Archives of Computational Methods in Engineering (2022) 29:1591–1610
https://doi.org/10.1007/s11831-021-09631-5

REVIEW ARTICLE

Survey on Wireless Network Security

Rashid Nazir[1] · Asif Ali laghari[1] · Kamlesh Kumar[2] · Shibin David[3] · Munwar Ali[4]

Received: 13 December 2020 / Accepted: 4 July 2021 / Published online: 13 July 2021

Abstract
A wireless network is used to connect various wired organizational structures and provide connectivity within the organization for employees to move freely by avoiding the hurdle of a physical network. Maintenance of WLAN security is crucial to an organization because WLANs are directly linked to the core organization's network. In this paper, we reviewed the architectures and protocols of wireless communication, security issues, and type of threats used to launch an attack as well as their solutions. Finally, we discuss open research for future development to make a secure wireless network and safe for data transfer.

1 Introduction

Nowadays, the Internet becomes the basic need of human life and is used not only for entertainment purposes, but it helps in doing routine activities like fund transfer, paying bills, ticket reservations, educational research, learning perspectives, business trade, media coverage, etc. If we define the Internet in a single line then it should be, "network of networks known as internet". If we talk about just a network, then what exactly the definition of a network is? Where it came from? So, the answer is: two or more than two nodes (sometimes known as system or computer systems) are connecting to share crucial information or resource. In 1961, Leonard Kleinrock proposed an idea named ARPANET (Advanced Research Project Agency Network) in his research titled "Information Flow in Large Communication Nets" [1].

The term 'packet' came in 1965, and it aims to send data from one node to another. In the era of 1969, ARPANET was one of the first packet-switching networks; this was first used for sharing research from Stratford Research Institute at UCLA (University of California, Los Angeles). Bob Kahn invented TCP/IP in 1978; the aim was to route data from one form to another [2]. The first version of the 802.11 standards for WIFI has a transmission speed up to 2Mbps [3]. In 2018, WAP3 introduced WIFI encryption; more security means more protection [4]. The main objective of computer networks is to exchange resources; there are two main types of networks: (1) wired network and (2) wireless network. In computer networks, data exchange through a connection called data link between nodes, establish a link with the help of cable like coaxial, fiber-optics, and twisted pair. In a Wireless network (WLN), the network is set up by frequency signals, and it means accessing the network without a cable connection [5]. It means accessing internet services without a physical connection but in a particular domain (range) for example WIFI (stands for wireless fidelity).

In computer networks, nodes or hosts are desktops, cell phones, and servers, each has some unique code known as MAC address [6]. In the early stage, diversity arises when different network vendors sell products such as switches, routers, and other products in the market. A method by which home, business, and telecommunication networks

✉ Asif Ali laghari
asif.laghari@smiu.edu.pk

Rashid Nazir
rashid.nazir.baloch@gmail.com

Kamlesh Kumar
kamlesh@smiu.edu.pk

Shibin David
zionshibin@gmail.com

Munwar Ali
munwar.ali@sbbusba.edu.pk

[1] Department of Computer Science, Sindh Madressatul Islam University, Karachi, Pakistan

[2] Department of Software Engineering, Sindh Madressatul Islam University, Karachi, Pakistan

[3] Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India

[4] Department of Information Technology, Shaheed Benazir Bhutto University, shaheed Benazirabad, Sindh, Pakistan

establish connectivity was required to avoid cables into a building; one is the costly and time-consuming process, which is why to consider as lengthy process. It provides a way to develop different wireless connections such as wireless local area networks (WLAN), cell phone networks, wireless sensor networks, satellite communication networks, and microwave networks [7].

Still, wireless network security is a major issue for the organization because of the growth in hacking techniques and different types of threats [8]. Organizations set filters for data to avoid threats and malware attachments, which slow down the data transfer [9]. So this paper will address the topic of wireless security, the start of security issues, solutions, and how to solve security issues in wireless networks.

This paper is organized into 8 sections, and Sect. 2 is based on the wireless network architecture. Section 3 provides protocols and standards and Sect. 4 categorizes issues of wireless security. Sections 5 and 6 provide information on wireless networks, security challenges, and solutions respectively. Section 7 is based on the open research issues and directions for future research for researchers. Finally, in Sect. 8 we conclude the research work.

2 Wireless Network Architecture

The wireless network is the combination of different networks, which allow one computer to access another without means of wired connection physically [10]. The authors recommended an energy managing technique named RadioHub for saving energy consumption in Wireless Network-On-Chip (WiNOC) architecture. In this type of environment, the physical wired connections are not used; however, in some complex architecture wired cables can also be used. These days the most common wireless communication channels are radio signals in the form of the frequency range. Wi-Fi connections are the most common example of such networks. Wireless networks are implemented in the physical layer, which is layer 1 of the OSI reference model [11]. Access points are used to establish a network connection in a wireless environment. This access point is a type of hardware device, which detects and permits the network to access remotely. The next hardware device considered as the most essential part of wireless networks is the router device, which provides a physical way to communicate different networks [12].

Wireless access points work efficiently with a radio transceiver for developing a connection that allows both the transmission and reception of radio signals [13]. These signals are received by client devices that identify the signals, and after confirmation of communication channels, it grants further access to the network. Wireless access points adopt the general standard of wireless communication, which is the IEEE 802.11 protocol. The most common application of this standard is the Wi-Fi termed as Wireless Fidelity.

There are two main types of wireless network architecture, which discussed below:

Standalone Architecture (also known as Ad-hoc mode): In Ad-hoc architecture, all devices are directly connected for communication just like peer-to-peer connection [14]. For setting up on Ad-hoc mode, manual configuration is required instead of an automated process, and no access point such as a router/switch is required for communication. Such type of architecture is used in a small environment e.g. a centralized business domain [15]. Ad hoc wireless network architecture illustration is given in Fig. 1 [15].

Centrally Coordinated Architecture (also known as Infrastructure mode): Devices are connected with the help of an access point means a router/switcher is required for communication. Automatically configure instead of manually handling. Such type of architecture is used in a large environment, e.g. distributed business domain [15]. Centrally Coordinated wireless network architecture, illustration is given in Fig. 2 [15].

3 Wireless Protocols and Standards

The term wireless refers to the transmission of information through electromagnetic waves rather than a wire. The first wireless transmitters were used in the early twentieth century by the use of radiotelegraphy in Morse code [16]. Technology keeps evolving and is becoming a very important part of the life of many people. It has caused many people to become reliant on technology for almost all kinds of work.

Types of wireless access technologies.

(1) *Wireless Personal Area Network (WPAN)*: These are designed for a range of 10 m. Examples of such include IrDA and Bluetooth. More technologies that are currently on the rise for this system are 802.15.4a—Zigbee and 802.15.3c—UWB [17].
(2) *Wireless Local Area Network (WLAN):* This system has a range of 100 m and a speed that can cater to up to 200 Mbps. Wi-Fi (802.11a/b/g) is one of the most widely used WLAN technologies [18].
(3) *Wireless Metropolitan Area Network (WMAN):* This technology can deliver to 75 Mbps. Several iterations of 802.16 have been certified under a brand called WiMAX [19].
(4) *Wireless Wide Area Network (WWAN):* This system has a range of a few hundred Kbps and extends services to larger areas such as cities, regions, and even countries. Commonly used technologies are GSM/GPR/EDGE [20]. Third-generation technologies consist of HSUPA and EV-DO Rec C [21].

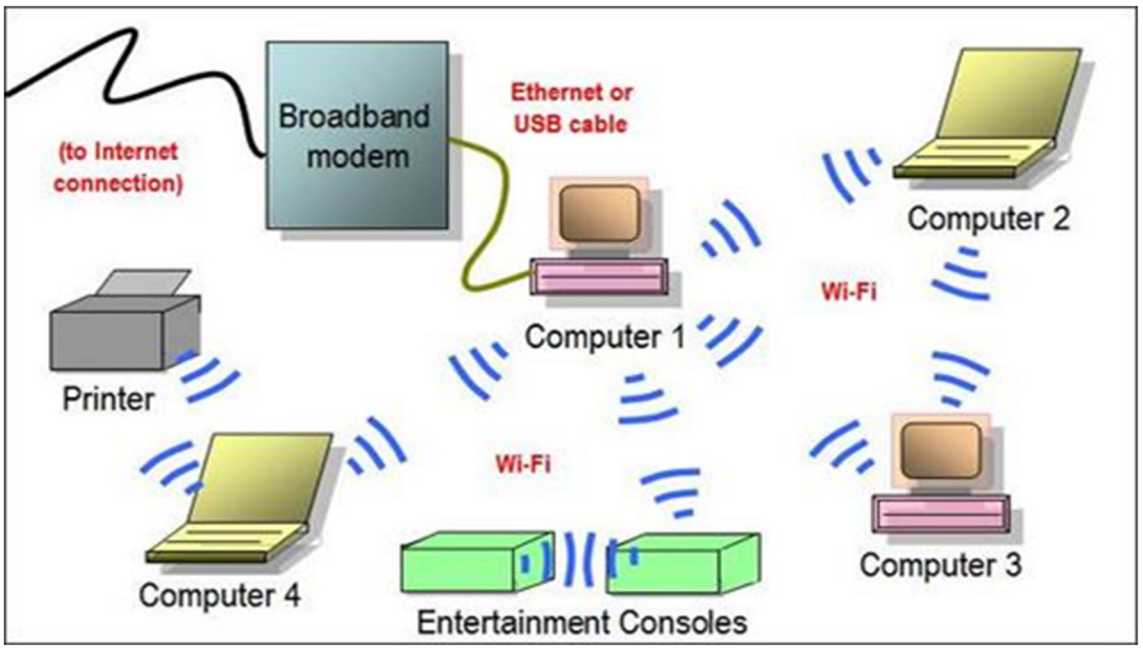

Fig. 1 Ad hoc mode

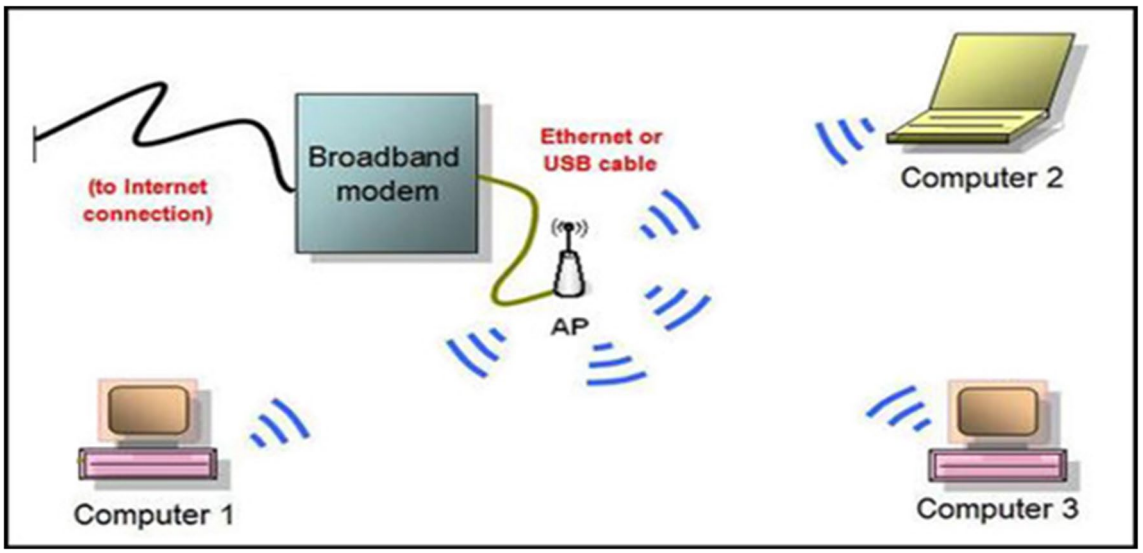

Fig. 2 Infrastructure mode

In a WLAN, a mobile user connects to LAN by a wireless connection. WPAN refers to a personal area network used to interconnect devices inside the workspace to operate wirelessly. Even though systems like Bluetooth and IrDA are quite advanced, WPAN continues to develop quickly.

3.1 Wireless Protocols

3.1.1 Wi-Fi

It is a term used to specify one of the types of 802.11

families. Wi-Fi Alliance [22] coins the term 'Wi-Fi'. The wireless LAN node is responsible for a public connection via Wi-Fi that is given from a certain location is called a hot spot. A lot of airports, hotels, fast-food chains, and public spaces allow access to their Wi-Fi networks.

I. *WiMAX:* It has a range of 30 miles and presents a provider network that can be accessed by a wireless solution [23].
II. *Bluetooth:* It is the development of the telecommunications industry that leads to the understanding of how phones, computers, and PDAs can connect to wireless connections at a short distance.
III. *Ultra wideband:* Ultra-wideband is also commonly known as is also called UWB [24]. It is a wireless technology set up to transmit huge amounts of data digitally over a wide range of frequency bands for low power at a short distance.
IV. *802.11*: This belongs to a currently changing family of the WLANs developed by the Institute of Electrical and Electronics Engineers. New specifications are added from time to time.
V. *Wireless Standards:* 802.11 are the specifications of the over-the-air interface between a wireless device and a station that exists between two wireless clients.

There are different kinds of specifications in the family:

(1) *802.11a:* It provides 54 Mbps in a 5 GHz band to wireless LANs. 802.11a makes use of the orthogonal frequency encoding rather than FHSS or DSSS [25].
(2) *802.11b:* It applies to wireless LANs and gives a speed of 11 Mbps in the 2.4 GHz band. This type of specification only uses DSSS. 802.11b was ratified in 1999, which allowed it to function wirelessly [26].
(3) *802.11e:* It is a draft standard that determines the Quality of Service (QoS) support for LANs; this is an enhanced version of the other WLAN specifications. The 802.11e provides features such as being able to support multimedia devices and allow wireless connectivity to 802.11a and 802.11b standards [27].
(4) *802.11 g:* This specification applies to wireless LANs and can be used for short-distance transmissions like 54 Mbps in the 2.4 GHz bands [28].
(5) *802.11n:* This one adds a feature of multiple-input-multiple-output (MIMO) in the other standards [29]. Extra antennas are added for transmitting and receiving large amounts of data through spatial multiplexing and diversity by using code like Alamouti coding. The speed is 100 Mbits/s, which is five times faster than 802.11 g.
(6) *802.11ac:* It builds upon the 802.11n standard to deliver 433 Mbps per stream or 1.3 Gbps in the three-stream design [30]. The 802.11Ac specification works in the 5 GHz range and allows support for many channels. It also has beam forming capabilities to cater to better speed.
(7) *802.11ac Wave 2:* This is an update of the 802.11Ac, which uses MU-MIMO technology and has other advancements that help increase speed to 6.93 Gbps [31].
(8) *802.11ad:* It is a wireless specification that is undergoing development and set to operate in the frequency of 60 GHz band. It offers a transfer rate, which is as high as 7 Gbps [32].
(9) *802.11ah:* This is also known as the Wi-Fi HaLow [33]. It is the first wireless standard that operates in a frequency band below one gigahertz and possesses a range of twice as many as the other Wi-Fi technologies.
(10) *802.11r:* This is also called Fast Basic Service Set (BSS) Transition [34]. It allows support for VoWi-Fi handoff to enable access points operating between VoIP roaming on a Wi-Fi network that has authentication of 802.1X.
(11) *802.1X:* The 802.1X is an IEEE standard used for port-based Network Access Control [35]. It allows the network admins to use IEEE 802 LAN services on a restriction. It helps in establishing secure communication between authenticated and authorized devices.

4 Categorization of Security Issues

Security categorization is the classification of vulnerabilities or threats that the system of information might face in real-time processes. These categories are based on different factors such as the potential impact of any event or it could likely be a result of any malpractice of manipulation. It depends on the overall management system of an organization that deals with such issues. There are several risks involved in the categorization of security issues like potential loss or damage or misuse of information. The important part of security categorization is identifying the various forms of information that the organization process, store and retrieve. In every situation, it is essential to avoid the expected risk and minimize discrepancies. Several standards followed to enlist the threats. These threats sometimes damage the confidentiality of data or its integrity as well. The companies classify their security issues as per their perceived models or sometimes by their functional practices. This can be multiple forms of security weaknesses, amongst all the most common are misinformation, falsifying the statistical information, theft or damage of data, web-based hacking, and internal employee manipulation.

To find these threats, sources, and specific areas of the system that may be affected should be known so that the information security assets can be protected in advance. Effective security classification is necessary to understand and identify threats and their potential impacts. Security threats can be observed and classified in different ways by considering different criteria like source, agents, and motivations. While having a glance at different wireless security papers, it is clear that the security threats and vulnerabilities are advancing with the exploration of technology. In our research paper, the trend of emerging security threats are analyzed by reviewing security-related papers as well as recording the real occurrence of risks in the industry.

4.1 Threat Classifications Principles

A general taxonomy is used to gain an overall understanding of the security patterns to propose a way to develop a classification model of security matters. The below principles should be adopted to classify security issues and develop a specific model.

- The threats pattern varies from company to company, but the general effects remain exclusive in functionality, and sometimes it overlaps.
- The second principle is that it must cover all the possibilities like every threat type.
- The third part is that it should be simple and clear to everyone.
- It should be repetitive.
- It must be logically accepted in every domain.
- It must be beneficial in one way or the other.

4.1.1 Type of Security Threats/Vulnerabilities

4.1.1.1 Source of threat Depending on the information or data of the system, the source can be varied. Cloud computing environment deals mostly with third party hacking or malware attacks, whereas a local business company may get lost due to internal damages by the trusted employee or person. Generally, there are two most common terms used for such threats, external and internal. Different programs or applications are run by the end-users disrupt the system as an external source. The internal working class will put efforts into fraud or forgery operations and unusual working anomalies [36].

The agency for Network and Information Security (ENISA) is a European center, which works closely with the neighboring countries for addressing cybersecurity issues by classifying the threats as well as forming policies for addressing those threats [37]. ENISA shares its ENISA threat landscape for propagating the list of threats encountered during a year such as 2018 [38]. The most innovative trends in wireless network security have emerged the state of art plans for maintaining high profile security policies. The shape and path followed by hackers have reinforced companies to think and act smartly. These threats have changed dramatically with time. The general categories of vulnerabilities or attacks become much understandable when ETL starts listing the threats [39, 40]. By observing the pattern and background of a specific category, sometimes a large number of attacks were DOS or phishing and vice versa (Table 1).

O maintain wireless services, it is essential to handle threats as soon as possible that create hindrance for both

Table 1 List of threats according to ETL

Malware	Type of software that affect or destroy the user's computer or data
Web-based attacks	Software programs that identify any vulnerability weakness and create a path to exploit the attack
Web application attacks	Server/client side scripting can be used to store, retrieve the legitimate user's data with unauthorized access
Phishing	A fraudulent way to gain access of confidential information mostly done by email
Denial of service	DOS is malicious attempt to discontinue services for user
Spam	A possible unsolicited junk email use to damage the computer resources
Botnets	Series of compromised devices that can be exploited by the hackers
Data breaches	Access of sensitive and legitimate data by an authorized user through a fraudulent way
Insider threat	Security risk to organization which can be initiated by an employee or trusted person
Physical manipulation/Damage/Theft/Loss	This can damage, manipulate and altered the data physically which provide loss financially as well
Information leakage	An unintentional leakage of information attract hackers to further expose the vulnerability
Identity theft	An authorized use of personal information of someone to ascertain non legitimate benefits
Cryptojacking	A kind of theft of computational power to acquire crypto currency
Ransomware	A malware to affect someone's data or files for intention of grabbing money
Cyber espionage	This is way of taking unauthorized access of secret data of high profile government agencies by entering into the network
Exploit kits	An automated toolkit with range of exploited programs to disrupt the system

user and service providers. Certainly, threats are varied but have identical losses such as financial loss, loss of assets and reputational loss, etc. There is another way to evaluate the possible vulnerability by researching the scope of the threat of Data/Information, Applications, Infrastructure, and cloud service in the computing environment [41].

By summarizing the analysis of different surveys the different forms of threats/obstacles in the cloud computing environment comprise four classifications: Threats to applications, Threats to data, Threats to infrastructure, Threats to cloud services. The trend of operations has been shifting from on-premise to cloud environment, which needs to develop plenty of online application services [41]. By having such a live environment, it is much likely to face severe risks associated with the security of applications and data. The development of the Cloud Computing application can further proceed to legal protection, ownership of devices, compatibility of machines, and other policy related complexities.

Large organizations heavily rely on the review or feedback of the information security's risk assessment specifically when migrating to the cloud environment [42]. There are several risks associated with the assets of the company. The possible source of the attack on online data sharing, authentication, data storage should be identified earlier to avoid any damage. The researchers suggest the simplest way to discuss and identify the risk derived from the security perspective of the cloud and involve a five-step process for discovering a different kind of threats.

- Write formulation of risk or threat
- Search by writing the keywords
- Select and make assessment
- Analysis of threats identified
- Consolidate the results

4.1.1.2 Group or Individual Threat This is globally covered under a threat agent who can propose a series of damages to the organization in several different methods. If a person is involved in any such criminal offense, it might lead to a human-based threat. The threat can involve information systems and cybersecurity aspects. If a breach occurs due to poor regulations or misuse of the standard set by the organization, it leads to an information security threat, and if anything going goes wrong with the web application, it could be a cyberattack. In this type of threat, the attacker first strike and tries to take control of the system, if it succeeds then the attack turns into EXPLOIT. The human threat, environmental threat, and technology-based threats are a few of the examples of a group or individual threat [43].

The Threat agent remains more active in a wireless network as compared to a wired network [44]. The most likely cause is that wireless networks specifically cloud networks are more vulnerable to threats. The cloud applications are used for a rental basis, which provides an exorbitant income for service providers and attracts severe security threats at the same time. In such an environment, both individual and group agents can attack the system to disrupt the cloud environment. The hackers can develop multiple ways to initiate their strikes such as involving human intervention or by machine interruption. These days the web-based applications have suffered from online system breakdowns or sluggish network flow. In either way the cloud computing networks are badly affected by single or series of security attacks, which results in data loss, malware drive, DoS attacks, misuse of data, and uncertain application programming interfaces.

Cloud applications are mainly using interfaces through the web [45]. The cloud service providers handle the APIs by allocating certain regulations [46]. It helps in identifying any mishaps or anomaly that is stored and monitored. In some cases, unauthorized users and lead to data loss or breach can use the API. One or multiple threat agents can perform it. The human threat is an essential element in breach of data because users who want to achieve the target of disrupting the network can produce every possible attack regardless of its position. To damage, the cloud computing environment person is persuaded by social engineering. In this kind, the activist or attacker disguises and pretends the trusted user for performing the offensive act. It can be done by inserting malicious programming code into the storage drive or by extracting the USB port for unauthorized access. It cannot be the only way to destruct the system, however; it depends on the intention and capacity of the hacker. Therefore, the giant companies always enforce the highly recommended system security features in the cloud network to minimize the possible risk and loss.

4.1.1.3 Threat Motivation It represents the reasoning of the threat that occurred due to an event. The incident is analyzed and assessed for understanding the comprehensive facts and figures of the threat. The most popular formula for analyzing or some way of estimating the proposed risk is by multiplying the threats to vulnerability as below [47].

$$\text{RISK} = \text{THREAT x VULNERABILITY}$$

Threat motivation studies provide a way to understand the combinational consequences of threat and vulnerability factors as it may be inappropriate to illustrate the exact conclusion while keeping only a vulnerability viewpoint. In the past, organizations developed their system security architecture based on threat or vulnerability separately however, it is not considered to be a progressive approach to handle security mishaps. Threat motivation involved a comprehensive analysis of all sorts of hardware and software-related elements as a part of investigating the

vulnerabilities. To minimize the impact of vulnerabilities it is essential to understand the interactive approach of threat, system specification, and security mitigation [47]. The author suggests that the success of the attack depends on multiple variables like attacker type, funding, skill level, the motive behind the attack, etc.

Security professionals adopt multiple ways to address the effects of security mitigation [48]. However, in any of the methods, threat motivation should never be ignored. It is recommended by the authorized security institutions to emphasize threat events and exploitation of vulnerabilities at the same time. The understanding motive behind the scene or event is more reliable. However, the motivation for threat varies from case to case basis. In a broad spectrum, the two categories of threats for understanding motivation are human and natural.

To build a valuable security system analysis, professional guesses the motivational factors behind any threat because it provides flexibility when resources are in scarcity. The study reveals that risk mitigation tools are more applicable than risk elimination tools. While developing a comprehensive plan for combating the possible threat vulnerabilities, an engineer must emphasize collective motives rather than individual motives, which portray an individual's ambition. Collective motive detects the likely "attacker type. Threat motivation can also be assessed with one of the key factors like estimating the funded amount of driving an attack. It is also possible to use cost-free tools, but their results remain unreliable. It mainly depends on the type of attack, and funding involves a large number of people and time as well.

Threats can be categorized into several segments, such as human and natural threats. The human threat is more severe as compared to the natural. The only reason for this comparison is that human intention may lead to a controversial plan before committing any attack, which does not apply to the natural threat. Hence humans are the leading role player in terms of the volume of threats. To take a glimpse of the motivation of potential attacks, information security engineers focus on potential attack vehicles. Social engineering is also an effective aspect to persuade people for getting into a system for malpractices. Phishing is the most common element of a social engineering attack [49]. Mitigations are addressed by analyzing the system security architecture, which resides in the hardware and software applications, a block diagram of a system, the control, and the data panel. The threat motivation is dependent on the system design and security mitigation, which are mostly interlinked for operational functionality. This will be the role of security engineers to strengthen the security system architecture by providing maximum protection tools and applications, which somehow mitigate the possible attack or vulnerability.

4.2 Threat intent

The threat may come from the action of a person, which may be intentional or not.

4.2.1 Intentional Threats

Intentional threats refer to the purposeful actions resulting in theft or damage of computer resources, equipment, and data. Intentional threats include viruses, denial of service attacks, and theft of data, sabotage, and destruction of computer resources.

Cloud computing applications as a whole provide a wide range of services to their consumers like a professional programmer or computer scientist and an ordinary user as well. These services range from storage to virtualization besides several other purposes. Using the internet to access emails, playing online games, e-commerce, and social communication apps are evidence of a variety of cloud usage applications. With exclusive applications of the cloud, it is sometimes possible to use cloud services without any charge as a promotional facility by the companies. It will provide free access to Facebook, Skype calls, and download storage entities. There can be more than the stated reasons for granting packages to cloud users of the service provider. While promoting the cloud applications and propagating the network of services, there is a boundless chance for misuse of cloud services, which will be termed as an intentional threat [50]. The hackers can exploit the vulnerabilities of systems to leak the data of users. The purposeful disclosure of information can be done for several reasons such as to damage reputation, bring falsified achievements, and steal the resources.

Intentional threats are types of offensive acts in which the suspected strikers have more options for attacks as compared to unintentional threats. To compromise the system, the attacker can initiate a series of battles such as DOS attacks, theft of service, hidden scripting codes, leakage of information, and several other ways. The cloud servers are sometimes rented for online services and to maximize the storage capacity of the data which may engage developers and programmers to switch from one server to another. In doing this kind of activity the intended user attempts to get unauthorized access. Like hackers can use Amazon's EC2 facilities to damage the gaming workstations of other competitors. Companies sometimes leak personal information for unjustified reasons. Epsilon and Stratford are examples of such intentional expose of information, which disclose the customer's name, email address, and other information meaningfully [50]. The authors in their research extract data breach and their financial impact information with the help of data mining method. Different sources for calculating data breaches were used like IBM's gold standard research,

Wikileak disclosure of secret information, and Data-loss (DB) data breach report.

4.2.1.1 Intentional Threat in Cloud Environment The wireless network is the most effective part of the cloud computing environment, which consists of more than a single network, sometimes also termed as a network of networks. It consists of computing models such as SaaS, PaaS, and IaaS [51, 52]. These models work as per the requirement of the user and by sharing a way to store, retrieve, and compute the data through virtualization. It is evident that despite its number of benefits, the major concern to maintain the overall network is security and privacy. According to the latest blogs and surveys, the top ten service providers of cloud applications are Microsoft, Amazon Web Service, Salesforce.com, IBM, Google, SAP, Oracle, Workday, and VMware.

4.2.1.2 Data Leakage or Breach The most common risk dealt with by the cloud environment is the data breach, which can be produced by human intervention and system malfunctioning [53]. The attacker can ascertain the information about the vulnerabilities of the system and may affect a series of machines just like a botnet attack. The disclosure of secret information can be done by internal and external agents, however; threat poses damage to an organization's reputation.

4.2.1.3 Malpractice of Cloud Resources Cloud applications are supposed to be powerful processing programs, which compute the programs much faster as compared to normal applications [54]. The hackers can use and exploit the computation power for several threatening activities. For instance, the brute force attack can be accomplished by breaking encryption and attempting several passwords for accessing the system.

4.2.1.4 Malicious Insider Threat They are the ones who have legitimate access to the environment and occupy a functional role in organizational operations. The current or ex-employees can be persuaded to expose the hidden information. The grievances of an employee can influence him or her to invade unlawful acts to disrupt the organization. There can be several reasons to act negatively by the insider, such as gaining illegal profits and damaging the operations.

There are several methods for detecting the possible vulnerabilities or weaknesses in the network. However, the companies apply VAPT (Vulnerability and Penetration Testing) to check out possible holes in the network [55]. The threat agents can exploit susceptible parts of the system and aggravate their intentional threat to the organization. The VAPT can be done by both internal and external entities that depend on the requirement of the organization. The author in [55] performed both manual and automated penetration testing on the web application. Open source and commercial web-based tools did the penetration testing. They have proved that manual penetration testing is more successful than an automated web-based tool in terms of accuracy for detecting vulnerabilities. They followed a comparative and conceptual approach to analyze vulnerabilities. Furthermore, the best practice of vulnerability testing is considered to be more valuable if processed by third-party consultants. The scope and strength testing are settled by discussing the knowledge base regarding any expected loopholes in the system. It is one of the effective ways in a cloud environment to handle discrepancies within the organization. This activity will minimize the risk, which finally compromises the devices and network. As a part of the comprehensive vulnerability analysis, different tools are used to defuse the intended threat from hackers. It can be using SQL injection, port scanning, and analyzing packet signals.

Unintentional threats are a kind of risk in which human interruption remains a major contributing factor. The threat occurs due to some inadvertent behavior of a single or combination of several factors. Sometimes the negligent actions cause severe consequences in the form of exploitation or vulnerabilities [56]. It is said that such avoidance of responsibility causes different kinds of damages to assets. However, simple ignorance can be termed as a disastrous result if precautionary steps are not taken by the organization.

Breach of information is one of the most critical risks for the company's reputation, and the likely reason for this can be an unintentional human mistake, ignorance of security measures, and information security shadow [57]. Most of the time perpetrators of breach or misuse of information is insider person that can be a trusted employee. These days the cloud computing application involves many social applications, which are mainly persuaded by social engineering as well. The true attacker may ascertain the information of any such unintended activity of employees so that the actual attack can be initiated. The trend of bringing personal devices like laptops is used for official purposes also called to bring your own devices (BYOD) [58].

A personal device that creates a way for attackers to detriment the rules. The organizations must evaluate an assessment of risks regarding the culture, behavior, and feedback of the employee for following the rules like a code of ethics.

Insider attackers play a vital role in dealing with the risks as they may or not involve intentional or unintentional threats [59]. The insider is pertinent to mental disorder factors such as professional jealousy, competition, career growth, and fatigue, and strength limitation. There is a possibility that the insider may not intentionally involve in criminal activity but somehow assist indirectly the hackers. The simplest way of such manipulation is social engineering, which one can easily persuade by fictitious statements

[60]. With the advent of such activities, the chance of any mishap or misuse of the system will be possible through social engineering. In this type of threat, the proposed user remains unaware of any wrongful act of the attacker. However, companies involve security professionals to mitigate the threat by providing awareness training sessions to workers and other factors as well.

An insider working in an organization can be an internal staff either a full-time or part-time worker or ex-employee [61]. The two broad categories of insider threat are an intentional threat and unintentional threat. The unintentional threats are influenced by some major factors such as the behavior of the employee, the motive behind an event, strength, capacity, and risks. Unintentional threats are mainly caused by human error, which is sometimes derived from environmental pressure or personal mental stress and by machine operations. In the normal course of the cloud environment, the end-user tends to be free from any such obligation or responsibility, which aligns it to any damage. To protect the assets of the organization, and personal dignity, there needs to propagate awareness to insiders in the form of training, through messaging and email alerts.

Unintentional threat havoc may arise in several forms like illegal transfer of information, data breach, reputational and financial loss. As per the Partner survey regarding the risk of leakage of information, the main cause is bringing your device concept. The effects of the BYOD concept in the organization brought 72% of information leakage, 56% of illegal access to data, 54% of prohibited software applications, and 52% of malware threats. To minimize the impact of unintentional threats, there needs to develop a comprehensive security framework based on human resource preferences such as employee behavior, satisfaction, and career growth. It will somehow minimize the devastating impact of threat intentional risk.

4.3 Effects of Threats

There can be plenty of damage happen with information or data. The common two effects would be the corruption or misuse of data and disclosure of information. The money launderers and smugglers normally do this. The data can be manipulated by mixing it with scripting viruses stored on tapes, hard disks, and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes. These threat actions can cause unauthorized use of leakage of perusal or sensitive data.

4.3.1 Theft of Service

Theft of services is the legal term for a crime that is committed when a person obtains valuable services (as opposed to goods) by deception, force, threat, or other unlawful means, i.e., without lawfully compensating the provider for these services [62].

Cloud computing is best for providing fast and reliable services to end-users. Mostly the services offered by cloud computing applications are done through virtual machines, which are supposed to be much faster and cheaper as compared to physical devices [63]. The author in [63] has provided a solution to detect and minimize theft-of-service attacks through an API-based VM's power consumption. The author applies two different research methods. First, by taking a substantial literature survey on the KVM and secondly by doing an experiment on private cloud with different virtual machines to detect theft of service attack. As per the software-based approach, the attacker likely creates a hindrance to the services offered to the cloud users. The possible act of such an offense can be paying minimum service fees by modifying or manipulating the virtual machine's usage. It is simply termed theft of service. The cloud server can be badly affected by the extra load, which in turn causes operational and financial loss to the service provider. At the same time, security matters must be addressed otherwise; it portrays severe damage to companies' image. To maintain the exact data regarding software consumption the possible theft of service, several steps must be taken by security engineers. However, the working capacity of the kernel virtual machine must be analyzed in the context of the QEMU emulator. It will prevent possible theft and virtual machine functional utilization from a cloud provider to a service user [63].

Virtualization is one of the features of the cloud, which provides a way to access cloud infrastructure [64]. This is normally done through leasing where the user as like the real hardware machine operates the different virtual machine. For handling the VM, the hypervisor transmits the information as per the requirement of users' needs. Normal theft of service attacks involves a few variables such as modifying the storage limits, processor time and memory usage, etc. In the cloud computing application hypervisor maintains the virtualization facility as per the communication transmitted for further scheduling of the resource. The common types of hypervisors are XEN and KVM. The hypervisor also acts as an intermediary between the host operating system and hardware. The service provider as per the demand of users and infrastructure capacity adopts different virtualization techniques.

The possible attacker can access the hypervisor by conceiving hostile or concealment actions. In broad terms, both actions are part of the theft of service attacks. The possible intention of an attacker can be exploring the hidden data or accessing the virtual machine for an unrestricted time limit. In either case, the machine can be compromised, and attackers may ensure to be hidden for illegal intent.

To mitigate the likely risks of compromising the service the first step should be to apply API that can be processed to

detect the theft of service invasion, which triggers in case of any breach or interception of the striker [65]. The KVM virtualization as per QEMU architecture should be constructed to maximize the protection capacity of the application system. The best practice to keep the service safe the API must be placed on other than the primary cloud, which might alert in case of virtualization machine, is compromised.

The second step is to take control of statistical data regarding the consumption of resources by the user at moderate intervals. While calculating the individual usage of services, the concerned user profile must be examined and analyzed its activities during its stay online and offline. The legitimate user can also perform some unusual operations and initiate an offensive approach of theft of service. Data regarding several VM consumptions should be investigated and calculated at different intervals. This kind of activity will lead to detecting a breach in normal services orientation. The administrator can check the low and high-level periodical consumption and trace the variable usage by the possible attacker. By implementing the API process and calculating consumption data, any malicious code activity of the attacker can be traced.

Security issues are the biggest concerns for the cloud computing environment [66]. Insiders as well as external attackers have targeted wireless network applications. However, a large number of such offensive activates are initiated by the trusted worker or employee of the organization. It is because of trust and confidence, which enables an attacker to exhibit a negative venture. Infrastructure as a service is one of the models of the cloud where users acquire virtualized facilities through the internet. In this type of model, there need to ascertain and analyze data of user services such as user logs, bandwidth usage, number of attempts of authentication to detect any anomaly detection. One way to demonstrate such detection of breaches is by using Eucalyptus cloud software to retrieve the maximum detection rate for any kind of unusual event.

The authors in [66] apply progressive methodology by observing, training, and discovering anomalies to identify the internal attacker. It is the simplest method to identify the internal attack and to estimate the volume of theft of service over clouds. The manipulation of services by cloud users involves several types of activities, it comprises malicious or non-malicious acts. The possibility of such stealing of resources is for intentional gains or conspiracy against the organization as well. The attacker can damage the cloud resources in multi-directional approaches like in the shape of paying fewer amounts for service usage, alteration of information, breaching copyright regulation, and misleading memory or processor limits. It is advised to curtail such theft to expand tenant services for cloud service usage so that data can be recorded without intimating the user. Meanwhile, the profiling approach is best to cut off the stealing once the

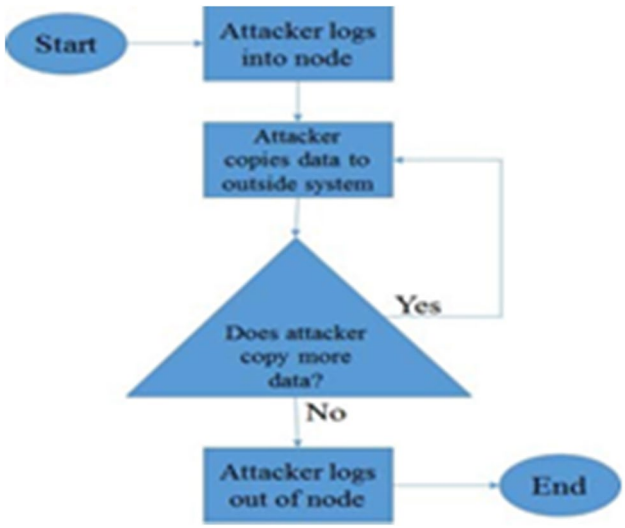

Fig. 3 Insider data theft flow chart [66]

Fig. 4 Anomaly detection is a three-phase process

administrator acquires the exclusive data regarding service usage. The below flowchart Fig. 3 will help to understand the insider data theft detection concept in an IaaS environment.

This approach involves other nodes to acquire red alert irregularities in the form of bytes transmitted through the network. The k-nearest neighbor is the classification algorithm for estimating statistical information, which can help in detecting abnormal data. The application used and information on the connected network will further provide accurate information of any variation. The system is processed and learned to be aware of the guideline of the algorithm and require some checks to monitor the run time data. A specific threshold is maintained for data transmission, online user time, and logging information. The uncommon pattern of data used to recognize the proposed theft of service with the help of k-neighbor peculiarity detection. Anomaly detection is a three-phase process such as training, monitoring, and detecting are given in Fig. 4.

This training process starts with training and ends with the detection of an event in the normal activity of the IaaS cloud application. Virtual machine usage data is checked in different workloads and evaluates two types of entities for handling insider attacks like the one by the end-user online status and packets transmitted.

The algorithm calculates a score for each process and develops a character sequence or pattern which resides in the memory. Each event is compared with the current value and

projected sequence raised through the character sequence. It moves from left to right direction as per score rises until a consolidated score of anomaly detection recognized. In the monitoring, the phase score stored in memory is compared with the values generated during the training phase. The final phase of detection identifies a false positive percentage of theft events in case any irregularity is recorded during the calculation. The tenant virtual machines of the IaaS cloud application propagate all such suspicious occurrences. This kind of approach is simply effective if anomaly detection of theft of service by insider attacker is restricted to packet transfer, several logins by the user, and rhetoric information [66].

4.3.2 DOS

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor [67]. The authors in their study have followed the systematic methodology to identify the problem, gather information, and conduct a test to validate the performance. To get optimal results, the honeypot game was introduced in the network to detect attackers and to acquire the attack-defense relationship followed by the concerned security engineers.

Denial of Service (DoS) attack is one of the common issues, which disrupts the user to reach out to network facilities. The proposed network system remains busy because of unusual traffic manipulation by the attackers. Such offensive strikes are challenges in maintaining wireless network security. To combat storming network flows DoS attack is on TCP layers, and their consequences should be analyzed [68].

Wireless networks are considered to be highly bonded with TCP protocols because these layers are more prone to vulnerabilities or threats [69, 70]. The wireless networks are strengthened by using different encryption techniques for sending messages while transmitting the data through multiple nodes or channels. There is a possibility of injection of malicious code or files at said TCP layers. Ultimately, the system may face a severe downfall of traffic in the shape of DoS attack, MITM, Spoofing, and falsification. Wireless network expands speedier as compared to a wired network meanwhile, the security problems expand with the same range in both types of networks such as data confidentiality, availability, integrity, and authenticity.

4.3.2.1 Denial of Service Attacks in Different Layers Wireless network architecture is mainly dependent on layering-based operations, which makes it more vulnerable to different attacks. Amongst all types of attacks, DoS is considered to be the most common attack. The physical layer is the first part of the OSI model, which performs different tasks like signal identification, frequency selection, and data encryption as well. The attacker can initiate its offensive strikes by leading operations at the physical layer in the form of Tampering and Jamming [71]. It is mostly done by adding access points to the network while keeping the process hidden or ignorable. Further, different codes can be applied to decrypt or capture the image. It will eventually lead to guided tampering of the information to make DoS attack successful. There is also possible to create obstacles in the form of traffic jams or inappropriate interference within the network. The communication process from node to node is interrupted by producing Bluetooth signals. It makes simple communication hard to reach. The engineers exclusively monitor the operational activities and network traffic, which triggers to apply security measures such as applying FHSS, detecting, and re-routing the packets [72].

The MAC layer works by storing the MAC address for identifying the user, which is stored in the NIC (Network Identity Card). In a wireless environment, different communication channels can be accessed by a shared medium. The suspected attacker can sometimes access the MAC address and try to falsify the services on a given network node [73]. These kinds of DoS attacks can be done as Collision, Interrogation, and Exhaustion through network injection.

Network Layer. Internet protocol is the major tool in this layer, which moves packet flow from network to network. An attacker can exploit the network by targeting the IP packets through Spoofing and Smurf attacks [74].

Transport Layer. This layer ensures a smooth connection from a node to another node. UDP and UTP protocols are sometimes affected by DoS attackers by striking the network in the form of flooding and de-synchronization [75].

Wireless networks have always-hard issues of security due to their operational and structural design. Despite several innovative features of the cloud environment, cloud users' biggest concern remains with security. As per the discussion of the DoS attacks on the network, it reveals the below classes of attacks.

- Destructive
- Resource consuming
- Bandwidth consuming

4.4 Elevation of Privilege

Use some illegal means or the use of loopholes in the system to get permission to access, which otherwise was not allowed.

Maintaining security is the leading risk in wireless application networks. Access privilege is rendered for normal activities, but it can spot away from exploitation by the attacker. Elevation of privilege is a kind of process in which the user enjoys the authorization at an absolute level. This

authority can be acquired intentionally or unintentionally, but this is mostly for exploiting the possible vulnerability by an attacker. Now wireless networks are more prone to such processes as internal and external users can affect them smoothly. Sometimes a user is granted limited permissions of reading only, which is further extended to read along with write permission. There is the possibility of some kind of manipulation by the trusted user [76].

SDWN is commonly used in wireless network systems these days, which disintegrates the operational functionalities of the control plane and data plane [77]. It is suggested that this kind of new paradigm requires some auxiliary requirements of security attacks. This helps in implementing proper network management for system administrators by having central control of network traffic. However, in SDWN, the detached management of the network also aggravates vulnerabilities for possible attacks. In such a condition, the authenticity and privilege controls along with confidentiality of data can be affected badly. The authors in [77] have provided a solution to mitigate spoofing-based network attacks by implementing SDWN within a Wifi network. Further, their research has enlightened the future expansion of IoT devices, which ultimately lead to a higher number of DDoS attacks.

Despite logical control of network management, SDWN becomes more vulnerable to attacks such as fictitious network traffic, attack on a single device, DOS attack to control the plane, malicious application, and many more strikes [78]. Maintaining authenticity, confidentiality, and integrity prove to be a challenge for cloud service providers. A simple breach can start by exploiting the authorization at an absolute level. This is simply an elevation of privilege.

4.5 Illegal Usage

It involves the use of the normal services of the system to behave and act like a threat to other illegal purposes. Cloud networks have brought a dramatic change of online resources to users. At first, the users have to rely on the website to navigate through a procedure, which faces problems of network bandwidth, processor speed, and storage. Now the cloud-based applications provide a faster and reliable platform to access the resources through mobile phones and laptops. Despite several advantages of the cloud network, still there is a chance of mishaps in form of misuse of services. The legitimate user can exploit the rules and regulations by helping criminals or committing an offense by using cloud services. Hackers sometimes use cloud storage for sharing illegal data and for perpetrating botnet attacks. Cloud storage is susceptible to manipulation for unauthorized access. Google Drive, one drive, and dropbox are a few of the examples of data storage applications to users [79].

Software virtualization, a cloud software application is mainly used for providing services to cloud users [80]. The terms and conditions for usage of the services are already illustrated in the service level agreement (SLA). Both user and service provider should maintain the abidance of the terms. The service provider must have the capacity to monitor and check the routine logs and must detect any unusual use of the service. For maintaining the utmost security and privacy, the companies introduce a dynamic security contract-provisioning framework, which emphasizes smooth functionality by maintaining the service level in accordance.

4.6 Threats by Social Messaging Apps

Major threats that whatsApp and other messaging and social media applications pose for mobiles are:

- Web Malware
- Unencrypted Backups
- Data Sharing with other Apps
- Encryption Vulnerabilities
- Malicious Code

With speedy internet access to users these days, social communication apps have become an essential part of life. These apps can be accessed simply through android phones as well as computing machines [81]. In this research, it is recommended to use the latest tools to strengthen diagnostic medical results by introducing machine learning algorithms in real-time. The research survey in [81] will help to sort out complex questions like:

- Will technology simplify mental prosperity assessments?
- Will machine learning refine mental happiness classification?
- How to use behavior reinforcement/counseling techniques?

The common communication way is by sharing photos, images, and commenting on the wall page of friends, community, and professional group or site [82]. However, despite billions of social messaging users, the unique issue faced by almost every user is security and privacy. There are several threats and risks associated with the usage of social applications. The major concern of having a huge amount of risk with social communication is the interconnected networks, which provide a way for hackers and manipulators to initiate an attack. LinkedIn, Twitter, Whatsapp, and Facebook are a few of the top-rated social communication applications. Amongst all apps, Facebook is presently having the most users across the world approximating 2.5 Billion users or more [83, 84].

It is suggested that the main contributing factor in overall scams and malware on the internet is through social media applications. As per 2014 research, India was the second leading country affected by cyber-attacks [85]. The hackers may involve several formalities to attack through social media networks. In either way, it needs to adopt certain procedures to exploit the risk or vulnerabilities. The risk can be socially disruptive of information, blackmailing or ransomware, malicious injection of code, failure of encryption technique, and many more. The common steps to strike an attack on social media networks are as below.

- Data/information collection
- Access to social networks
- Propagating malware attacks
- Breach of secret information

To mitigate social media risk, the companies hire security professionals to analyze the latest trend of the attacker so that suitable policies can be implemented. The knowledge of the weaknesses and technology used as a tool is also the factor to address security concerns. There can be multiple types of attacks involved in social messaging applications; the most common are spamming, malware attacks, pop-up windows, scripting code, and manual editing dialogue boxes [85]. The user is persuaded by manipulating the content and advised to click on a certain item on the wall to acquire some kind of benefit. It ultimately leads to some kind of scam that pushes the user to go further, and following the fictitious instructions enables the attacker to gain unauthorized access to the social network.

Clickjacking is one of the classical examples of maligning users in some kind of fraud; however, the trend has been changed with the advent of social applications. The simple click of the user can lead to beginning a scripting program in the background, which remains invisible to the user. Cross-site scripting (XSS) and Cross-site request forgery (CSRF) are simple web-based attacks, which also breach the trust level and helps the hacker to initiate a request on account of a privileged user [86].

4.7 Social Media Security Risks

Phishing emails, scams, web-based frauds and human manipulation through social networks are the most common security risk that provides financial and social damages to society.

- Privacy concerns
- Information about you that *you* post.
- Information about you that *others* post.
- Information about you the *social networking sites* collect and share with others.
- Leakage of Personal and Professional Information shared with family, colleagues and trusted resources.
- The information may be used for social engineering and committing frauds and forgeries.

It is the era where social applications are ruling the technological domain. The number of applications is available for different usage. These applications made life more charming and comfortable. However, there are still queries questionable to software developers for improving these applications. Amongst all apps on the internet, messaging services are leading from the front by covering millions of their users. These messaging apps are available on the Android platform as well as on browsers. There can be thousands of applications for social networking, but the leading apps are Facebook, Twitter, and WhatsApp. These apps are also termed Social Network Sites (SNSs) as both computers and android devices [87] can access these. The authors are confident that two-factor authentication is more defensive as compared to one-factor authentication. The 2FA is also called dual-factor authentication. It adds an extra layer of security for authentication and consists of Token, CAPTCHA, and Password.

Now people interact and discuss plenty of information on the apps, infect share their personal information with friends and family. Despite the most commonly used applications, messaging apps are termed to be more prone to risks. Disclosure of personal information is at a higher pace because of the processing nature of these applications. Multiple risks arise due to the usage of social applications, which also lead to a severe threat to security. The most common vulnerabilities of social applications can be unauthorized information access, data breach, leakage of personal information, and credential theft. To mitigate the risk associated with social apps, there can be different measures to boost the security level. It can be done by updating the software apps, using encryption like 2 Factor Authentication, randomized password. The best tool to strengthen the security approach of social networks is using powerful authentication methods like Token and CAPTCHA. The attackers always try to reach out to the possible weakness or vulnerable parts of the network. In the case of social messaging apps users, there is a chance that the personal information of the user can be shared at different locations on Facebook or Whatsapp, which is ultimately entertained by an intentional threat agent. The user mostly remains unaware of the offensive intent of the attacker due to the senseless attitude of using social networking sites, which eventually results in digitalized cybercrime offenses [88].

Social application users face cyber offenses risks in the form of fraud, scams, ransomware, and blackmailing tactics. It is one of the major reasons that global social networking companies share their information security policies to

strengthen the user's profile and minimizing the risks. However, it is suggested to conduct awareness training sessions for mitigating any such risk. Social accounts are compromised due to flexible security settings, and hackers exploit the secret information, which has negative effects on the user's reputation [89].

In the first step for improving the security of the user's data, it is essential to implement two-factor authentications instead of single-factor authentication. The user must prompt to log in to any social application for providing a username and password along with a Token to make a successful attempt. CAPTCHA is one of the ways that differentiate human intervention from a robot. It is just to strengthen the authentication process.

The second approach should be to adopt algorithmic techniques, which involve data mining for understanding the user's behavior by analyzing the current and past history of information. In the case of anomaly detection, the user must be informed about any unusual action against its account. The most common example of such login detection is using Microsoft or Google account on a different machine instead of a regular device.

The third approach is to promote the social messaging site for the implantation of an integrated development environment for web server facilities. MySQL, PHP, and Apache are the few of the examples of the tool, which works efficiently in scripting programming. A strong access control mechanism can also be developed for online authentication processes.

5 Wireless Networks Security Challenges

Security is the primary concern specially when data is transmitting from end to end, it must be secured, and protected.

5.1 Security Requirements or Ethics in Network

5.1.1 Confidentiality

Only a receiver must read the transmitted data, and if data is hacked, the hacker cannot read it. The encryption of data is applied for confidentiality purposes [90].

5.1.2 Integrity

The transmitted data must be received by the receiver as same as sent by the transmitter without any alteration or modification in data.

5.1.3 Availability

Network should remain operational at all the time.

5.1.4 Non-Repudiation

The sender must accept the transmitted data at all times. For this, Digital Signature should be implemented to achieve Non-Repudiation [91].

5.2 Attack/Threat Types

5.2.1 Active

In this type, the hacker tries to modify or delete or append in transmitting data in between the transmission, and impacting on authenticity, integrity, and confidentially of data [92].

5.2.2 Passive

In this type, in this type, the hacker can view the data without updating it, and it is impacting confidentiality.

5.2.3 Insider

When any point is compromised, and from this point, data is captured and execute the malicious program/script.

5.2.4 Outsider

In this type, there is no access, it is just captured the data, which is transmitted.

5.3 Challenges

5.3.1 Vulnerabilities

5.3.1.1 Wireless Medium In a wireless network, jamming and scrambling are public security issues, and it is using a weapon in a wireless network by an attacker for effecting normal operations [93]. This paper reveals the upcoming security threats and challenges that emerged in the wireless satellite field about traditional safety measures. In the jamming type of vulnerability, the attacker can use the hardware for exploiting the powerful noises for disturbance in wireless transmission signals, and as a result, the connections between the nodes are affected. Scrambling is also a type of jamming but is used based on occasional intervals. In scrambling, the transmission sometimes works smoothly, however, there is also the possibility of sudden blockage, and the result is the same as jamming.

5.3.1.2 Cooperative MAC At the data layer level, the wireless network is using the Medium Access Control (MAC) protocol, and this is shared among all connection points. Cooperative MAC is creating a huge impact on wireless communication performance [94]. The authors divided the

study into three steps such as utilizing slack machines in multidirectional transmission, implanting a cross-network model, and measuring performance with Adaptive Cooperative Network Code- MAC protocols. It is creating a packet collision issue, generating an extra burden on bandwidth, power utilization, and computational processing. It is impacting when the sender is sending the packet ready to send (RTS) to the destination with clear to send (CTS). In this type, the malicious point hacks the MAC for a long time, and unnecessary transmission generates and other points are unable to contribute to communication.

5.3.1.3 Multi-hop Environment A wireless environment is a multi-hop architecture because it provides convenience in process and easy to deploy. In this architecture, the user data is transmitted from source to destination by hop to hop. Multi-hop architecture is cost-effective, point flexible, easily configurable, and manageable [95]. It is providing reliability and multi-points as well. In this architecture, if any point fails, the alternate path is used to the communication process. There are three main issues in this architecture (1) Increase the burden on routing, (2) Risk will be increased in security aspect (3) Bandwidth utilization will be high.

5.3.1.4 Power Limitations The wireless device is using power via its battery. There is a challenge in case an unwanted process executes on the device, and it is consuming power without requiring the process [96]. A sleeping mode is an option, which overcomes this limitation, and the device is still in connecting mode.

5.4 Layer Wise Attack

5.4.1 Physical Layer

On the physical layer, jamming is the most common attack, which abruptly affects the transmission between the source and destination nodes. Jamming utilizes the excess energy and power consumption of sender and receiver devices. The four types of threats, which affect the physical layer are [97]:

Jamming
Tampering
Sybil
Interference

5.4.2 Data Link Layer

In this layer, the attacker attacks the collision technique to send the messages on the network, and it affects the communication channel. Due to this attack retransmission of data, consume the power of devices, and channel utilization as well. Following types of a possible attack on this layer [98]:

Spoofing
Collision
Sybil
De-synchronization
Exhaustion
Eavesdropping

5.4.3 Network Layer

Multiple hoping is the advantage of a network for transmission, and it is the network where data transmit from one to another node. The attacker enters into the network by force or unauthorized access and disturbs the routing table as data transmission is affected. There are two types of attacks in this layer [99].

5.4.3.1 Passive This type of attack will just monitor the activity and keep the information, but it does not disturb the communication as it only discovers the information without altering the data [100].

5.4.3.2 Active This type of attack directly affects the data and updates the data packet, and drop the packet as well. It is attacking routing packets and impacting the unnecessary routing table, therefore, the sender is consuming the extra energy. Following are the type of attack categorized in an active attack.

DoS attacks
Routing attacks
Black hole attacks
Wormhole attacks
Byzantine attacks

5.4.4 Transport Layer

A flooding attack is attempting in this layer. Flooding is creating many connections. These connections are known as vulnerable nodes. In this condition, the sender is allocated to manage the connection request [101]. The study proposes an attack detection model in an IP and optical transport layer-based environment through VPN connections established between hospitals. Such a system involves a healthcare monitoring system to reach out to patient's medical information from remote locations. The authors in [101] initially propose a DoS detection model, analyze intrusion systems, and finally proved that the suggested model will not only identify flooding attacks, but also address user rights, sharing rules, and security assurance effectively.

6 Security Solutions of Wireless Networks

In the previous section, we have addressed some security issues, and the main threats to produce, change, and intercept. Many safety measures that resolve security threats are below.

6.1 Encryption

The organization can use various encryption methods. It is one of the safest ways to protect the information transmitted over the network. For regulatory organizations, symmetric key encryption and asymmetrical key encryption methods are important [102].

6.2 Securing Wireless Access Point

In violating network security, unauthorized installed wireless connections play an important role. By taking the following countermeasures, the organization can reduce the risk of these types of access points:

(1) Remove rogue access points
(2) Default configuration must be updated i.e. the permitted access must be done safely.

6.3 Minimize the Risk of Denial-of-Service Attacks

The problem areas may be detected through routine wireless networking audits; removal of offending devices may reduce the risk of DOS attacks [103].

6.4 Techniques of Signal Hiding

Attacks need wireless networks to be located and identified. The SSID is an identification number broadcast by APs. The SSID is a network identifier. If he/she knows the SSID code, STAs cannot access the network. Therefore, we should turn the SSID transmission off when, not in use and allocate cryptic names to SSIDs to prevent the network [104].

6.5 The Secure use of the Wireless Network

(1) Firewall Technology
(2) Encryption and Decryption Technique
(3) Don't Access Public Hot Spots

6.6 Soft Computing Techniques

Soft computing and its related methodologies are new; therefore, they can extend in various fields.

6.6.1 Artificial Neural Network

ANNs are non-algorithmic neuron systems inspired techniques used in non-linear wireless applications. It makes the system efficient and reliable than traditional linear procedures by its ANN communication. [105].

6.6.2 Fuzzy Logic

It is a rules-based system to address a variety of wireless network problems. We stress the need to control confusion and ambiguity when working with wireless networks. Fuzzy logic thus offers an uncertain device structure that is hard to examine [106].

6.6.3 Genetic Algorithm

This soft computing approach is genetically engineered and natural. A genetic algorithm is a very effective tool to deal with multifaceted wireless network optimization needs [107].

7 Open Research Issues

There are many issues in wireless security, and security is a major issue to avoid information leakage [108]. We discuss issues to be addressed in future research to overcome security issues. Wormhole attack is an issue in wireless communication, and no robust detection method is proposed for routing purposes, which accurately detects this type of attack [109]. It is an open research area where work is still required to develop or propose a routing base scheme, which consumes less energy and detects wormhole attacks [110]. Similar to the wormhole attack, the sinkhole is another type of security issue in wireless networks, and a solution will be required in the shape of a framework or scheme, which drops packets to avoid sinkhole attacks [111]. Spoofed, altered, or replayed routing information feature/sign of the sinkhole attack is rarely considered in the detection [112].

Many types of security attacks are based on watchdog mechanism detection, however, it has many issues and unable to detect attacks accurately [113]. One major problem of the watchdog mechanism is that it consumes high energy for transmission overheating. It can be reduced by decreasing frequency overhearing based on the detection priority criteria. Watchdog methods also have a problem as it does not distinguish among packet drops and particular issues may

arise like collision, channel condition, and so forth [114]. Still, more work is required to solve the issue of lack of focus on the low duty cycle of nodes in watchdog detection methods.

Sybil attack is another type of security problem in wireless communication, and we did not find any state-of-the-art work on this [115]. Still, research is required to propose a method or mechanism to control this type of attack and increase the trust threshold in wireless communication for data transfer. The trust threshold will increase the performance of wireless networks.

8 Conclusion

In this paper, we surveyed and reviewed security issues and threats, which are used to hack the data of the client and make the network untrustworthy. We review different protocols, security issues, and their solutions, proposed through research to overcome the security issues of WLAN. WLAN protection is a system that is constantly changing when running on OTA and exposed quickly to a group of hackers we have raised different wireless network security issues. These security approaches in an organization are fairly good and easy to implement. Soft Computing is an emerging field and a forum for the detection and prevention of intrusion into networks and other attacks. We have discussed open research issues, which leads the researcher to the development of a better security mechanism for WLAN.

Declarations

Conflict of interest Authors did not have any conflict of interest.

References

1. Bay M (2019) Hot potatoes and postmen: how packet switching became ARPANET's greatest legacy. Internet Hist 3(1):15–30
2. Cerf VG, Abbas AE (2019) Internet, technology, and the future: an interview with vint cerf. Next-generation ethics: engineering a better society. Cambridge University Press, Cambridge, p 54
3. Yalda E, Obraczka K, Amiri B (2018) A machine learning approach for dynamic control of RTS/CTS in WLANs. In proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services, pp 432–442
4. Al-Mejibli IS, Alharbe NR (2020) Analyzing and evaluating the security standards in wireless network: a review study. Iraqi J Comput Inform 46(1):32–39
5. Low KS, Win WNN, Er MJ (2005) Wireless sensor networks for industrial environments. In international conference on computational intelligence for modelling, control and automation and international conference on intelligent agents, web technologies and internet commerce (CIMCA-IAWTIC'06), vol 2. IEEE, pp 271–276
6. Allen-Ware MS, Bloom J, Chou JHH, Cochran M, Hughes KA, Iannicelli AT, Pearce JG, Ross A (2019) Preparing computer nodes to boot in a multidimensional torus fabric network. U.S. Patent 10,169,048, issued January 1, 2019
7. Poonam KK, Laghari A, Laghari R (2019) A Step towards the Efficiency of Collisions in the Wireless Sensor Networks. EAI Endorsed Transactions on Scalable Information Systems, 6, no. 23
8. Wang Z, Ruan Q (2020) Research on network security subsystem based on digital signal. J Intell Fuzzy Syst 38(1):97–103
9. Nguyen G, Nguyen BM, Tran D, Hluchy L (2018) A heuristics approach to mine behavioural data logs in mobile malware detection system. Data Knowl Eng 115:129–151
10. Catania V, Mineo A, Monteleone S, Palesi M, Patti D (2017) Improving energy efficiency in wireless network-on-chip architectures. ACM J Emerg Technol Comput Syst (JETC) 14(1):1–24
11. Liu Y, Chen H-H, Wang L (2016) Physical layer security for next generation wireless networks: theories, technologies, and challenges. IEEE Commun Surv Tutor 19(1):347–376
12. Karp B, Kung HT (2000) GPSR: Greedy perimeter stateless routing for wireless networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pp 243–254
13. Pärlin K, Riihonen T, Wichman R, Korpi D (2018) Transferring the full-duplex radio technology from wireless networking to defense and security. In 2018 52nd Asilomar Conference on Signals, Systems, and Computers. IEEE, pp 2196–2201
14. Aneja N, Gambhir S (2018) Profile-based ad hoc social networking using Wi-Fi direct on the top of android. Mob Inf Syst 2018:1–7
15. https://www.louiewong.com/archives/407. Accessed 18 July 2020
16. Nalajala P, Godavarth B, Raviteja ML, Simhadri D (2016) Morse code generator using microcontroller with alphanumeric keypad. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). IEEE, pp 762–766
17. Howitt I, Gutierrez JA (2003) IEEE 802.15. 4 low rate-wireless personal area network coexistence issues. In 2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003, vol 3. IEEE, pp 1481–1486
18. Deng D-J, Lien S-Y, Lee J, Chen K-C (2016) On quality-of-service provisioning in IEEE 802.11 ax WLANs. IEEE Access 4:6086–6104
19. Panda PK, Chattopadhyay S (2019) A modified PKM environment for the security enhancement of IEEE 802.16 e. Comput Stand Interfaces 61(2019):107–120
20. Sowlati T, Rozenblit D, Pullela R, Damgaard M, McCarthy E, Koh D, Ripley D, Balteanu F, Gheorghe I (2004) Quad-band GSM/GPRS/EDGE polar loop transmitter. IEEE J Solid-State Circuits 39(12):2179–2189
21. Kim H (2020) Design and optimization for 5g wireless communications. John Wiley & Sons, Hoboken
22. O'Regan G (2018) Wi-Fi technology. The innovation in computing companion. Springer, Cham, pp 261–263
23. Chang BJ, Chou CM (2006) Adaptive polling algorithm for reducing polling delay and increasing utilization for high density subscribers in WiMAX wireless networks. In 2006 10th IEEE Singapore international conference on communication systems. IEEE, pp 1–5
24. Naqvi SA (2017) Miniaturized triple-band and ultra-wideband (UWB) fractal antennas for UWB applications. Microw Opt Technol Lett 59(7):1542–1546
25. de Carvalho JARP, Veiga H, Pacheco CFR, Reis AD (2017) Performance evaluation of IEEE 802.11 a 54 Mbps open laboratory

links. In Proceedings of the world congress on engineering, vol 1
26. Hisham M, Elmogy A, Sarhan A, Sallam A (2020) Energy efficient scheduling in local area networks. Wireless Netw 26(1):685–698
27. Kumar P, Govindaraj E (2019) Quality enhancement with fault tolerant embedding in video transmission over WMSNs in 802.11 e WLAN. Ad Hoc Netw 88(2019):18–31
28. Park S, Kim J, Kyuntae JO, HanGyu CHO (2020) Method for transmitting and receiving signal in a wireless local area network and device for same. U.S. Patent Application 16/876,309, filed September 3, 2020
29. Dhawankar P, Le-Minh H, Aslam N (2018) Throughput and range performance investigation for IEEE 802.11 a, 802.11 n and 802.11 ac technologies in an on-campus heterogeneous network environment. In 2018 11th international symposium on communication systems, networks & digital signal processing (CSNDSP). IEEE, pp 1–6
30. Cheruvu S, Kumar A, Smith N, Wheeler DM (2020) Connectivity technologies for IoT. Demystifying internet of things security. Apress, Berkeley, CA, pp 347–411
31. Karmakar R, Chattopadhyay S, Chakraborty S (2020) An online learning approach for auto link-Configuration in IEEE 802.11 ac wireless networks. Computer Networks 181(2020):107426
32. Rajan MNU, Babu AV (2017) Theoretical maximum throughput of IEEE 802.11 ad millimeter wave wireless LAN in the contention based access period: with two level aggregation. In 2017 international conference on wireless communications, signal processing and networking (WiSPNET). IEEE, pp 2531–2536
33. Khorov E, Krotov A, Lyakhov A, Yusupov R, Condoluci M, Dohler M, Akyildiz I (2019) Enabling the internet of things with Wi-Fi halow—Performance evaluation of the restricted access window. IEEE Access 7:127402–127415
34. Moura H, Alves AR, Borges JRA, Macedo DF, Vieira MAM (2020) Ethanol: a software-defined wireless networking architecture for IEEE 802.11 networks. Comput Commun 149(2020):176–188
35. Marques N, Zúquete A, Barraca JP (2020) EAP-SH: an EAP authentication protocol to integrate captive portals in the 802.1 X security architecture. Wireless Personal Commun 2020:1–25
36. Kettani H, Wainwright P (2019) On the top threats to cyber systems. In 2019 IEEE 2nd international conference on information and computer technologies (ICICT). IEEE, pp 175–179
37. Drogkaris P Network and Information Security (ENISA) and his interests focus on privacy enhancing technologies, personal data protection and trust. Previously he was involved in several EU-funded research projects and held teaching assistant positions in higher education institutions in Greece. *Surveillance, Privacy and Security*
38. Vozikis D, Darra E, Kuusk T, Kavallieros D, Reintam A, Bellekens X (2020) On the importance of cyber-security training for multi-vector energy distribution system operators. In proceedings of the 15th international conference on availability, reliability and security, pp 1–6
39. Muddu S, Tryfonas C (2020) Interface providing an interactive trendline for a detected threat to facilitate evaluation for false positives. U.S. Patent 10,666,668, issued May 26, 2020
40. Kettani H, Cannistra RM (2018) On cyber threats to smart digital environments. In proceedings of the 2nd international conference on smart digital environment, pp 183–188
41. Abdurachman E, Gaol FL, Soewito B (2019) Survey on threats and risks in the cloud computing environment. Procedia Comput Sci 161(2019):1325–1332
42. Akinrolabu O, Nurse JRC, Martin A (2019) New S (2019) "Cyber risk assessment in cloud provider environments: current models and future needs." Comput Secur 87:101600
43. Alhenaki L, Alwatban A, Alamri B, Alarifi N (2019) A survey on the security of cloud computing. In 2019 2nd international conference on computer applications & information security (ICCAIS), pp. 1–7. IEEE.
44. Shukla AK (2020) An efficient hybrid evolutionary approach for identification of zero-day attacks on wired/wireless network system. Wireless Personal Commun 2020:1–29
45. Laghari AA, He H, Khan A, Kumar N, Kharel R (2018) Quality of experience framework for cloud computing (QoC). IEEE Access 6(2018):64876–64890
46. Kekki S, Featherstone W, Fang Y, Kuure P, Li A, Ranjan A, Purkayastha D et al (2018) MEC in 5G networks. ETSI White Paper 28(2018):1–28
47. Pramanik S (2013) Threat motivation. In 2013 10th international conference and expo on emerging technologies for a smarter world (CEWIT). IEEE, pp 1–5
48. Kitchin R, Dodge M (2019) The (in) security of smart cities: vulnerabilities, risks, mitigation, and prevention. J Urban Technol 26(2):47–65
49. Airehrour D, Nair NV (2018) Madanian S (2018) "Social engineering attacks and countermeasures in the new zealand banking system: advancing a user-reflective mitigation model." Information 9(5):110
50. Mozumder DP, Mahi JN, Whaiduzzaman MD, Mahi MDJN (2017) Cloud computing security breaches and threats analysis. Int J Sci Eng Res 8(1):1287–1297
51. Laghari AA, He H, Halepoto IA, Memon MS, Parveen S (2017) Analysis of quality of experience frameworks for cloud computing. IJCSNS 17(12):228
52. Nazir R, Ahmed Z, Ahmad Z, Shaikh NN, Laghari AA, Kumar K (2020) Cloud computing applications: a review. EAI Endorsed Trans Cloud Syst 6(17):e5
53. Jouini M, Rabai LBA (2019) A security framework for secure cloud computing environments. Cloud security: concepts, methodologies, tools, and applications. IGI Global, Pennsylvania, pp 249–263
54. Ferrari P, Flammini A, Rinaldi S, Sisinni E, Maffei D, Malara M (2018) Impact of quality of service on cloud based industrial IoT applications with OPC UA. Electronics 7(7):109
55. Nagpure S, Kurkure S (2017) Vulnerability assessment and penetration testing of Web application. In 2017 international conference on computing, communication, control and automation (ICCUBEA). IEEE, pp 1–6
56. Saxena N, Hayes E, Bertino E, Ojo P, Choo KKR, Burnap P (2020) Impact and key challenges of insider threats on organizations and critical businesses. Electronics 9(9):1460
57. Gwebu KL, Wang J, Wang Li (2018) The role of corporate reputation and crisis response strategies in data breach management. J Manag Inf Syst 35(2):683–714
58. Palanisamy R, Norman AA, Kiah MLM (2020) Compliance with bring your own device security policies in organizations: a systematic literature review. Comput Secur 2020:101998
59. Homoliak I, Toffalini F, Guarnizo J, Elovici Y, Ochoa M (2019) Insight into insiders and it: a survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Comput Surv (CSUR) 52(2):1–40
60. Weber K, Schütz AE, Fertig T, Müller NH (2020) Exploiting the human factor: social engineering attacks on cryptocurrency users. In international conference on human-computer interaction. Springer, Cham, pp 650–668
61. Moncada A (2020) Employee branding: a mixed method study for implementing an employee branding model in practice
62. Gupta CM, Kumar D (2020) Identity theft: a small step towards big financial crimes. J Financ Crime 27:897–910
63. Ahmad A, Nasser N, Anan M (2016) An identification and prevention of theft-of-service attack on cloud computing. In 2016

international conference on selected topics in mobile & wireless networking (MoWNeT). IEEE, pp 1–6
64. Odun-Ayo I, Ajayi O, Okereke C (2017) Virtualization in cloud computing: developments and trends. In 2017 international conference on next generation computing and information systems (ICNGCIS). IEEE, pp 24–28
65. Khan S, Parkinson S, Qin Y (2017) Fog computing security: a review of current applications and security solutions. J Cloud Comput 6(1):19
66. Nikolai J, Wang Y (2016) A system for detecting malicious insider data theft in IaaS cloud environments. In 2016 IEEE global communications conference (GLOBECOM). IEEE, pp 1–6
67. Wang K, Miao Du, Maharjan S, Sun Y (2017) Strategic honeypot game model for distributed denial of service attacks in the smart grid. IEEE Trans Smart Grid 8(5):2474–2482
68. Singh RS, Prasad A, Moven RM, Sarma HKD (2017) Denial of service attack in wireless data network: a survey. In 2017 Devices for Integrated Circuit (DevIC). IEEE, pp 354–359
69. Abdelsalam A, Luglio M, Roseti C, Zampognaro F (2017) TCP connection management through combined use of terrestrial and satellite IP-Based links. In 2017 40th international conference on telecommunications and signal processing (TSP). IEEE, pp 37–42
70. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A (2019) IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J 6(5):8182–8201
71. Jameel F, Wyne S, Kaddoum G, Duong TQ (2018) A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun Surv Tutor 21(3):2734–2771
72. George W, Sliteris R (2019) Apparatus and methods for mitigation of network attacks via dynamic re-routing. U.S. Patent 10,341,379, issued July 2, 2019
73. Manesh MR, Kaabouch N (2018) Security threats and countermeasures of MAC layer in cognitive radio networks. Ad Hoc Networks 70(2018):85–102
74. Yusof MAM, Ali FHM, Darus MY (2017) Detection and defense algorithms of different types of ddos attacks. Int J Eng Technol 9(5):410
75. Yang G, Dai L, Wei Z (2018) Challenges, threats, security issues and new trends of underwater wireless sensor networks. Sensors 18(11):3907
76. He D, Chan S, Guizani M (2016) Securing software defined wireless networks. IEEE Commun Mag 54(1):20–25
77. Mohammadnia H, Slimane SB (2020) IoT-NETZ: practical spoofing attack mitigation approach in SDWN network. In 2020 seventh international conference on software defined systems (SDS). IEEE, pp 5–13
78. Chien W-C, Weng H-Y, Lai C-F, Fan Z, Chao H-C, Ying Hu (2019) A SFC-based access point switching mechanism for software-defined wireless network in IoV. Futur Gener Comput Syst 98:577–585
79. Ahmed AA, Li CX (2016) Locating and collecting cybercrime evidences on cloud storage. In 2016 international conference on information science and security (ICISS). IEEE, pp 1–5
80. Pahl C, Jamshidi P, Zimmermann O (2018) Architectural principles for cloud software. ACM Trans Internet Technol (TOIT) 18(2):1–23
81. Woodward K, Kanjo E, Brown D, McGinnity TM, Inkster B, MacIntyre D, Tsanas T (2020) Beyond mobile apps: a survey of technologies for mental well-being. IEEE Trans Aff Comput. https://doi.org/10.1109/TAFFC.2020.3015018
82. Laghari AA, He H, Shafiq M, Khan A (2018) Assessment of quality of experience (QoE) of image compression in social cloud computing. Multiagent Grid Syst 14(2):125–143
83. Laghari AA, He H, Karim S, Shah HA, Karn NK (2017) Quality of experience assessment of video quality in social clouds. Wireless Commun Mob Comput 2017:1–10
84. Thakral A, Rakesh N, Gupta A (2016) "Space in space": cyber security capabilities in Indian context. In 2016 online international conference on green engineering and technologies (IC-GET). IEEE, pp 1–6
85. Qamar A, Karim A, Chang V (2019) Mobile malware attacks: Review, taxonomy & future directions. Futur Gener Comput Syst 97:887–909
86. Rodríguez GE, Torres JG, Flores P, Benavides DE (2020) Cross-site scripting (XSS) attacks and mitigation: a survey. Comput Netw 166:106960
87. Abudu AO (2019) Tackling online social network threats: proposed security measures. Abacus (Mathematics Science Series) 44(1)
88. Jouini M, Rabai LBA, Aissa AB (2014) Classification of security threats in information systems. Procedia Comput Sci 32(2014):489–496
89. Heartfield R, Loukas G (2016) Evaluating the reliability of users as human sensors of social media security threats. In 2016 international conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, pp 1–7
90. Medhane DV, Sangaiah AK (2016) Source node position confidentiality aspects in wireless networks: an extended review. Int J High Perform Syst Archit 6(2):61–81
91. Yildiz HU, Bicakci K, Tavli B, Gultekin H, Incebacak D (2016) Maximizing wireless sensor network lifetime by communication/computation energy optimization of non-repudiation security service: node level versus network level strategies. Ad Hoc Netw 37(2016):301–323
92. Shahzad F, Pasha M, Ahmad A (2017) A survey of active attacks on wireless sensor networks and their countermeasures. *arXiv preprint* arXiv: 1702.07136
93. Manulis M, Bridges CP, Harrison R, Sekar V, Davis A (2020) Cyber security in new space: analysis of threats, key enabling technologies and challenges. Int J Inf Secur 2020:1–25
94. Datsika E, Antonopoulos A, Zorba N, Verikoukis C (2017) Cross-network performance analysis of network coding aided cooperative outband D2D communications. IEEE Trans Wireless Commun 16(5):3176–3188
95. Cesana M, Redondi AEC (2017) Iot communication technologies for smart cities. Designing, developing, and facilitating smart cities. Springer, Cham, pp 139–162
96. Chaudhari A, Gandikota J, Sen A, Narayan S (2020) A realistic approach to enhance the battery performance of device-to-device (D2D) Relay UEs. In 2020 IEEE 17th annual consumer communications & networking conference (CCNC). IEEE, pp 1–2
97. Lee E-K, Gerla M, Oh SY (2012) Physical layer security in wireless smart grid. IEEE Commun Mag 50(8):46–52
98. Jadhav R, Vatsala V (2017) Security issues and solutions in wireless sensor networks. Int J Comput Appl 162(2):14–19
99. Bouabdellah M, Kaabouch N, Bouanani FE, Ben-Azza H (2018) Network layer attacks and countermeasures in cognitive radio networks: A survey. J Inf Secur Appl 38(2018):40–49
100. Ee SJ, Ming JWT, Yap JS, Lee SCY (2020) Active and Passive Security Attacks in Wireless Networks and Prevention Techniques
101. Liagkou V, Kavvadas V, Chronopoulos SK, Tafiadis D, Christofilakis V, Peppas KP (2019) Attack detection for healthcare monitoring systems using mechanical learning in virtual private networks over optical transport layer architecture. Computation 7(2):24

102. Manickam P, Shankar K, Perumal E, Ilayaraja M, Kumar KS (2019) Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography. Cybersecurity and secure information systems. Springer, Cham, pp 193–204
103. Demoulin HM, Pedisich I, Phan LTX, Loo BT (2018) Automated detection and mitigation of application-level asymmetric DoS attacks. In proceedings of the afternoon workshop on self-driving networks, pp 36–42
104. Gu Z, Hardjawana W, Vucetic B, Ho LS (2018) Multi-tenant spectrum and SSIDs controller for WiFi networks. In IEEE INFOCOM 2018-IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE, pp 318–323
105. Ghaleb FA, Zainal A, Rassam MA, Mohammed F (2017) An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications. In 2017 IEEE conference on application, information and network security (AINS). IEEE, pp 13–18
106. Ozera K, Inaba T, Bylykbashi K, Sakamoto S, Ikeda M, Barolli L (2019) A WLAN triage testbed based on fuzzy logic and its performance evaluation for different number of clients and throughput parameter. Int J Grid Util Comput 10(2):168–178
107. Cerina L, Santambrogio MD, Franco G, Gallicchio C, Micheli A (2020) EchoBay: design and optimization of echo state networks under memory and time constraints. ACM Trans Archit Code Optim (TACO) 17(3):1–24
108. Zhang X, Fu X, Hong L, Liu Y, Wang L (2020) Provable secure identity-based online/offline encryption scheme with continual leakage resilience for wireless sensor network. Int J Distrib Sens Netw 16(6):1550147720928733
109. Ghugar U, Pradhan J (2020) Survey of wormhole attack in wireless sensor networks. Comput Sci Inf Technol 2(1):33–42
110. Olaniyan OM, Omodunbi BA, Adebimpe E, Bolanle WW, Oyedepo OM, Adanigbo OO (2020) Power aware and secured routing protocol in mobile ad-hoc network: a survey. Technology 11(7):706–717
111. Dong S, Zhang X-G, Zhou W-G (2020) A security localization algorithm based on DV-hop against sybil attack in wireless sensor networks. J Elect Eng Technol 15(2):919–926
112. Salau AO, Marriwala N, Athaee M (2021) Data security in wireless sensor networks: attacks and countermeasures. Mobile radio communications and 5G networks. Springer, Singapore, pp 173–186
113. Ahmad Z, Khan AS, Shiang CW, Abdullah J, Ahmad F (2020) Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol 2020:e4150
114. Chakravorty R, Prakash J (2020) A review on prevention and detection schemes for black hole attacks in MANET. In 2020 8th international conference on reliability, infocom technologies and optimization (Trends and Future Directions)(ICRITO). IEEE, pp 801–806
115. Khalil M, Azer MA (2020) Crypto-SAP protocol for sybil attack prevention in VANETs. Advances in computer, communication and computational sciences. Springer, Singapore, pp 143–152