iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50222

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

A Study of Mobile and Wireless Network Communication from Security Perspectives

Rakesh Kumar[1], Dr. Anant Kumar Sinha[2], Dr. Narendra Kumar[3], Arif Md. Sattar[4]
[1]*Research Scholar, M. U. Bodh-Gaya*
[2]*Associate Prof. & Head Dept. of Physics, A. M. College, Gaya.*
[3, 4]*Assistant Prof. Dept. of Computer Applications and IT A. M. College, Gaya*

Abstract: ***It has been well recorded and is widely recognized worldwide that the usage of mobile devices to perform government business has expanded over the previous 15 years. Threat actors are consequently increasingly focusing on mobile devices and the mobile infrastructure environment in order to look for opportunities for malicious exploitation that could hurt or damage the reputation of government agencies and Enterprise as well. The various protocols, standards, techniques, and systems that are available determine the security measures that are taken. An overview of security procedures, standards, and related technologies is provided. The high-capacity wired and wireless broadband network serves as the foundation for the working environment. The main study areas, current projects, and services on offer are discussed. The future information society is the focus of all endeavors. In order to help organizations create an enterprise-wide mobile security strategy and policy, this paper explains the security features of the mobile security management ecosystem like products, tools, technologies and services.***
We have talked about how mobile phone services are protected from dangers to information security from the standpoint of developers. Mobile Internet usage has grown, and with it, threats against mobile phones and the services they offer. On the other hand, various rapacious software or attackers are attempting to target these services.
Keywords: Mobile Security, Wireless, Communication Security, Mobile App., Hazards;

I. INTRODUCTION

Wireless network technologies allow for the communication of one or more devices without a direct physical link. While wired network technologies use cables to transfer data, wireless network technologies typically use radio frequency. Wireless technology has a wide variety of capabilities geared towards various uses and requirements.

In the past three decades, there have been three significant changes to the computer security requirements. The introduction of the computer was the first significant shift. It became clear that data and information needed to be protected. The general term for a group of tools created to safeguard data and prevent hacker assaults is computer security. Distributed systems, networks, and communication infrastructure for data communication were introduced as the second significant shift. Data transmission must be protected by network security methods. The present, rapid advancement of wireless networks and mobile communications is the third change. So today, wireless protection is very important.

Based primarily on their covering areas, wireless networks can be divided into three groups: WLANs, Wireless Personal Area Networks, and Wireless Wide Area Networks (WWAN) (WPAN). Wide coverage area technologies like 2G cellular, Cellular Digital Packet Data (CDPD), GSM, and Mobitex are all included in WWAN. 802.11, HiperLAN, and other wireless local area networks are included in WLAN. WPAN stands for wireless personal area networks, which include Bluetooth and infrared devices [1].

Wavelengths from the radio frequency (RF) band to the infrared (IR) band are used by wireless devices. The RF band's frequencies, which range from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz, encompass a sizable part of the electromagnetic radiation spectrum (GHz). EM energy enters the IR and then the visible spectrum as the frequency is raised past the RF spectrum.

The communications market's fastest expanding sector is wireless network (WLAN) technology. Worldwide shipments of WLAN units are anticipated to increase through 2007 at a 42% annual rate, according to Gartner study [2]. The strong return on investment made possible by much reduced installation costs, greater availability, and mobile data connectivity is the main driver of this development. A further important benefit of WLAN technology is that setting up wireless networks doesn't take as much work as it once did.

The security of wireless networks, however, is a significant concern because the airwaves, which serve as the communication medium, are vulnerable to intrusion.

Risks usually connected with wireless communications include the loss of confidentiality and integrity and the threat of denial of service (DoS) attacks [3]. Unauthorized users have the potential to access agency systems and data, tamper with agency data, use up bandwidth on the network, negatively impact network performance, launch attacks that bar authorized users from using the network, and even use agency resources to launch attacks on other networks.

II. MAJOR CONCERNS

The mobile phones, handheld communication devices and their communications poses some particular threats. These are enlisted below:

1) Wireless technologies share all of the flaws present in a traditional cable network.
2) When shared between two wireless devices, sensitive information that is not encrypted or that is encrypted using subpar cryptographic methods, may be intercepted and made public.
3) DoS or DDoS assaults could target wireless devices or wireless networks.
4) On internal or external corporate networks, malevolent actors may assume the identities of legal users and conceal their true affiliations.
5) It's possible for malicious entities to invade the private of authorised users and follow their movements.
6) Unauthorized devices, like client devices, access points, etc. can be used by malevolent entities to covertly access confidential data.
7) Portable devices can reveal private information and are readily stolen.
8) From devices that have been set incorrectly, data can be extracted undetected.
9) In order to initiate attacks and hide their actions, malicious entities may connect to other agencies or organizations via wireless connections.
10) To access the network resources of a company or other entity, malicious parties may use un-trusted wireless network services.

III. THE WIRELESS APPLICATION PROTOCOL (WAP)

It is a protocol made for micro-browsers that makes it possible for mobile devices to reach the internet. Instead of HTML, it employs the markup language WML (Wireless Markup Language), which is an XML 1.0 application. It makes it possible to build mobile-friendly web apps. Ericson, Motorola, Nokia, and Unwired Planet established the WAP Forum in 1998 with the goal of standardizing different wireless technologies through protocols. The combined efforts of the different WAP Forum members produced the WAP protocol. The WAP Forum and several other industry forums were combined in 2002 to create the Open Mobile Alliance.

A. WAP Model

The person launches a mobile device's mini-browser. He decides which website he wishes to visit. Using the WAP protocol, the mobile device transmits the URL-encoded request to a WAP gateway over the network. This WAP request is converted by the WAP router into a standard HTTP URL request before being transmitted online. A specific Web server receives the request, processes it as it would any other request, and then sends the answer back to the mobile device via a WAP gateway in the form of a WML file that can be viewed in the micro-browser.

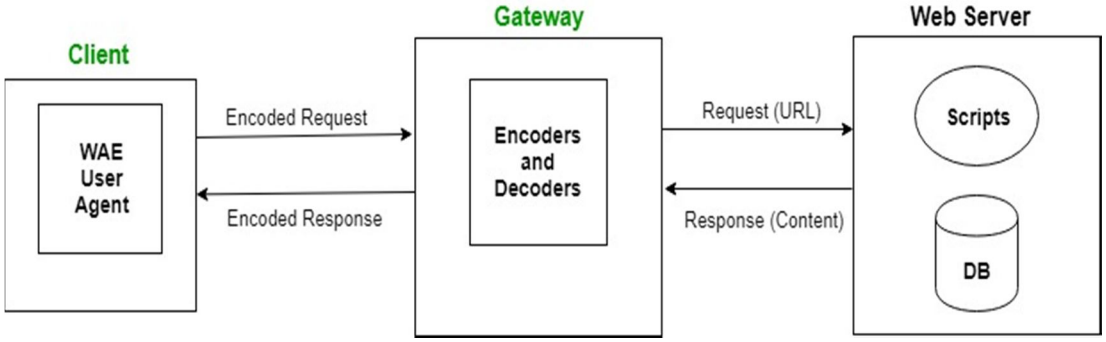
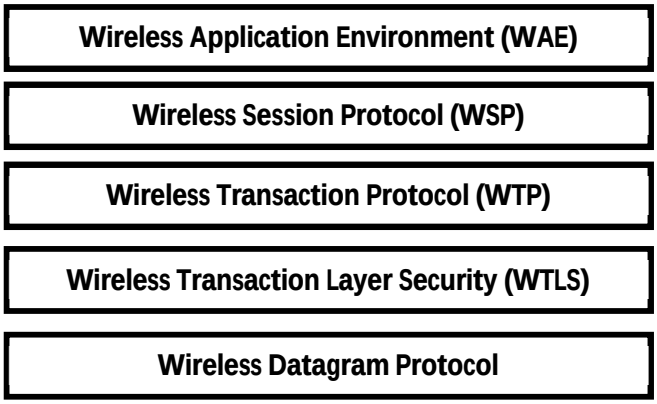


Fig. 2: Wireless Application Protocol

B. Protocol Stack



1) *WAE:* It includes standards for mobile devices and programming languages like WML for creating content.
2) *WSP:* It offers quick connections, disconnection and reconnection of connected device. .
3) *WTP:* It is a component of TCP/IP that operates on top of UDP and provides transaction support.
4) *Security Layer:* The Wireless Transaction Layer Security is present in this tier (WTLS). It provides authentication, anonymity, and data integrity.
5) *Transport Layer:* The Wireless Datagram Protocol is contained in this tier. It provides upper layers of the WAP protocol stack with a consistent data format.

IV. SECURITY THREATS AND VULNERABILITIES OF MOBILE PHONES AND COMMUNICATION

While wireless networking has a number of benefits over a conventional wired LAN, it also adds security risks that are not present in a wired LAN. Businesses using this technology must be aware of and manage the security risks associated with radio communication. Radio waves can easily spread sensitive information outside of a home or workplace because they are uncontrollable and can pass through the majority of physical barriers. If handled improperly, this could result in a significant security breach in a network.

Without using the conventional network Ethernet, one can set up a wireless network and travel anywhere within a 300-foot or greater area by using wireless access points (APs) with very little configuration. Any other Computer with a wireless network card will now be able to access the same network. Intruders can access your network without restriction if appropriate security measures are not taken. The "parking lot" attack, as given in Fig. 1, allows the attacker to reach hosts on the internal network while seated in the organization's parking lot.

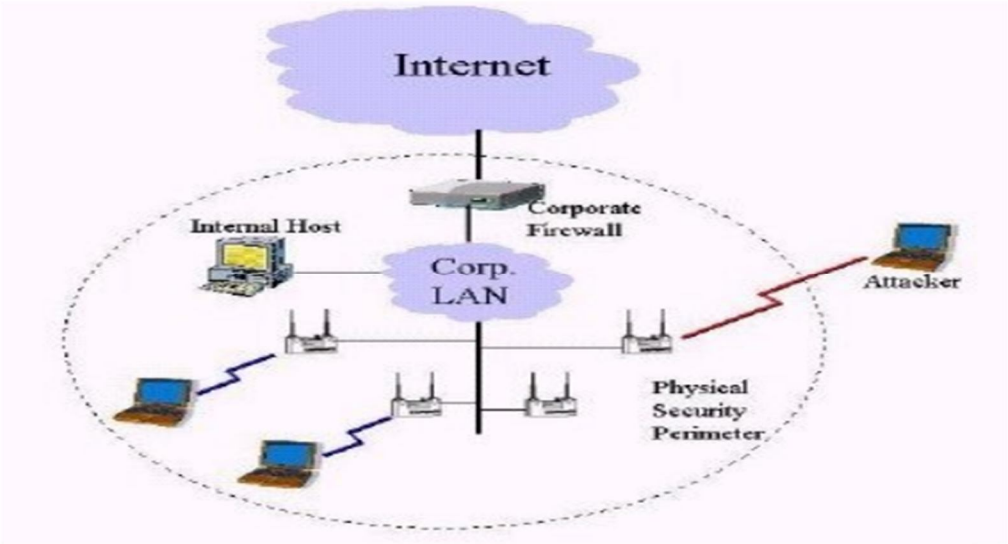


Fig 1: The Parking Lot Attack

Unsecured wireless networks essentially "open the front door" to your network, allowing intruders access to shared drives and data, the ability to sniff every network packet, the ability to read emails, the ability to access websites, the ability to capture data for later analysis, and the ability to take as long as necessary to break the rest of our system.

Following are the prominent threats and security vulnerabilities related with the mobile phones and wireless communication.

1) *Spoofing:* One of the simplest active attack types is when a hacker sets up their wireless terminal to share a MAC address with a legitimate access point or wireless terminal. When spoofing an access point, the attacker's terminal impersonates the legitimate access point in order to connect to a legitimate wifi terminal and gain access to that device's data.
   When a wireless terminal is spoofing, the attacker wants to obtain unauthorized access to the wireless network by making their terminal look like the authorized terminal.
2) *DoS Attack:* A denial of service attack stops a network in its tracks by clogging the capacity with useless data. All communications in a specific region can be shut down by continuously sending meaningless information to APs or clients. If used over a large area, this kind of attack may take a lot of power. DoS attacks on wireless networks may be challenging to halt and prevent **[4]**.
3) *Replay Attacks:* Between a wireless device and access point, the intruder watches and records packets that are sent over the air. This is accomplished using a passive surveillance tool known as a "sniffer," like Air Snort, which is easily accessible online as freeware. The infiltrator has two options after capturing the packet:

a) Transmit through the access point frequently to launch a DoS assault. The access point sends the packet to the host server, which will process it and reply with a data receipt message, because it includes valid data. If the packet is transmitted with enough regularity, the host server becomes overloaded.

b) Increase network data traffic to hasten the process of gathering enough information to decrypt a WEP encryption key.

4) *MITM (Man-in-the-Middle) Attack:* In this scenario, the intruder cleverly intercepts data as it is being transferred from one device to another. The intrusion may result in packets being dropped, replayed, modified, or even having their contents entirely altered.
5) *Eavesdropping:* Data packets can be intercepted, copied, stored, or analysed by attackers any time two (or more) computers interact over a network. Any wireless device can be modified to capture all data on a specific network channel or frequency [4].
6) *Analysis of Traffic:* The attacker gathers information by observing communication patterns in the transmissions. The messages that are sent back and forth between communicating parties hold a significant amount of information.
7) *Hardware Theft:* The physical theft of a gadget by an attacker is referred to as device theft. Giving a client a WEP key is a usual practise. By using the WEP key and MAC address of the client, the owner of the device can join the wireless LAN. The MAC address and WEP key are essentially shared by all users who use the same client. Uninvited users have access to the MAC address and WEP key when a client is taken. Administrator must update the MAC address and WEP key of every client that uses the same keys as the hijacked client after being notified by the rightful owner.
8) *Rouge and Open Access Points:* Rogue access points are those that have linked to the network without the network administrator's consent. They might be applied to enable network entry for unauthorized users. They can also be set up to function as an authorized AP to wifi client.
   Employees who want more freedom to move around at work often install rogue access points by bringing them from home and plugging them straight into the company LAN without permission. Additionally, not all employees who implement rogue access points do so with good intentions. Additionally, an attacker could set up an access point on your network and link to it at night [5].
   Since this is frequently the factory setting, many wireless networks are configured as "open," that is, without keys or authentication methods. Anyone with a wireless client can reach the Internet through such networks. In addition, the attacker has access to the network and can use its data and other resources.
9) *High Gain Antennas:* Minimal power wireless networks like the 802.11b network seem to be impenetrable to outside intruders. It has been established that this is untrue. It has been shown that an intruder can connect to an 802.11b network using high-gain antennas from up to 15 miles distant, despite the fact that the network is only intended to have a 300-foot maximum operational range.

V. MINIMIZING RISK FACTORS IN HANDHELD DEVICES AND WIRELESS COMMUNICATION

Two technological solutions, software and hardware, are used to reduce risks and aid in securing the wireless LANs. These solutions are briefly discussed below:

1) *Configuration of AP:* Access Points must be configured by network managers in accordance with established security requirements and policies. A vendor's software default setup contains a number of vulnerabilities that can be mitigated by properly configuring shared keys, SSID, Ethernet MAC Address Filtering, encryption settings, and default settings. Every WLAN device has a collection of pre-configured default settings. The network is still exposed if the security features are kept in their default positions. Hackers will be able to reach the AP by simply guessing the default IP address. It's like leaving the entrance open for a burglar when many APs are configured with "admin" as the administrative login name and without a password [6].
   The use of an SSID connected to an AP or collection of APs can be used to apply network access control. A way to "split" a wireless network into different networks served by one or more APs is made possible by the SSID. Each AP has an Identifier pre-programmed that corresponds to a particular wireless network. Client computers must be configured with the proper SSID in order to connect to this network. Depending on the level or department, a building may be divided into several networks. A client computer can typically be set up with multiple SSIDs for users who need network access from a variety of different places. The proper SSID must be presented by a client computer in order to access the AP, acting as a basic password and adding a layer of security.
2) *Software Upgrades:* When recognized software security flaws are discovered, vendors typically work to fix them. Security updates and upgrades are how these fixes are made. WiFi Protected Access (WPA) is an illustration of a software or firmware patch that that became available in late 2002. In order to increase the security of 802.11, WPA uses TKIP without the need for hardware changes.
   Although it wasn't a perfect answer, it rapidly enhanced protection for some of the WPA issues. Wi-Fi Protected Access 2 (WPA2), the second version of WPA security, was introduced by the Wi-Fi Alliance in 2004. Similar to WPA, WPA2 offers home and business Wi-Fi users a high level of assurance that their data will stay secure and that only authorized users can access their wireless networks. WPA2 requires updated hardware and encrypts data using the Advanced Encryption Standard (AES) **[7]**.
3) *Authentication:* A method for network access authentication limits access to authorized parties. Network access authentication is used to join a LAN. The system should approve the specific session after authenticating the entity. The system should ideally verify each packet after the entity has been verified and the session has been approved to prevent the session from being "hijacked" in the middle of it. Only entities with the shared key are allowed "physical" access to the network in IEEE 802.11 link layer, where WEP offers authentication services. The IEEE 802.1x standard has been accepted, and the Point-to-Point protocol, despite WEP's flaws. With this feature, mutual authentication using a RADIUS-compatible authentication server is made possible. When a client and an authentication server are mutually authenticated, a malicious AP cannot effectively persuade wireless clients of its legitimacy and force them to send traffic through it.
4) *Encryption:* If data is sent in wireless LANs without encryption, the substance of the data can also be seen. Data that has been encrypted is changed into an unreadable state that must be recovered through effort. Data should be shielded from eavesdropping assaults if encryption is used correctly.
5) *Firewalls:* Resources on public wireless networks are typically less protected than those on private networks, making them more vulnerable to assault. Personal filters provide some defense against specific attacks. Software-based personal firewalls can either be remotely or client-managed and are installed on the client's computer. Client-managed versions work best for low-end users because each user can set up the firewall independently and may not adhere to any strict security policies. Solutions that are configured and remotely managed by IT departments offer a higher level of protection than solutions that are not centrally controlled.
   Solutions that are configured and remotely managed by IT departments offer a higher level of protection than solutions that are not centrally controlled. A consistent security strategy for all remote users can be maintained and client firewalls can be modified by companies using centrally managed solutions. These premium goods some of which also have VPN and audit capabilities. Personal firewalls provide some protection, but they are not adequate to fend off highly sophisticated attacks. Agencies might still require additional layers of security depending on the security requirement.
6) *Intrusion Detection Systems (IDS):* In order to determine whether unauthorized users are trying to access the network, have already accessed it, or have compromised it, IDS watch real-time network traffic. IDS for WLANs comes in three different flavors: host-based, network-based, or mixed, which combines the best aspects of both. A piece of software called a host-based IDS (HIDS) typically keeps an eye on the system for any suspicious behavior. This entails checking system files for alterations or installing new software, drivers, or kernel tweaks [9].

On each device, a host-based agent is installed (for example, a database server). Although a host agent's main job is to record and analyze events and send alerts, in some circumstances an agent can stop an attack on a system. A network-based IDS (NIDS) that can track network traffic is deployed on the network. By comparing network data to the signatures of known attacks or by keeping an eye out for anomalies, the NIDS either keeps an eye out for suspicious behavior. When the network monitor detects packets that fit this pattern, it will take the stated action, such as terminating the network session or notifying the administrator via email.

One advantage of NIDS over HIDS is that a single NIDS sensor can keep an eye on a network with numerous hosts, making IDS installation and setup simpler. Some HIDS have the potential to significantly reduce the hot operating system's efficiency. NIDS can be installed throughout the network, unlike HIDS, to identify all traffic on a segment. It may be situated in front or behind a firewall, in the middle of an organization's and a partner network, in the network's backdrop, with important servers, a remote access server, or as the backbone of a wireless LAN **[**10].

7) *VPN:* The ability to send data safely between two network devices over an insecure data transport medium is made possible by VPN technology. The Internet is frequently used to connect distant computers or networks to a business server. But it's also the best option for cellular network data security. VPNs operate by building a tunnel over a system, like IP, to transmit data. The tunnel's traffic is completely separated and encrypted**.** Three layers of security, including user authentication, encryption, and data authentication, are offered by VPN technology:

a) Only authorized users are able to connect to, transmit, and receive data over a wireless network thanks to authentication.

b) More security is provided by encryption because it makes sure that even if a communication is intercepted, it would be difficult to decode it.

c) Data integrity is guaranteed over wireless networks by data authentication, which also guarantees that only authenticated devices can transmit data.

Combining VPN with other security features can increase its advantages. The fourth chapter will go into more depth about VPN technology.

8) *Smart Card:* Smart cards might provide an additional layer of security. Smart cards offer the additional feature of authentication in wireless networks. In environments requiring authentication that goes beyond a username and password, smart cards are useful. Users typically only need to recall a PIN number when accessing user certificates and other information that is stored on the cards themselves. Because smart cards are portable, users can safely access their networks from different places.

9) *Biometric:* Optical scanners, such as retina and iris scanners, facial recognition scanners, and speech recognition scanners are examples of biometric devices. They also include fingerprint and palm print scanners. When used either by themselves or in conjunction with another security measure, biometrics offer an extra layer of security.

10) *PKI:* Public key certificates can be created, produced, distributed, controlled, and recorded using PKI's infrastructure and services. It gives applications with secure encryption and authentication of \network interactions as well as data integrity and non repudiation, using \public key certificates to do so. PKI can be integrated into WLANs for network security and identification. For instance, third-party producers offer wireless PKI, mobile devices, and smart IDs that work with WLANs.

Users needing high security levels ought to seriously consider PKI. It offers strong authentication through user certificates, which can be \sused with application-level security, to sign and encrypt communications. Given that the credentials are built into the card, smart cards are even more useful. Both a token and a secure (tamper-resistant) method of keeping cryptographic credentials are provided by smart cards. On the other hand, users who require lower levels of security should closely consider the difficulty and expense of setting up and maintaining a PKI before implementing this solution.

VI. CONCLUSION

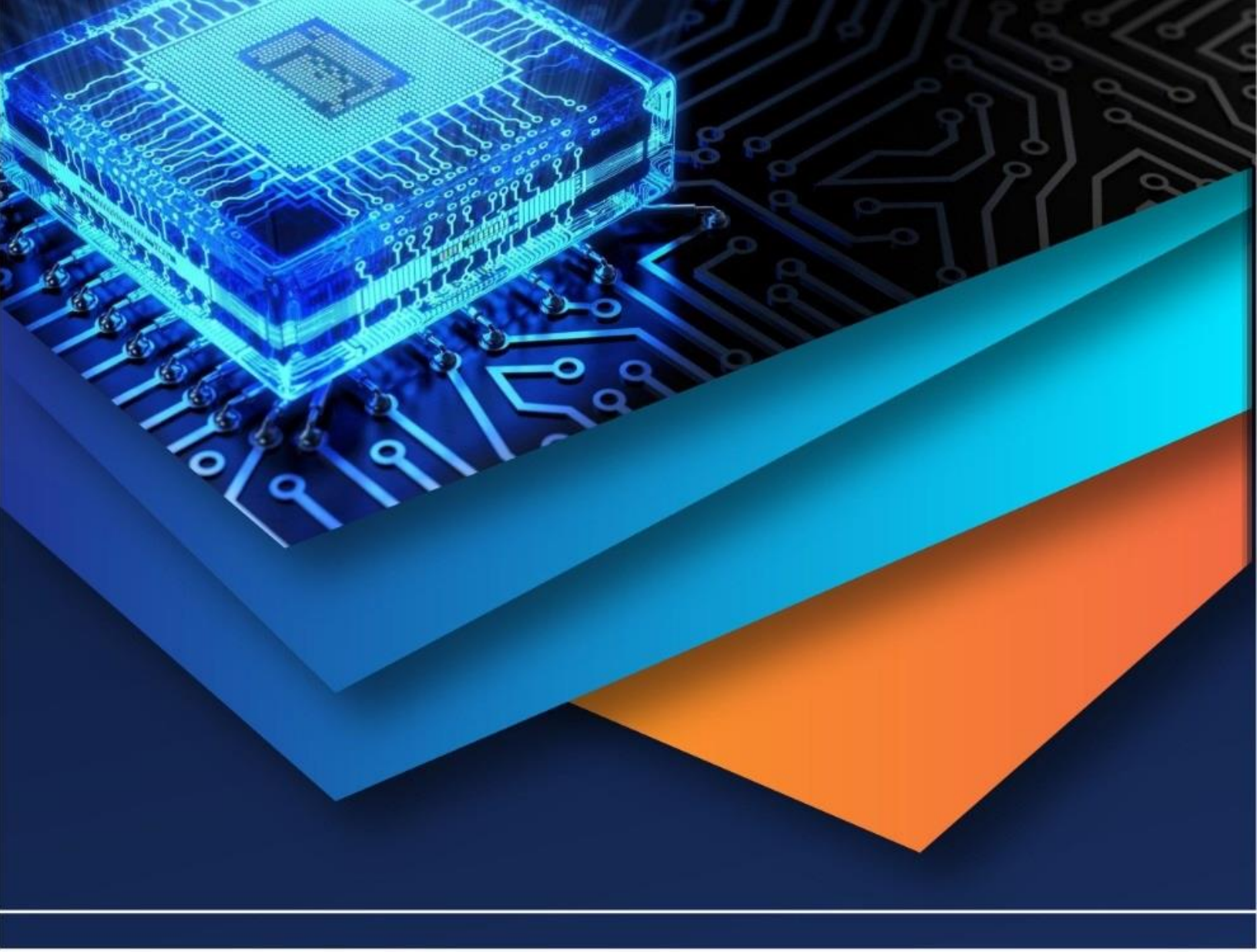
By removing the restriction of physical connections to networks, wireless technologies allow freedom of mobility for users and easy access to the Internet virtually from anywhere. In addition to these benefits, the intrinsic broadcast nature of wireless networks has sparked security concerns because when data is exchanged over the air, anyone with radio access equipment can more easily intercept and eavesdrop. As a result, security services offered by security protocols must be implemented.

At various network levels, current security protocols offer security features. For instance, the first protocol to be examined for a wireless network is Wired Equivalent Privacy (WEP), which operates at the link layer but has been found to have significant security flaws. The WPA standard, which also operates at the link layer and offers port-based access control for wireless devices, was created to address WEP's flaws. Extensible Authentication Protocol (EAP), which is used as a transport method, is also utilized by EAP.

At the network layer, we take into account the IP Security (IPsec) protocol suite, which was initially developed for wired networks but is now also taken into account for cellular networks due to its robust authentication and encryption techniques. The most frequently used security protocol on the Internet today is Secure Sockets Layer (SSL), a transport layer standard.

REFERENCES

[1] http://ftp.vub.ac.be/~sijansse/2e%20lic/BT/Voorstudie/ PreliminaryStudy.pdf
[2] Gartner's website. Contents publically available at: www.gartner.com
[3] Raj Kumar Patel, Dr. Lalan Kumar Singh , Dr. Narendra Kumar."Literature Review of Distributed: Denial of Service Attack Protection ", Volume 11, Issue I, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 1032-1036, ISSN : 2321-9653, www.ijraset.com
[4] http://www.cs.umd.edu/~waa/wireless.pdf
[5] Dr. Peikari C., Fogie S. (2003) Maximum Wireless Security. An Insider's Guide to Protecting Your Wireless Network, Macmillan Computer Publication.
[6] http://www.bit.tekotago.ac.nz/staticdata/papers04/linsecurity.pdf.
[7] NIST-FIPS (2001), Announcing the Advanced Encryption Standard(AES), Publication no: 197.
[8] Daemen J., Rijmen V., The Block Cipher Rijndael, Lecture Notes in Computer Science, Volume 1820, Springer-Verlag.
[9] Kiran Bala, Narendra Kumar, Ashok Kumar Singh (2018), Performance Evaluation of Advanced Intrusion Detection System, pp, 10-15.
[10] Carter B. , Shumway R. (2002), Wireless Security End To End.Johnwiley & Sous, Inc.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY