iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4358

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: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Secure Wi-Fi Network (WLAN) using Proxy Server and Encryption Algorithms

Yogesh Singh Senger[1], Rahul Saini[2]
[1, 2]*National Institute of Technology Kurukshetra, National Institute of Technology Kurukshetra*

Abstract: ***Now a day's Wireless systems are extremely popular and the reason behind that is ease to usage of Wi-Fi. Inside 20 meter of a proximity anybody can connect to any wireless gadget with no need of wire but it also leads to increase in security are also increasing. Many techniques are available to secure Wi-Fi network like usage of strong passwords, Usage of good wireless encryption algorithm and shutdown the network. Many encryption algorithm are used to secure wife network like WEP (Wired Equivalent privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access) but encryption algorithm can be easily decrypt by the brute force attack. In this paper we are discussing about how to secure our Wi-Fi network.***
Keywords: WEP, WPA,WPA2, AES, Proxy Server

I. INTRODUCTION

Wi-Fi is the name of a mainstream wireless networking technology that utilizations radio waves to give wireless fast internet[1][5]. Wireless innovation is the best powerful, high portability go-to network in the quickly changing technological world. Expanding data transfer capacity, opportunity and adaptability of the specialized technique is making it the best correspondence foundation by decision[7]. The wireless innovation gives the capacity to lead business at wherever and with any person, where correspondence component is set up. The system is falling under to a pyramid high to low (Core layer, Distribution layer and Access Layer).[7]

The customer's availability to the system is done through the entrance layer and Wireless network connectivity additionally falls under to this classification. Extensive scale associations secure that the pyramid design is appropriately settled and dependably keep up the engineering due to the multifaceted nature will increment of the system. The core layers are firmly combined with security countermeasures, for example, edge firewalls, gatecrasher counteractive action frameworks. Despite the fact that the counter measures can keep away from aggressors who are attempting to enter the substantial scale association structure from other web availability techniques, for example, wired, in Wi-Fi availability customers can be a danger as the customers are progressively changing with expanding number of set up associations in the systems' inward access layer gadgets are not which is static. Which make this availability strategy more defenceless that is a fundamental disadvantage to this high scale association and considering about systems administration entire as a hypothesis. WPA/WPA2 are the most regularly utilized Wi-Fi Connection conventions and the greater part of the modern switches which underpins Wi-Fi, take after these connection foundation conventions to build up an connection[7].

II. METHOD OF SECURING WI-FI AND PROTECT OURSELVES

Here two types of securing methods are given below-

A. Compulsory and Sensible controls:

1) Change Usual Passwords and Usernames.
2) Go to the WPA / WEP Encryption option and turn on.
3) Validate Firewalls On every Computer and the Router.

4) Deactivate Auto-connect property.
5) Position the Router or Access Point (AP) Safely.
6) Switch of the power switch of Router/AP, when not in use.
7) Allot Static IP Addresses to Devices.
8) Change the usual SSID
9) Deactivate SSID Broadcast
10) Validate MAC Address Filtering

B. Encryption Algorithms

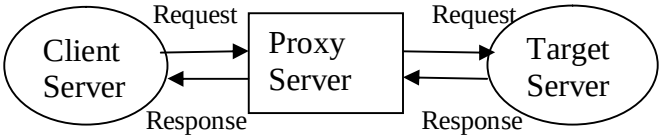
There are many methods available for the Wi-Fi security, many encryption schemes such as WEP, AES, WPA, WPA2 etc and many security tips are developed.

III. SCOPE OF STUDY

Proxy Server**:** Proxy server is a computer that acts as an intermediary between the computer you use and the Internet. It masks the IP address of your machine with the IP address of the proxy. It is designed to provide business networks with additional security and privacy benefits[3].

Usage of proxy server:

A. Proxy server protects identity form another party and obscure the client IP address.
B. It blocks malicious traffic.
C. It helps to block sites.
D. To stay anonymous over the network.



Client server send the request to the proxy server and proxy server send it to target server, and target response to the proxy server not the client server because of security purpose. Target server doesn't know about the real IP address. Then, proxy server response to the client.

Types of proxy server

1) *Forward proxy:* A proxy server is server which acts as a intermediate between client and the server[6][8]. The client sent its request to the proxy server to connect the server to which the client wishes to communicate. The proxy server forward client request to the server but using its own credentials. That is, it does not show the IP address of the client to the server. For the server, request came from the proxy server further it doesn't know anything about the client side. All it knows that some machine ask for a page which is bring hosted on the server and its serve the request to the proxy server . This type of proxy also called forward proxy. It might happen that the client is not able to directly connect to the server may be because of server block the client IP address or may be some restriction to on the client side. So, client use the forward proxy[3][4].
2) *Reverse proxy:* It's a complete opposite to the forward proxy server would be a reverse proxy server. A Reverse proxy server works the same way as a forward proxy server but it works on the behalf of the server not client. The client doesn't know the that its request is being forward to some other server by the reverse proxy server. Based on the request at which website client is trying to access the proxy server would forward client request to that server [3][4].
3) *Open proxy:* An open proxy is a proxy server that is accessible by any Internet user[3][8]. A proxy server allows to the user to store and forward internet services within a network group (LAN, MAN, WAN).

IV. ENCRYPTION ALGORITHMS

A. WEP protocol

WEP stands for Wired Equivalent Privacy. WEP is only algorithm mentioned in IEEE 802.11-1999 standard. WEP uses Stream Cipher RC4 for confidentiality and CRC for integrity. The actual encryption will be done by stream cipher RC4 and the maintaining

the integrity of the massage CRC 32 will be use. WEP is completely broken this time and it is deprecated from wireless security measures but still lots of devices in the market which support the WEP as an encryption algorithm.
For WEP-64-bit the key size is 40 bit (sometimes called WEP-40) and for WEP 128-bit the key size is 104 (sometimes called WEP-104)[6][8].

B. WPA protocol

WPA means Wi-Fi Protected Access. WPA was designed by Wi-Fi alliance in conjunction with IEEE.WPA is optimized version of WEP. WPA is replacement of WEP because which all the devices that support the WEP also support the WPA.WPA uses the Temporal Key Integrity Protocol (TKIP). Broadcast key rotation (BKR).Dynamic key rotation. Message integrity code (MIC). WPA is, every time it's going to change key for its client with the help of dynamic key rotation. In such a way that every time the TKIP key encryption uses a higher and it is safe[6][8].

C. WPA2 protocol

The 802.11i wireless security standard based protocol was introduced in 2004. This is upgration of WPA. The improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES). It uses counter mode with cipher block and chaining message authentication protocol (CCMP) for encryption and uses standard IEEE 802.1 x/EAP. Till now this is the highest security in Wi-Fi security. It is unbreakable till now. The possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too. And even though breaking into a WPA/WPA2 secured network through this hole will take anywhere around 2 to 14 hours it is still a real security issue and WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector[6][8].
Wpa2 technology that is based on four factors:

1) Or mutual authentication (mutual authentication)
2) Strong encryption (strong encryption) or
3) Interoperability (Interoperability)
4) Ease of Use, or (Ease of use)

D. AES Protocol

AES is a more secure encryption protocol introduced with WPA2. AES isn't some creaky standard developed specifically for Wi-Fi networks, either. It's a serious worldwide encryption standard that's even been adopted by the US government. For example, when you encrypt a hard drive with True Crypt, it can use AES encryption for that. AES is generally considered quite secure, and the main weaknesses would be brute-force attacks (prevented by using a strong passphrase) and security weaknesses in other aspects of WPA2[6][8].

V. FUTURE WORK

The anticipated solution for huge scale associations to secure access layer Wi-Fi associated gadgets are conveying through the association IP-VPN. We are studying various encryption techniques We are going to increase the performance of AES and fix the bugs of AES encryption algorithm. We are also working of proxy server. We can also secure our Wi-Fi network via proxy server.

VI. CONCLUSION

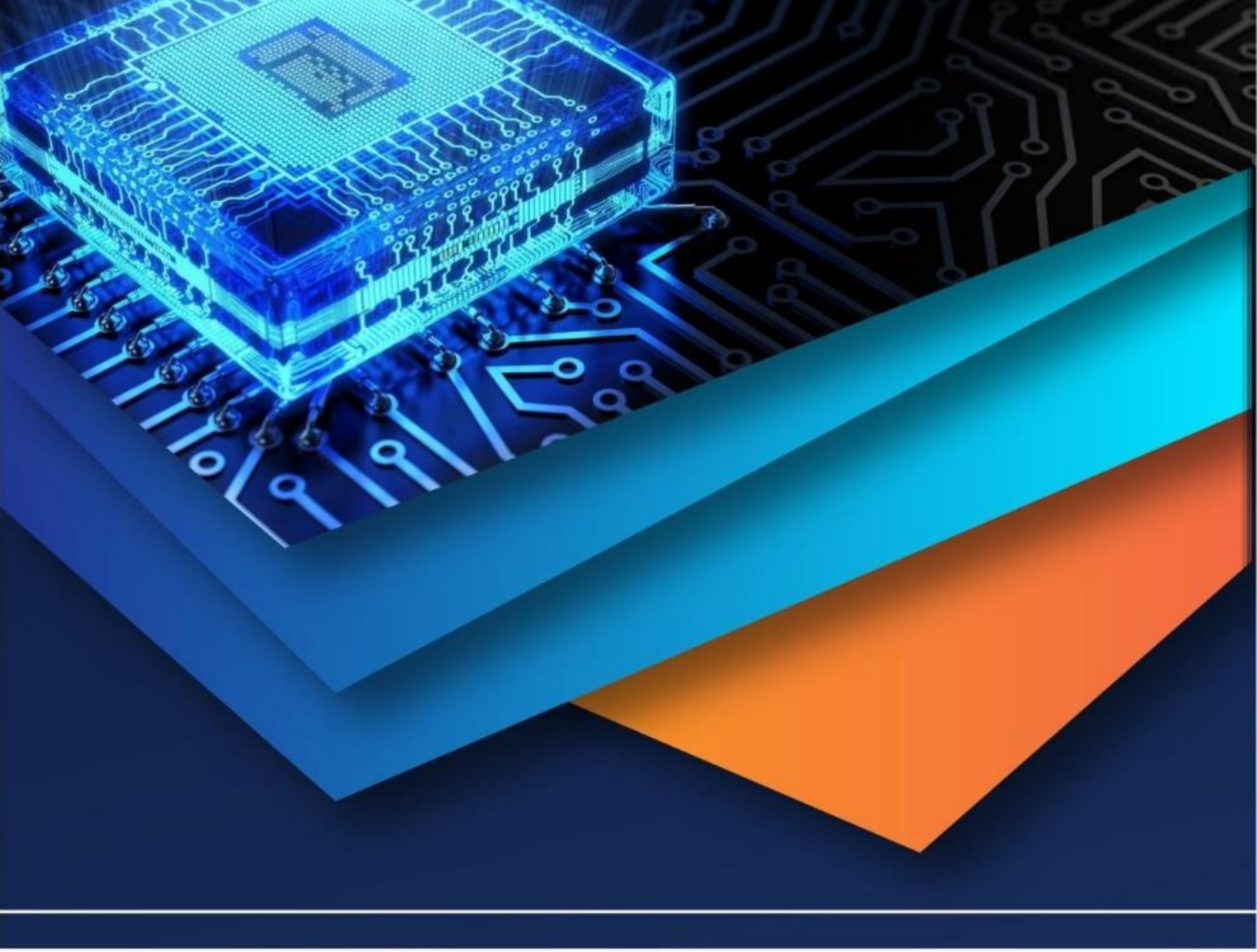
WI-FI networks are simultaneously increasing day by day. The advance challenges or we can say the security threat are also increases. We can upgrade the performance as well as the security with the help of proxy server and AES, if we can find the bug in AES and improve their performance. We can secure the Wi-Fi network up to 10-20% with the help of the proxy server and AES.

REFERENCES

[1] https://en.wikipedia.org/wiki/Network_security
[2] http://www.webopedia.com/TERM/W/Wi_Fi.html
[3] http://en.wikipedia.org/wiki/Proxy_server.
[4] Forward and Reverse Proxies". *httpd mod_proxy*. Apache. Retrieved 20 December 2010.
[5] Introduction to Wi-Fi Network Security By Bradley Mitchell .
[6] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.

[7] M. M. E. Adam and A. G. Elsid Abdallah, "WIFI SECURITY", Volume 2 Issue 2 (2015), [Online2016-02-09].http://www.sustech.edu/staff_publications/20150412092456586.pdf.

[8] The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices by Wi-Fi Alliance



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY