iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76198

Prevention of ARP Spoofing in WLAN

Balamurugan Aathavan
VIT University

Abstract: In this day and age, keeping up the security of data is an absolute necessity. These days WLAN has turned into the most widely recognized and mainstream arrange area. Network domains are constantly inclined to various system attacks. Among the expanding number of system assaults, ARP spoofing attack is a standout amongst the most perilous technique in the neighborhood. ARP is a stateless protocol and ARP Spoofing happens for the most part in view of the nonappearance of any system of checking the identity of the sending host. It has been seen that the greater part of the WLAN attacks results from ARP Spoofing. So avoidance, identification, and the decrease of this issue can stop the number of system attacks. This work talks about the avoidance of ARP ridiculing assault and some related deals with it.

I. INTRODUCTION

Each client accessing the internet in a wireless network posses two different addresses called hardware address (MAC address) and the IP address. The packets are encased into frames and are delivered across the links based on hardware addresses. ARP protocol is used to develop a linkage between the IP address and consequent MAC address. Whenever any device on a subnet wishes to exchange data with other device, first of all ARP cache of the sending device is checked. If the MAC address of the receiving node is found present in the ARP cache, that address is utilised for sending the data through. However, if the address is not there in the local cache, an ARP request is broadcasted on the network enquiring which machine has the required IP address. Each receiving client machine compares the IP address in the received ARP packet to its own IP address. Those client machines whose IP address do not match with the required IP in the ARP packet dispose the packet off without any further action. The device for which the required IP address in ARP packet matches with own IP address, an ARP reply message is composed. The destination device sends a unicast ARP reply containing its IP and MAC address back to the sender. The source machine in turn processes the ARP reply and updates itself with the required MAC address and IP address it receives from the reply message. The major drawback of ARP is that there is no foolproof mechanism for validating ARP replies in the network. The reply packets are always at a risk of being spoofed by some malicious hosts on the same subnet. The method of association of MAC address of one client with the IP address of another client is known as ARP Spoofing. An extensive survey, thus has been conducted on the different detection and mitigation strategies.

II. LITERATURE SURVEY

1) *Geo jinhua et.al ARP spoofing Detection Algorithm Using ICMP Protocol [1]*

In this paper, the authors discussed about ARP spoofing attacks and their violation in present technologies. They proposed an efficient algorithm based on ICMP protocol to detect malicious hosts that are performing ARP spoofing attack. The technique includes collecting and analysing the ARP packets, and then injecting ICMP echo request packets to probe for malicious host according to its response packets. It won't disturb the activities of the hosts on the network. They mentioned that it can also detect the real address mappings during an attack.

They divided ARP spoofing in to following modules:

a) *ARP Packet Sniffer Module*: This module sniffs all ARP packets from the Ethernet.
b) *Invalid Packet Detection Module*: This module classifies the ARP packets into valid and invalid packets in two steps. If there are any invalid packets turning up, it will be guaranteed that an ARP attack is occurring. All the new IP-MAC mappings are sent to the next module for in-depth analysis.
c) *ARP Spoofing Detection Module:* This is the main detection module. We feed the new valid packets into it as input.
d) *IP-MAC Mapping Database:* IP-MAC mappings proved to be valid will be added into the database.
e) *Response Module*: This module is used to alert the administrator the happening of ARP spoofing attack, automatically create and send repaired ARP packets to the victim, and deny the hosts that identified as malicious hosts by creating and sending ARP packets with random MAC address to the attacker.

2) *Saini, R. R. et al. A security framework against ARP spoofing. [2]*

In this paper, the authors discussed about ARP spoofing. Address resolution protocol is used at network layer in an OSI for mapping logical address that is also known as IP address to physical address that is known as MAC address in a local area network. ARP spoofing is dangerous attack because in this an attacker can sniff the data of the victims and prevent the victim to use the internet resource. The thing that ARP spoofing can do is either it can be performed by the software or command prompt. Software is easy to use for any kind of user on just snap of finger a user can use the software because it is really easy and have only 4 to 5 steps to perform the attack.

3) *Pandey, P. Prevention of ARP Spoofing: A Probe Packet Based Technique [3]*

In this paper the author discussed about Prevention of ARP spoofing. The Address resolution protocol is a data link layer protocol, which resolves any given logical address to its corresponding physical address. In a network, if a host wants to communicate with another host then it must know the IP and MAC address of destination/receiving host. In case, when sending node knows IP address of the receiving host but doesn't know the MAC address then the sending node broadcast a query in the form of ARP request packet. Number of techniques have been proposed till now to circumvent the problem of ARP spoofing. All the approaches proposed in this direction can be categorized as follows:

a) Cryptographic approaches
b) Non-cryptographic approaches

Cryptographic approaches use concept of cryptography so it modifies the standard ARP to some extent therefore it interferes with the standard layering architecture of network. Non-cryptographic approaches don't use the concept of cryptography and hence processing time of these is less SDE doesn't stand correctly for the strong attacker or intermediate attacker. Now in proposed technique they can easily detect the weak as well as strong attacker and we saw increment development of E-SDE. This technique is backward compatible so it can be easily implemented in LAN, there is no requirement to update all the host in the LAN.

4) *Kang, H. S. et al. Defence Technique against Spoofing Attacks using Reliable ARP Table in Cloud Computing Environment. [4]*

Authors of this paper mentioned that cloud service was introduced in many enterprises in order to achieve efficiency, reduction in cost and revolution in business process. Spoofing or poison attacks on VM inside the cloud cause the deterioration of cloud system and those attacks can make the huddle for spreading the cloud services. Many researches are now under way to solve such problems but most of these seem to be passive and limited in terms of detecting attacks and applying to large scale of networks. They proposed a method to defence the spoofing attacks. They used reliable ARP to make cloud computing more reliable. There are two main parts in the proposed technique, one for creation and management of the ARP tables and the other for ARP Reply Message handling called Comparison Handler. They used keystone authentication service provided by Open stack itself so there is no need for any additional equipment. Limitation of the proposed technique is one of the most important thing in cloud computing system that is resource management but it is the fact that there is partial loss of resources to maintain Comparison Handler and the table.

5) *Sharma, D. et al. Detection of ARP Spoofing: A Command Line Execution Method [5]*

In this paper, the authors used command line execution method to detect ARP spoofing. In the proposed work they detected ARP-Spoofing occurring in the local subnet.

Following are the steps followed in order to detect ARP- Spoofing:

- User logs on to window and establishes the network connection, after he establishes the connection.
- An interface box appears in which he has to input the network path.
- After he inputs the network path a file name of its allocated IP address containing a genuine mac address is stored in the provided network path.
- When a hacker tries to change mac address and performs ARP-Spoofing by changing the mac address of the system.
- The network administrator can easily check for the mismatched mac address occurring in his subnet by inputting the IP address corresponding and the network path where the genuine mac address was stored. Hence the ARP-Spoofing was detected.

6) *Yong Wu et al. ARP Spoofing Based Access Control for DLNA Devices[6]*

In this paper, the authors have discussed about access control for DLNA devices. Various kinds of Internet- enabled devices have been developed.

The dissemination of such smart devices has increased the use and exchange of multimedia contents, leading to the need for easy media sharing and seamless contents access. Several technological solutions have been developed to meet this demand, among which one of the most popular for the home networking environment is DLNA. The main objective of DLNA certified devices is to establish an infrastructure to provide a seamless environment for sharing digital media and content services. DLNA aims to build an interoperable network that can manage personal computers, consumer electronics and mobile electronic devices throughout home in a centralized manner, and to create a novel seamless environment of sharing and developing digital media and content services.
The ARP is used by Internet Protocol to bind the IP addresses to the MAC addresses used by the link layer in a LAN environment. When a host wants to communicate with another host over the network, the IP address of destination host is used. Communication between two nodes over link layer is possible through the exchange of MAC addresses once the DACS connects to the network, it will search for devices and terminals in the LAN. The user shall specify the target devices that need to be protected from unwanted access and the policies of each terminal access to each target devices the proposed technique cause high impact to users. To

7) *Jitpukdebodin et al. A Novel Web Content guarantee that the proposed technique works in a real Spoofing Technique on WLAN and Its Coun- world scenario, they developed a prototype and per-termeasures [7] formed an analysis to demonstrate that the proposed technique cannot be detected by a general IDS with cur-*

In this paper they implemented spoofing tech- rent signature database at a time of writing the paper. nique on WLAN. WLANs have several security They successfully detected attacks on WLAN using two standards, such as Wired Equivalent Privacy detection modes.
(WEP), Wireless Protected Access (WPA), Wireless
They are:
Protected Access 2 (WPA2), etc. However, they are 1. Signature-Based detection not sufficient to prevent attackers. This is because 2. Anomaly-Based detection each security standard has inherent vulnerabilities. They found that current countermeasures of WLAN They explored a new attacking technique that uti- are not sufficient. So they introduced a new technique lizes a flaw in WLAN. They proposed a technique that explores vulnerability in WLAN communications. that works in a real world scenario using HTTP traffic from users in public WLAN. The results of

TABLE I
TECHNIQUES AND DRAWBACKS

S. No	Title	Author(s)	Methods and techniques	Drawbacks
1.	ARP spoofing Detection Algorithm Using ICMP Protocol [1]	G Jinhua, X Kejian	ICMP protocol, packet detection modules, spoofing detection modules	Packet injection is fairly minimal and the performance of the network will not be influenced.
2.	A security framework against ARP spoofing. [2]	Saini, R. R., & Gupta, H.	Binding logical address to physical address	Performance and cost
3.	Prevention of ARP Spoofing: A Probe Packet Based Technique [3]	Pandey, P.	Probe packet based technique	SDE doesn’t sand for strong attacker

4.	Defence Technique against Spoofing Attacks using Reliable ARP Table in Cloud Computing Environment. [4]	Kang, H. S., Son, J. H., & Hong, C. S.	Keystone authentication service by Open stack	Partial loss of resources
5.	Detection of ARP Spoofing: A Command Line Execution Method [5]	Sharma, D., Khan, O., & Manchanda, N.	1. Network security enhancement 2. Works with dynamic IP Addresses 3. No network congestion	DOS attack
6.	ARP Spoofing Based Access Control for DLNA Devices[6]	Wu, Y., &Zhi, X.	Access control methods of DLNA	Treats device as a Single access unit.
7.	A Novel Web Content Spoofing Technique on WLAN and its countermeasures [7]	Jitpukdebodin, S., Chokngamwong, R., & Kungpisdan, S.	1. Signature based Detection 2. Anomaly based Detection	Countermeasures are not sufficient.

III. PROPSOED APPROACH

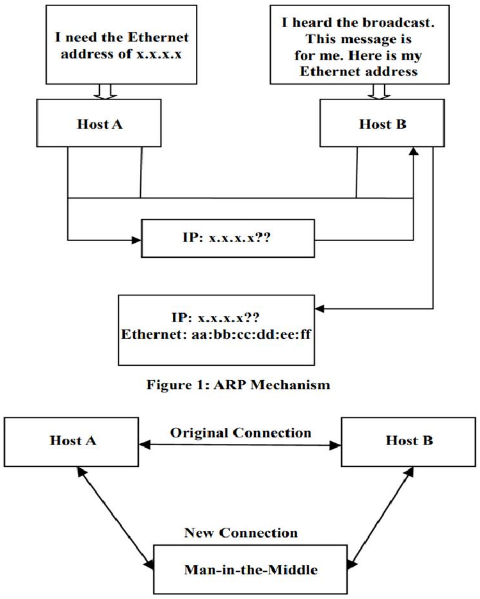

I need the Ethernet address of x.x.x.x
I heard the broadcast. This message is for me. Here is my Ethernet address
Host A
Host B
IP: x.x.x.x??
IP: x.x.x.x?? Ethernet: aa:bb:cc:dd:ee:ff
Host A
Original Connection
Host B
New Connection
Man-in-the-Middle

Figure 1: ARP Mechanism

Figure 2: Scenario of ARP Poisoning

Figure 1: Scenario of ARP Spoofing

In this technique, as presented in the figure 1 receiver takes its own IP and MAC locations and after that utilizations secure hash work SHA-512, to deliver a hash esteem. In this manner scrambles the hash code utilizing its key, making a computerized signature. Receiver sends the ARP REPLY message alongside the mark. Sender create the hash code utilizing collector's IP and MAC addresses and unscrambles the mark utilizing beneficiary's critical. In the event that both produced hash codes are same, it implies no modification has been finished amid transmission. This guarantees authenticity and integrity.

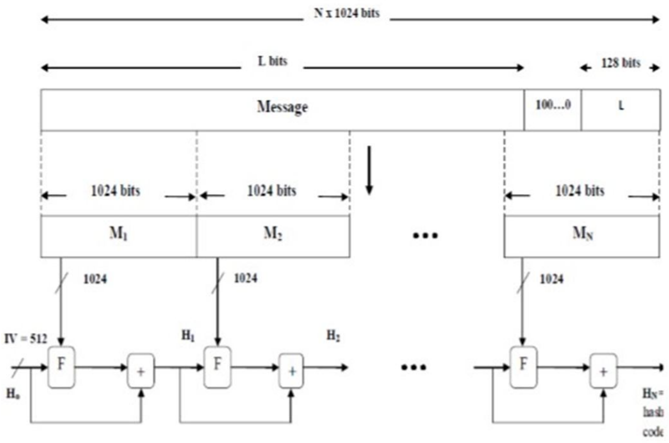


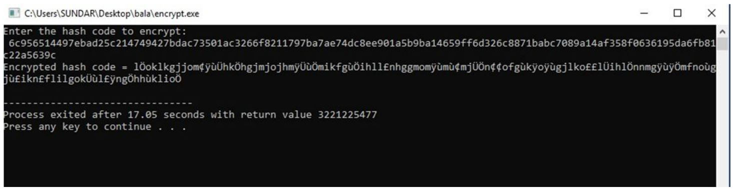
Figure 2: Generation of hash code

Hash work changes a variable length message into a settled length yield. To guarantee uprightness of the message hash calculations are utilized. The protected hash calculation utilized as a part of the proposed approach is SHA512 on the grounds that it is sufficient secure and harder to split. The calculation takes a message (with a greatest length of under 2128 bits) as info and produces 512-bits message process as yield. The input is isolated into 1024piece obstructs for preparing. This is shown in figure2

IV. IMPLEMENTATION AND RESULT

Suppose the receiver's IP address is <192.154.63.4,>. This is input message to the hash algorithm.
The initialization of the eight buffers in hexadecimal is given below:
a = 0x7a02e633f3bcc108ULL; b= 0xba68ae8584caa33bULL; c= 0x5c6eb372fe94f72bULL; d= 0xa54ff53a5f1d36f1ULL; e = 0xa10e427fade685d1ULL; f= 0xab05666c2b3e6c1fULL; g = 0xbf83b9abfb41bd6bULL; h = 0x7be0ad19137e2179ULL;

This hash code along with the IP address is encrypted and sent to the sender

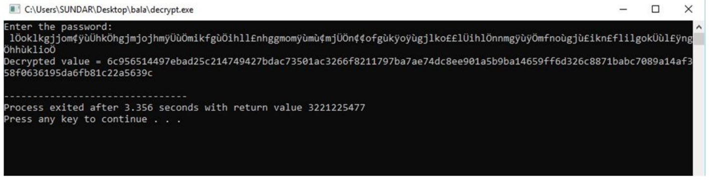


```
Enter the hash code to encrypt:
 6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871babc7089a14af358f0636195da6fb81
c22a5639c
Encrypted hash code = lÖoklkgjjom¢ÿùÜhkÖhgjmjojhmÿÜùÖmikfgùÖihll£nhggmomÿùmù¢mjÜÖn¢¢ofgùkÿoÿùgjlko££lÜihlÖnnmgÿùÿÖmfnoùg
jù£ikn£flilgokÜùl£ÿngÖhhùklioÖ

--------------------------------
Process exited after 17.05 seconds with return value 3221225477
Press any key to continue . . .
```

Figure 3: encryption of the hash code

This when sent to the sender , is first decrypted to check the hash code for the former to send the message to the actual receiver.

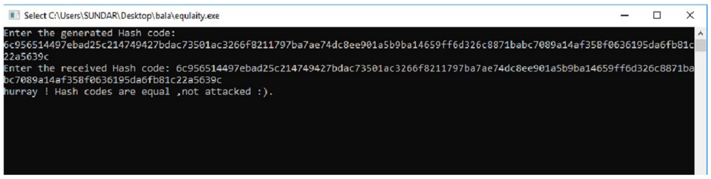


```
Enter the password:
 lÖoklkgjjom¢ÿùÜhkÖhgjmjojhmÿÜùÖmikfgùÖihll£nhggmomÿùmù¢mjÜÖn¢¢ofgùkÿoÿùgjlko££lÜihlÖnnmgÿùÿÖmfnoùgjù£ikn£flilgokÜùl£ÿng
ÖhhùklioÖ
Decrypted value = 6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871babc7089a14af3
58f0636195da6fb81c22a5639c

--------------------------------
Process exited after 3.356 seconds with return value 3221225477
Press any key to continue . . .
```

Figure 4: decryption of the hash code

The verification of the hash code has two cases, CASE I: If no alteration has been done during transmission by an attacker.



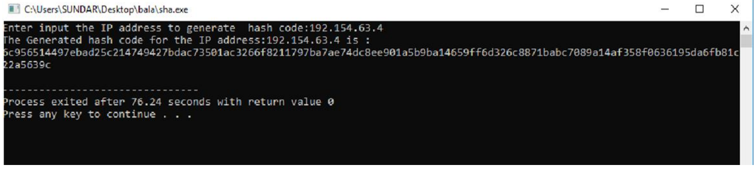
```
Enter the generated Hash code:
6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871babc7089a14af358f0636195da6fb81c
22a5639c
Enter the received Hash code: 6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871ba
bc7089a14af358f0636195da6fb81c22a5639c
hurray ! Hash codes are equal ,not attacked :).
```

Figure 5: no presence of attacker

Then sender compares both these generated hash codes. These two are same, this assures the message is in original form as send by receiver

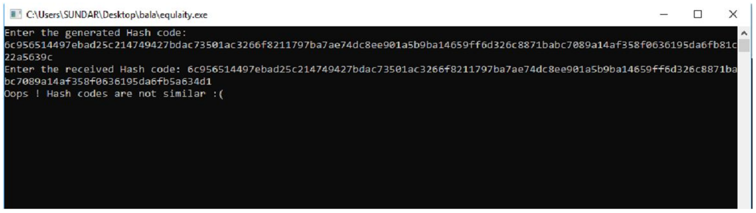
CASE II: If alteration has been done during transmission by an attacker.

The hash value of the receivers IP address is generated.



```
Enter input the IP address to generate  hash code:192.154.63.4
The Generated hash code for the IP address:192.154.63.4 is :
6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871babc7089a14af358f0636195da6fb81c
22a5639c

--------------------------------
Process exited after 76.24 seconds with return value 0
Press any key to continue . . .
```



```
Enter the generated Hash code:
6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871babc7089a14af358f0636195da6fb81c
22a5639c
Enter the received Hash code: 6c956514497ebad25c214749427bdac73501ac3266f8211797ba7ae74dc8ee901a5b9ba14659ff6d326c8871ba
bc7089a14af358f0636195da6fb5a634d1
Oops ! Hash codes are not similar :(
```

Figure 6: Presence of an attacker due to the change in the hash value.

The sender compares both hash codes and he/she finds both are different. This assures that the message is not authentic.

V. CONCLUSION

Amid the previous quite a long while, the establishment of remote WLAN in military and association is colossally expanding. ARP spoofing is regular attack in WLAN even after preventing rogue access point. The above talked about papers propose various practical techniques to identify and anticipate ARP mocking. These proposed arrangements anticipate ARP spoofing. SHA-512 followed by encryption provided authentication and confidentiality to the sent IP and MAC address which makes sure that there is no attack. Maybe a couple of these procedures can likewise be stretched out to other parodying assaults.

REFERENCES

[1] Jinhua, G., &Kejian, X. (2013). *ARP spoofing detection algorithm using ICMP protocol*. In International Conference on Computer Communication and Informatics 2013.

[2] Saini, R. R., & Gupta, H. (2015, September). *A security framework against ARP spoofing*. In Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions),2015 4th International Conference on (pp. 1-6). IEEE.

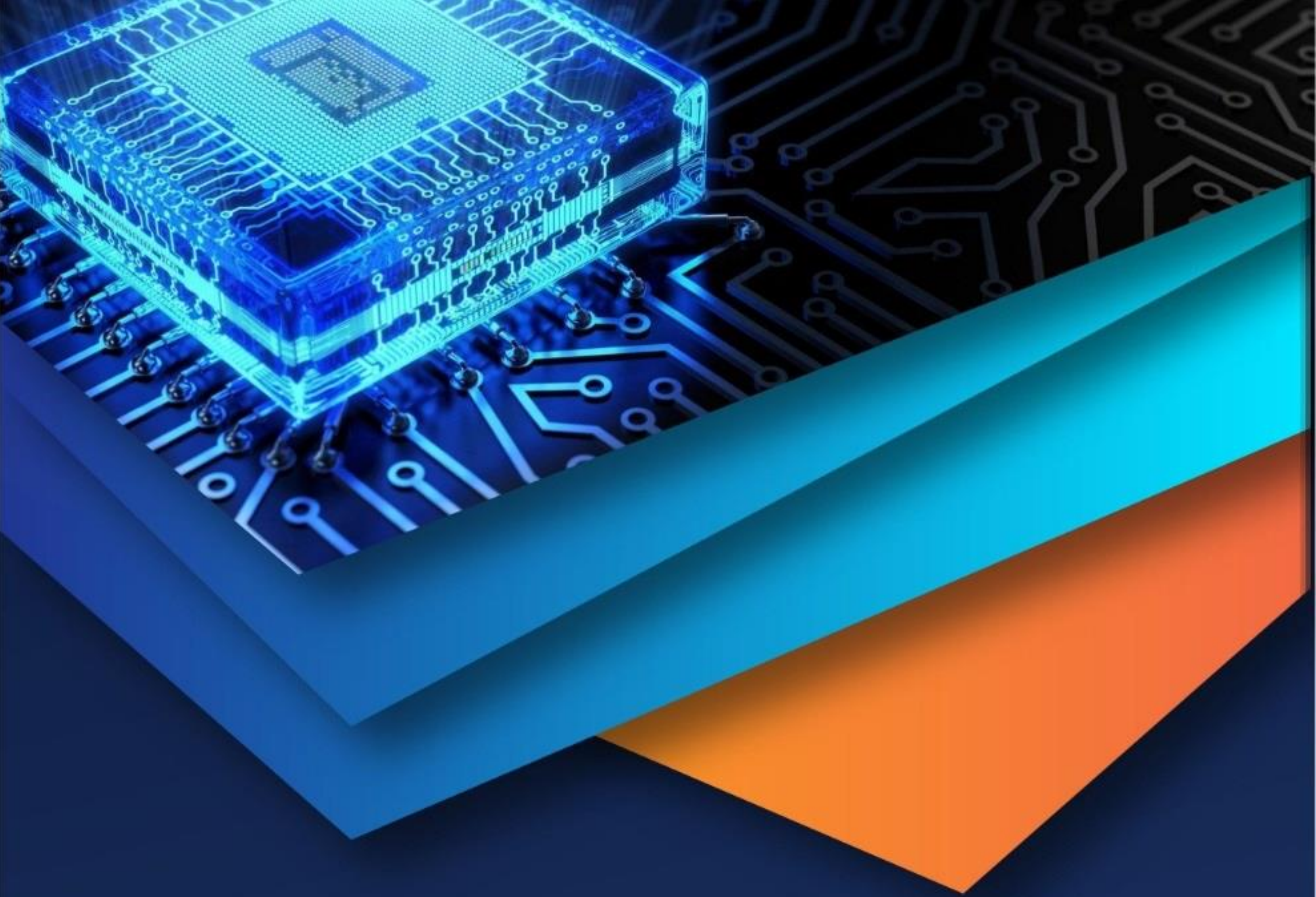
[3] Pandey, P. (2013, February). *Prevention of ARP spoofing: A probe packet-based technique*. In Advance Computing Conference (IACC), 2013 IEEE 3rd International (pp. 147-153). IEEE.

[4] Kang, H. S., Son, J. H., & Hong, C. S. (2015, August*). Defence technique against spoofing attacks using reliable ARP table in cloud computing environment*. In Network Operations and Management Symposium (APNOMS), 2015 17th Asia-Pacific (pp. 592-595). IEEE.

[5] Sharma, D., Khan, O., &Manchanda, N. (2014, March). *Detection of ARP Spoofing: A command line execution method*. In Computing for SustainableGlobalDevelopment (INDIACom), 2014 International Conference on (pp. 861-864). IEEE.

[6] Wu, Y., & Zhi, X. (2015, August). *ARP Spoofing Based Access Control for DLNA Devices*. In Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UICATC-ScalCom), 2015 IEEE 12th Intl Con(pp. 1371-1376). IEEE.

[7] Jitpukdebodin, S., Chokngamwong, R., &Kungpisdan, S. (2014, September). *A novel web content spoofing technique on WLAN and its countermeasures. In Communications and Information Technologies (ISCIT), 2014 14th International Symposium on (pp. 254-258). IEEE.*



INDEX COPERNICUS

10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY