a standard, it refers to the spectrum expansion and designation for the use of Wi-Fi 6 into the radio frequency of the 6 GHz band (Cisco, n.d.). The recently released Wi-Fi 6 and 6E will soon be surpassed by Wi-Fi 7, which is expected to deliver Extremely High Throughput (EHT) and is projected for release in 2014 according to the developmental timelines. Wi-Fi 7 aims to improve data speeds of at a minimum of 30 Gb/s per access point, about 4X faster than Wi-Fi 6, efficient operations in and backward compatibility with 2.4, 5, and 6 GHz devices. MIMO or Multi-Input, Multi-Output technology is the ability of the network to multi-task by sending data to many devices simultaneously instead of one at a time. Wi-Fi 7 improvements will include MIMO enhancements by doubling the maximum number of supported SU-MIMO (single-user MIMO) and MU-MIMO (multi-user MIMO) spatial streams per station to 16 [101].

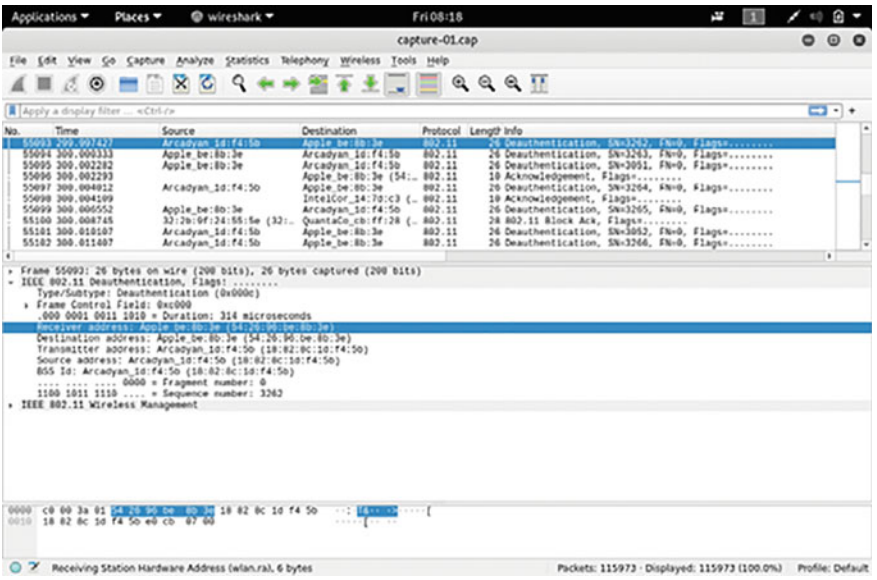

Fig. 35 Deauthentication details of packet number 55093

According to Wang et al. [102], the significant improvement of 5G technology is the facilitation of connecting the rising and challenging numbers of devices like smartphones and IoT connecting to networks. 5G technology will accommodate simultaneous "high-quality services", making networks more dynamic. 6G networks are intended to give low latency (6G radio latency is 0.1 ms or 10% of 5G), higher reliability, efficient and secure transmission services, and will have "AI-empowered" capabilities. Though 5G systems are compliant with IoT, 6G networks will work with IoE and be decentralised with the capacity to make intelligent decisions. However, the large quantum of devices and services can overload and overwhelm networks that can lead to increased vulnerabilities and more cyberattacks such as DoS and MiTM. There are security and privacy issues such as access control, authentication, encryption, and malicious behaviour concerns due to many diverse application scenarios and business types using 5G and 6G networks. Blockchain and machine learning technologies could assist in the prediction of incoming cyberattacks [102].

Security is a critical component of wireless networks, whether in Wi-fi 6 or 7, as data is transmitted in the airwaves. Nonetheless, the prevention of unauthorised data access and tampering will be dependent upon the data confidentiality and integrity mechanisms of the Wi-Fi Protected Access 3 protocol and further future security enhancements.

4.7 Wi-Fi and Human Health

Wi-Fi network traffic has grown over recent years and is projected to increase further, coupled with a considerable increase in the number of smartphones and other devices with Wi-Fi installed accessing the Internet [103]. Whereas only 9% of 55 to 64 years olds used a smartphone in 2012, this rose to 87% by 2020 [104]. Among older adults of 64 + years, smartphones are used for varied social and non-social reasons, and research done in this area suggests that it contributes towards self-control, emotional gain, social influence, self-control, loneliness, and fear of missing out [105]. However, smartphones have been "associated with excessive dependency" and "nomophobia", which is fearing the inability to avail oneself of their smartphone. For many smartphone users, the device has become an extension of the individual and may have become an "addiction" to the smartphone [106].

However, what is generally not discussed is the potential effects of Wi-Fi on human health, although extensive literature exists on the subject. This section does not form part of this original research proposal; however, it is worth discussing, albeit briefly. Research by Pall [107] contends that as Wi-Fi use becomes more and more common, so does the increased exposure to potential Wi-Fi health effects, considering that many individuals could be unsheltered to Wi-Fi fields for 4 to 8 + hours daily. The researcher argues that multiple peer-reviewed scientific research has demonstrated that Wi-Fi engenders sperm/testicular damage, neuropsychiatric effects like electroencephalographic (EEG) changes, cellular DNA damage, oxidative stress, apoptosis, endocrine changes, and calcium overload in human beings as well as in animals. Additionally, the author argues that each of the effects may also be generated by other microwave frequencies or EMF (electromagnetic frequencies). The author suggests that the use of aluminium mesh wire will aid in reflecting the impact of EMFs and, hence lowering the possible effects.

5 Conclusion and Future Work

With the ever-increasing growth in the use of Wi-Fi technology in volume and frequency, especially among smartphone users, so is the urgent need to mitigate risks against cyberattacks involving users' PII and financial data breaches. DoS and MiTM cyberattacks against data in transmission through the air medium cannot be made 100% safe, "these risks cannot be removed entirely" [108]. This paper started with a review of existing literature encompassing a brief history of the evolution of financial institutions, the definition of and what MiTM entails, and the security vulnerabilities and attacks on mobile banking and trading apps. This is followed by cyberattack vectors, methods and technics employed during the COVID-19 pandemic and their successes. Blockchain and self-sovereign identity systems are the novel technologies being employed to address cyberattacks; these are discussed. However, SSI technology is still in its infancy without a universally agreed standard framework or

protocol. The new security features in the Wi-Fi WPA3 protocol and the recently discovered Dragonblood vulnerability is extensively reviewed. The Dragonblood attack is currently the most critical vulnerability in the WPA3 security protocol requiring immediate attention and correction before WPA3 enabled devices become widely available for use.

Research methodologies and philosophical underpinnings are discussed, followed by evaluating the different and popular frameworks available in cybersecurity domain research. The paper posits the Kali Linux in a virtual environment as the most favourable framework to utilise for this project. DoS and MiTM ARP poisoning attack scenarios are demonstrated against iPhone smartphone clients and a British Telecom router (access point) using Aircrack-ng suite of tools and Ettercap software within Kali. The resulting DoS and MiTM attack data are captured in a capture file and used for data analysis. Wireshark Statistics tool combined with cybersecurity data visualisation is utilised as the method to view data captured during attack simulations. Data visualisations provide security experts with the ability to quickly identify malicious threat activity, anomalies, and business threat intelligence. However, data visualisation also has implications for data governance and data management. The new sixth-generation or Wi-Fi 6 (and 6E) based on 802.11ax standard could be a game-changer as a countermeasure against MiTM cyberattacks; this is discussed.

In terms of future work will be beneficial to replicate Dragonblood pen testing attacks on WPA3 systems as discovered by researchers Vanhoef, Piessens and Ronen. This will help ascertain to what extent such attacks can be carried out. More importantly, such future work will aid in establishing the degree of complexity an attacker requires to bypass the enhanced security features in WPA3 and then perform a downgrade attack leading to DoS and MiTM exploits on smartphones. A successful attack on the new WPA3 protocol requiring a high level of sophisticated laboratory setup would imply that WPA3 cannot be easily breached ordinarily by hackers. Therefore, the latest security features in WPA3 are working better than its predecessors, WPA2. Future work will also involve obtaining permission from equity trading platforms (i.e., IG, Interactive Brokers, FinecoBank, and Saxo Markets) for pen-testing smartphone and Wi-Fi 6 DoS and MiTM attack scenarios.

Furthermore, as a critical countermeasure against DOS and MiTM attacks, the implementation and use of data protection protocols like VPN technology in all operating systems and devices using Wi-Fi as the means of communication will exceptionally "provide data confidentiality, integrity, and origin authentication across untrusted networks such as the internet" [109]. All smartphones sold to the public should have VPN software pre-installed in client devices. IPsec (IP Security) and IKE (Internet Key Exchange) VPNs should be incorporated in all systems at the business or organisational level. The adoption of VPNs in conjunction with implementing the new WPA3 and Wi-Fi 6 standards will significantly improve data security

References

1. Khorov E, Levitsky I, Akyildiz IF (2020) Current status and directions of IEE 802.11be, the future Wi-Fi 7. Available online at: https://ieeexplore.ieee.org/document/9090146. [Accessed on: 31st Dec 2021]
2. Chauhan S, Sharma A, Pandey S, Rao KN, Kumar P (2021) IEEE 802.11be: A review on Wi-Fi use case. Available online at: https://ieeexplore.ieee.org/document/9596344. [Accessed on: 29th Nov 2021]
3. Artech House (2021) 'Wi-Fi 6 protocol ad network'—New book release by Artech House. Available online at: https://artechhouse.prowly.com/152110-wi-fi-6-protocol-and-network-new-book-release-by-artech-house. [Accessed on: 22nd Nov 2021]
4. Internet Society (2020) Fact sheet: machine-in-the-middle attacks. Available online at: https://www.internetsociety.org/resources/doc/2020/fact-sheet-machine-in-the-middle-attacks/. [Accessed on: 8th Sept 2021]
5. Conrad E, Misenar S, Feldman J (2014) Chapter 7—Domain 7: operations security. Available online at: https://www.sciencedirect.com/topics/computer-science/session-hijacking. [Accessed on: 8th Sept 2021]
6. Australian Cyber Security Centre (2020) Person-in-the-middle. Available online at: https://www.cyber.gov.au/acsc/view-all-content/glossary/person-middle. [Accessed on: 8th Sept 2021]
7. Choi H, Kwon H, Hur J (2015) A secure OTP algorithm using smartphone application. Available online at: https://ieeexplore.ieee.org/document/7182589. [Accessed on: 29th Sept 2021]
8. Ahmad DRM, Dubrawsky I, Flynn H et al (2002) Session hijacking. Hack proofing your network. Available online at: https://www.sciencedirect.com/topics/computer-science/man-in-the-middle-attack. [Accessed on: 8th Oct 2021]
9. Hilliard AG (2010) Kemet (egypt) historical revision: Implications for cross-cultural evaluation and research in education. Available online at: https://reader.elsevier.com/reader/sd/pii/S0886163389800480?token=ED42893A8B31F4062E6F49A8387994C9AB328CF74C1C52373D896730257ABFE3F7F5F110A4CCA47BD8DAF27324BC7638&originRegion=eu-west-1&originCreation=20211024102646. [Accessed on: 24th Oct 2021]
10. Labate V (2016) Banking in the Roman World. Available online at: https://www.worldhistory.org/article/974/banking-in-the-roman-world/. [Accessed on: 24th Oct 2021]
11. Henry JF (2002) The social origins of money: The case of Egypt. Available online at: https://www.csus.edu/indiv/h/henryjf/PDFS/Egypt.PDF [Accessed on: 24th Oct 2021]
12. Thakor A (2020) Fintech and banking: What do we know? Available online at: https://reader.elsevier.com/reader/sd/pii/S104295731930049X?token=29DD3820FA5696C91B4F5B624E2E6B76CA0311E57B9A71EBF3E38ECC25A6A4078DBBDDAB48B0406850FAE3885608D1E1&originRegion=eu-west-1&originCreation=20211024123857 [Accessed on: 24th Oct 2021]
13. Frame WS, Wall LD, White LJ (2018) Technological change and financial innovations in banking: Some implications for banking. Available online at: https://poseidon01.ssrn.com/delivery.php?ID=936024072000088007124097104085070011037045010029091017099126060018014112005116119102042034085030032003037019022011074028116005112067029071017063124066081006109073068084031076125092004076110106120080012097016104068074003020&EXT=pdf&INDEX=TRUE. [Accessed on: 25th Oct 2021]
14. Bhushan B, Sahoo G, Rai AK (2018) Man-in-the-middle attack in wireless and computer networking—a review. Available online at: https://ieeexplore.ieee.org/document/8344724. [Accessed on: 25th Oct 2021]
15. Malik A, Ahsan AShahadat MMZ, Tsou JC (2019) Understanding man-in-the-middle through a survey of the literature. Available online at: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiljOzTzdb0AhWNGewKHTdaA28QFnoECAIQAQ&url=https%3A%2F%2Fpdfs.semanticscholar.org%

2Fc2c7%2F182b3fce4003e4dff71c0ed85e0a34aaf830.pdf&usg=AOvVaw0rUR5MgqsKmLdBetYaI182. [Accessed on: 9th Dec 2021]
16. Oriyano S-P, Shimonski R (2012) Mobile Attacks. Available online at: https://www.sciencedirect.com/topics/computer-science/man-in-the-middle-attack. [Accessed on: 25th Oct 2021]
17. Su Z, Wang H, Wang H, Shi X (2021) A financial data security sharing solution based on blockchain technology and proxy re-encryption technology. Available online at: https://ieeexplore.ieee.org/document/9332363. [Accessed on 25th Oct 2021]
18. ICO (2018) Guide to the general data protection regulation (GDPR). Available online at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. [Accessed on: 26th Oct 2021]
19. Gov.uk (2018) Data Protection Act 2018. Available online at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted. [Accessed on: 20th Oct 2021]
20. FCA (2018) Effective global regulation in capital markets. Available online at: https://www.fca.org.uk/news/speeches/effective-global-regulation-capital-markets. [Accessed on: 24th Oct 2021]
21. Carnegie (2021) Timeline of cyber incidents involving financial institutions. Available online at: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline [Accessed on 24th Oct 2021]
22. Zheng X, Pan L, Yilmaz E (2017) Security analysis of modern mission-critical android mobile applications. Available online at: https://www.researchgate.net/publication/312428641_Security_analysis_of_modern_mission_critical_android_mobile_applications. [Accessed on 23rd Mar 2021]
23. Ciscomag (2020) Half of mobile banking apps are vulnerable to fraud data theft. Available online at: https://cisomag.eccouncil.org/flaws-in-mobile-banking-apps/. [Accessed on: 19th Sept 2020]
24. Coker J (2020) Widespread security vulnerabilities in mobile banking apps. Available online at: https://www.infosecurity-magazine.com/news/security-vulnerabilities-mobile/. [Accessed on: 30th Mar 2021]
25. IBM (2021) IBM X-Force threat intelligence index. Available online at: https://www.ibm.com/security/data-breach/threat-intelligence. [Accessed on: 13th Sept 2021]
26. Kaspersky (2020) Top 7 mobile security threats in 2020. Available online at: https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store. [Accessed on: 15th Mar 2020]
27. Kaspersky (2021) Kaspersky threat intelligence. Available online at: https://www.kaspersky.com/enterprise-security/threat-intelligence. [Accessed on: 16th Mar 2021]
28. Insights.com (2021) Insights external threat protection (ETP) suite. Available online at: https://intsights.com/products. [16th Mar 2021]
29. OWASP (2016) OWASP mobile top 10. Available online at: https://owasp.org/www-project-mobile-top-10/. [Accessed on: 7th Dec 2021]
30. Garg S, Baliyan N (2021) Comparative analysis of Android and iOS from security viewpoint. Available online at: https://www.sciencedirect.com/science/article/abs/pii/S1574013721000125. [Accessed on: 13th Mar 2021]
31. CVEDetails (2021) The ultimate security vulnerability data source. Available online at: https://www.cvedetails.com [14th Mar 2021]
32. WHO.int (2021) Naming the coronavirus disease (COVID-19) and the virus that causes it. Available online at: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it#:~:text=Official%20names%20have%20been%20announced,%2DCoV%2D2). [Accessed on: 3rd Nov 2021]
33. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X (2021) Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Available online at: https://www.sciencedirect.com/science/article/pii/S0167404821000729. [Accessed on: 12th Oct 2021]

34. Sharma R, Sharma N, Mangla M (2021) An analysis and investigation of infostealers attacks during COVID'19: A case study. Available online at: https://ieeexplore.ieee.org/document/9478163. [Accessed on: 16th Oct 2021]
35. WHO (2021) Coronavirus disease (COVID-19) update. Available online at: https://www.who.int/bangladesh/emergencies/coronavirus-disease-(covid-19)-update#:~:text=On%20this%20website%20you%20can,on%2031%20December%202019. [Accessed on: 12th Oct 2021]
36. Hiscox (2021) The Hiscox cyber readiness report 2021. Available online at: https://www.hiscox.co.uk/cyberreadiness. [Accessed on: 13th Oct 2021]
37. Statista3 (2020) Most prevalent banking trojans worldwide in 2020, by type. Available online at: https://www.statista.com/statistics/1238991/top-banking-trojans-worldwide/. [Accessed on: 12th Oct 2020]
38. Interpol (2020) Interpol report shows alarming rate of cyberattacks during COVID-19. Available online at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. [Accessed on 12th Oct 2021]
39. WHO (2020) Attacks on health care in the context of COVID-19. Available online at: https://www.who.int/news-room/feature-stories/detail/attacks-on-health-care-in-the-context-of-covid-19. [Accessed on: 12th Oct 2021]
40. Deloitte (2021) CBEST: Putting cyber defences to the test. Available online at: https://www2.deloitte.com/uk/en/pages/financial-services/articles/cbest.html. [Accessed on: 15th Mar 2021]
41. Cole E (2013) The changing threat. Available online at: https://www.sciencedirect.com/topics/computer-science/advanced-persistent-threat. [Accessed on: 12th Oct 2021]
42. NCSC (2020) Advisory: APT29 targets COVID-19 vaccine development. Available online at: https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf. [Accessed on: 12th Oct 2021]
43. CPS (2019) Cybercrime—prosecution guidance. Available online at: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance. [Accessed on: 12th Oct 2021]
44. NCSC (2021) Using TLS to protect data. Available online at: https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data. [Accessed on: 24th Sept 2021]
45. Cucko S, Turkanovic M (2021) Decentralized and self-sovereign identity: Systematic mapping study. Available online at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9558805. [Accessed on: 13th Oct 2021]
46. Susukailo V, Opirskyy I, Vasylyshyn S (2021) Analysis of the attack vectors used by threat actors during the pandemic. Available online at: https://ieeexplore.ieee.org/document/9321897. [Accessed on: 25th Oct 2021]
47. Azourlt (2021) Azourlt. Available online at: https://any.run/malware-trends/azorult. [Accessed on: 17th Oct 2021]
48. Microsoft.com (2021) Microsoft 365.Bring out your best in school, work, and life. Available online at: https://www.microsoft.com/en-us/microsoft-365. [Accessed on: 17th Oct 2021]
49. Fartitchou M, Makkaoui KE, Kannouf N, Allali ZE (2020) Security on blockchain technology. Available online at: https://ieeexplore.ieee.org/document/9199622. [Accessed on: 25th Oct 2021]
50. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Available online at: https://web.williams.edu/Mathematics/lg5/302/RSA.pdf. [Accessed on: 25th Oct 2021]
51. Orcutt M (2019) Once hailed as unhackable, blockchains are now getting hacked. Available online at: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/. [Accessed on: 25th Oct 2021]
52. Bandara E, Liang X, Foytik P, Shetty S, Zoysa KD (2021) A blockchain and self-sovereign identity empowered digital identity program. Available online at: https://ieeexplore.ieee.org/document/9522184. [Accessed on: 13th Oct 2021]
53. NIST (2017) NIST special publication 800–63–3. Digital identity guidelines. Available online at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. [Accessed on 10th Sept 2021]

54. Bokkem DV, Hageman R, Koning G, Nguyen L, Zarin N (2019) Self-sovereign identity solutions: The necessity of Blockchain technology. Available online at: https://arxiv.org/pdf/1904.12816.pdf [Accessed on: 14th Oct 2021.]
55. Stockburger L, Kokosioloulis G, Mukkamala A, Mukkamala RR, Avital M (2021) Blockchain-enabled decentralised identity management: The case of self-sovereign identity in public transport. Available online at: https://www.sciencedirect.com/science/article/pii/S2096720921000099#bib14. [Accessed on: 14th Oct 2021]
56. Stokkink Q, Pouwelse J (2018) Deployment of a blockchain-based self-sovereign identity. Available online at: https://arxiv.org/pdf/1806.01926.pdf. [Accessed on: 14th Oct 2021]
57. Zhang P, Schmidt DC, White J, Dubey A (2019) Chapter seven – Consensus mechanisms and information security technologies. Available online at: https://www.sciencedirect.com/science/article/abs/pii/S0065245819300245 [Accessed on: 14th Oct 2021]
58. Bhattacharya MP, Zavarsky P, Butakov S (2021) Enhancing the security and privacy of self-sovereign identities on Hyperledger Indy blockchain. Available online at: https://ieeexplore.ieee.org/abstract/document/9297357. [Accessed on: 14th Oct 2021]
59. Aggarwal S, Kumar N (2020) Chapter sixteen—Hyperledger. Available online at: https://www.sciencedirect.com/science/article/abs/pii/S0065245820300711. [Accessed on: 15th Oct 2021]
60. Zhang B, Zhang T, Yu Z (2018) DDoS detection and prevention based on artificial intelligence techniques. Available online at: https://ieeexplore.ieee.org/document/8322748/references#references. [Accessed on: 13th Sept 2021]
61. Li X, Zhang T (2017) An exploration on artificial intelligence application: From security, privacy and ethic perspective. Available online at: https://ieeexplore.ieee.org/document/7951949/authors#authors [Accessed on: 13th Sept 2021]
62. Anandshree N, Kh J, De T (2016) Distributed denial of service attack detection *using Naïve Bayes Classifier through info gain feature selection.* Available online at: https://www.researchgate.net/publication/309638524_Distributed_denial_of_service_attack_detection_using_Naive_Bayes_Classifier_through_Info_Gain_Feature_Selection. [Accessed on: 13th Sept 2021]
63. Yuan X, Li, C, Li X (2017) Deep Defense: Identifying DDoS attack via deep learning. Available online at: https://ieeexplore.ieee.org/abstract/document/7946998/authors#authors. [Accessed on: 13th Sept 2021]
64. Verisign (2018) Q1 2018 DDoS trends report: 58 per cent of attacks employed multiple attack types. Available online at: https://blog.verisign.com/security/q1-2018-ddos-trends-report-58-percent-of-attacks-employed-multiple-attack-types/. [Accessed on: 13th Sept 2021]
65. Wi-Fi Alliance (2021) Discover Wi-Fi. security. Available online at: https://www.wi-fi.org/discover-wi-fi/security [Accessed on 24th Oct 2021]
66. Vanhoef M, Ronen E (2019a) Cryptology ePrint Archive: Report 2019/383. Available online at: https://eprint.iacr.org/2019/383. [Accessed on: 13th Nov 2021]
67. Vanhoef M (2017) Key reinstallation attacks. Breaking WPA2 by forcing nonse reuse. Available online at: https://www.krackattacks.com. [Accessed on: 27th Oct 2021]
68. NSA (2018) Cybersecurity report. WPA3 will enhance Wi-Fi security. Available online at: https://media.defense.gov/2019/Jul/16/2002158109/-1/-1/0/CTR-CYBERSECURITY-TECHNICAL-REPORT-WPA3.PDF. [Accessed on: 25th Oct 2021]
69. Shanley A (2010) *Penetration testing frameworks and methodologies:* a comparison and evaluation. Available online at: https://ro.ecu.edu.au/theses_hons/1553. [Accessed on: 21st Sept 2021]
70. NIST (2008) Technical guide to information security testing and assessment. Available online at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf. [Accessed on: 29th Oct 2021]
71. ISECOM (2010) OSSTMM 3. The open-source security testing methodology manual. Available online at: https://www.isecom.org/OSSTMM.3.pdf. [Accessed on: 29th Oct 2021]
72. Rounsavall R (2017) Storage area networking security devices. Available online at: https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual. [Accessed on 29th Oct 2021]

73. Wilhelm T (2010) Methodologies. Available online at: https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual [Accessed on: 29th Oct 2021]
74. Pentest-standard.org (2014) PTES. Available online at: http://www.pentest-standard.org/index.php/Main_Page. [Accessed on: 29th Oct 2021]
75. Faircloth J (2017) Wireless penetration testing. Available online at: https://www.sciencedirect.com/topics/computer-science/penetration-testing [Accessed on: 29th Oct 2021]
76. Knowles W, Baron A, McGarr (2016) The simulated security assessment ecosystem: Does penetration testing need standardisation? Available online at: https://www.sciencedirect.com/science/article/pii/S0167404816300906#fn0055. [Accessed on: 29th Oct 2021]
77. Gantz SD (2014) Audit-related organization, standards, and certifications. Available online at: https://www.sciencedirect.com/topics/computer-science/open-web-application-security-project. [Accessed on: 29th Oct 2021]
78. Kritikos K, Magoutis K, Papoutsakis M, Ioannidi S (2019) A survey on vulnerability assessment tools and databases for cloud-based web applications. Available online at: https://www.sciencedirect.com/science/article/pii/S2590005619300116. [Accessed on: 29th Oct 2021]
79. Holik F, Horalek J, Marik O, Neradova S, Zitta S (2015) Effective penetration testing with Metasploit framework and methodologies. Available online at: https://ieeexplore.ieee.org/abstract/document/7028682 [Accessed on: 29th Oct 2021]
80. Rapid7 (2021) Metasploit modules and locations. Available online at: https://www.offensive-security.com/metasploit-unleashed/modules-and-locations/ [Accessed on: 29th Oct 2021]
81. Offensive Security (2021) Armitage. Available online at: https://www.offensive-security.com/metasploit-unleashed/armitage/. [Accessed on: 29th Oct 2021]
82. Filiol E, Mercaldo F, Santone A (2021) A method for automatic penetration and mitigation: a red hat approach. Available online at: https://www.sciencedirect.com/science/article/pii/S1877050921017063?via%3Dihub. [Accessed on: 6th Dec 2021]
83. Patil S, Jangra A, Bhale M, Raina A, Kulkarni P (2018) Ethical hacking: The need for cyber security. Available online at: https://ieeexplore.ieee.org/document/8391982 [Accessed on: 6th Dec 2021]
84. Bacudio AG, Yuan X, Chu BTB, Jones M (2011) An overview of penetration testing. Available online at: https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing. [Accessed on: 8th Nov 2021]
85. Vanhoef M, Ronen E (2019) Dragonblood: Analysing the Dragonfly handshake of WPA3 and EAP-wpd. Available online at: https://eprint.iacr.org/2019/383. [Accessed on: 8th Nov 2021]
86. Conrad E, Misenar S, Feldman J (2016) Chapter 5—Domain 4: Communication and network security (designing and protecting network security). Available online at: https://www.sciencedirect.com/science/article/pii/B9780128024379000059. [Accessed on: 7th Dec2021]
87. ALPHA (2020) AWUS036NHA. Available online at: https://www.alfa.com.tw/products/awus036nha?variant=36473966166088. [Accessed on: 13th Nov 2021]
88. Vanhoef M, Piessens F (2017) Key reinstallation attacks: forcing nonce reuse in WPA2. Available online at: https://papers.mathyvanhoef.com/ccs2017.pdf. [Accessed on: 24th Nov 2021]
89. Wireless Hacking (2004) A brief overview of the wireless world. Available online at: https://www.sciencedirect.com/topics/computer-science/key-authentication. [Accessed on: 24th Nov 2021]
90. Al-Rushdan H, Shurman M, Alnabelsi SH, Althebyan Q (2019) Zero-day attack detection and prevention in software-defined networks. Available online at: https://ieeexplore.ieee.org/document/8991124. [Accessed on: 22nd Nov 2021]
91. Johansen HD, Johansen D, Renesse RV (2007) FirePatch: secure and time critical dissemination of software patches. Available online at: https://www.researchgate.net/publication/220722547_FirePatch_Secure_and_Time-Critical_Dissemination_of_Software_Patches. [Accessed on: 22nd Nov 2021]
92. Sherman R (2015) Advanced analytics. Available online at: https://www.sciencedirect.com/topics/computer-science/data-visualization-tool. [Accessed on: 19th Nov 2021]

93. Shealy M (2021) How data visualization helps prevent cyberattacks. Available online at: https://www.klipfolio.com/blog/how-data-visualization-prevents-cyber-attacks. [Accessed on: 2nd Dec 2021]
94. Ryan L (2016) Data visualization as a core competency. Available online at: https://www.sciencedirect.com/topics/computer-science/data-visualization-tool. [Accessed on 19th Nov 2021]
95. Cobb C, Sudar S, Reiter N, Anderson R, Roesner F, Kohno T (2017) Computer security for data collection technologies. Available online at: https://www.sciencedirect.com/science/article/pii/S2352728516300677. [Accessed on: 19th Nov 2021]
96. Bank of England BoE (2021) CBEST threat intelligence-led assessments. Available online at: https://www2.deloitte.com/uk/en/pages/financial-services/articles/cbest.html. [Accessed on: 15th Mar 2021]
97. Bulletproof (2019) Bulletproof annual cyber security report 2019. Available online at: https://www.bulletproof.co.uk/industry-reports/2019.pdf. [Accessed on: 13th Sept 2021]
98. Apple (2007) Apple reinvents the phone with iPhone. Available online at: https://www.apple.com/uk/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/. [Accessed on: 8th Sept 2021]
99. Apple (2021) iPhone 12 and iPhone 12 mini. Available online at: https://www.apple.com/iphone/. [Accessed on: 8th Sept 2021]
100. Gulasekaran SR, Sankaran SG (2021) Wi-Fi 6 protocol and network. Artech House, Norwood, MA
101. Garcia-Rodriguez A, Lopez-Perez A, Galati-Giordano L, Geraci G (2021) IEEE 802.11be: Wi-Fi 7 strikes back. Available online at: https://ieeexplore.ieee.org/document/9433521. [Accessed on: 29th Nov 2021]
102. Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W (2020) Security and privacy in 6G networks: new areas and new challenges. Available online at: https://www.sciencedirect.com/science/article/pii/S2352864820302431. [Accessed on: 1st Dec 2021]
103. Cisco (2020) Cisco annual internet report (2018–2023). White paper. Available online at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Accessed on: 13th Sept 2021]
104. Statista (2021) Number of smartphone users worldwide from 2016 to 2021 (in billions). Available online at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Accessed on 13th Mar 2021]
105. Busch PA, Hausvik GI, Ropstad OK, Patterson D (2021) Smartphone usage among older adults. Available online at: https://www.sciencedirect.com/science/article/pii/S0747563221001060 [7th Sept 2021]
106. Fryman S, Romine W (2021) Measuring smartphone dependency and exploration of consequences and comorbidities. Available online at: https://www.sciencedirect.com/science/article/pii/S2451958821000567. [Accessed on 7th Sept 2021]
107. Pall ML (2018) Wi-Fi is an important threat to human health. Available online at: https://www.sciencedirect.com/science/article/pii/S0013935118300355. [Accessed on: 29th Nov 2021]
108. Kovacic S, Dulic E, Sehidic A (2017) Improving the security of access to network resources using the 802.1x standard in wired and wireless environments. Available online at: [Accessed on 16th Oct 2021]
109. Kleidermacher D, Kleidermacher M (2012) Data protection protocols for embedded systems. Available online at: https://www.sciencedirect.com/topics/engineering/virtual-private-networks. [Accessed on: 2nd Dec 2021]