INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 468-472

IOT BASED SMART SECURITY SYSTEM WITH WPA AND WPA2 SECURITY WITH RADIUS SERVER

Anju Jessica C[1], Pradeepa S[2], Srisubiksha A[3], Dr. K. J. Prasanna Venkatesan[4]

[1,2,3]B. E, Ece, National Engineering College, Kovilpatti, India.

[5]M. E., Ph.D., Associate Professor (Sg), National Engineering College, Kovilpatti, India.

ABSTRACT

The role of technology in daily living has been expanding. Contrarily, cybercrime is a significant new danger. More information, both professional and personal,is shared online today. Data theft is constantly evolving as criminals look fornew methods to profit financially and illegally. As long as we continue to face this risk in our daily existence. All kinds of data should be protected from loss and theft. Authentication and authorization are necessary for secure communication.

1. INTRODUCTION

In the modern world, majority of people are forced to share some of their confidential information and business dealings online out of fear that a third party will steal it and use it inappropriately. In order to protect all of that material from outsiders, it must be secured. We are true of some authentication and permission in this situation. In this stimulation, we've used Radius Server, which offers centralised AAA (Authentication, Authorization, and Accounting), as well as WPA2 to protect wireless networks. In order to prevent data theft, both Radius Server and WPA2offer increased protection. The Cisco packet tracer utility wasalso used for this simulation.

2. OBJECTIVE

In the lives of humans, technology has been advancing daily. Cybercrime, on the other hand, is a significant new danger.The amount of personal and professional material we share online is increasing. To steal data for illegal activities and monetary gain, criminals come up with novel methods. Our everyday lives continue to carry this risk. Every form of dataneeds to be protected from loss and theft. Authentication and authorization are required in order to protect our data. Practically speaking, wireless signals don't respect the boundaries of a workplace, a house, or an organization and presentinherent security risks such as information leakage and unauthorized access to improve protection. WPA2 and RADIUSservices have both been used. With the help of the Cisco Packet Tracer Simulation application.

3. PROPOSED METHODOLOGY

Regarding authentication and secrecy, WPA2 is a reliable protocol. In the Enterprise edition, security measures like RADIUS server authentication are reliable and offer authentication along with other openness. Still a viable option for the IoT infrastructure is the technology (Wi-Fi), which uses a pre-Shared Key for device authentication. Weak against assaults, however, are the WPA and WEP protocols. The same key is sent with each data packet that is transmittedover the wireless network using WEP encryption, which employs a shared key authentication. Those who wish to do harm caneventually put together their key if given enough time and information. When using WPA, compatibility with older hardware and running systems is the main problem. WPA extends transmission time and raises data packet size while imposing a higher performance overhead. In this paper,we suggest a scenario in which authentication does not require the transmission of encrypted key during association or re-association. Users will manually distribute Pre Shared Key among themselves.

After the successful identification the key will be shared, needed verification will be done to connect with the enterprise network A greeting has now been established. Theencrypted code, will range in different length from 64 to 256 bits in the suggested method, is calculated using SHA-512. The adversary cannot associate with the network using the hash number, even if it is obtained. Let H stand for the encrypted code of the which was computed using the SHA 512 algorithm,

1. Selection of appropriate software and an configuration of the network service are proposed methodology for the host. 1.Firstly, identification process will take place to connect to the network.
2. Appropriate software package selection is more important because it helps to connect to the network correctly. In the server's hardware installation and configuration will be done3.For the identification purpose the user device will be configured
3. In order to have access, the network user accounts will be assigned to all user with appropriate login details to connect.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 468-472

4. To ensure the proper working of the host, the server will be tested for several times.
5. To ensure the secureness of the network the security patches and update must be up to date

4. PROCEDURE

To create a better identification Cisco packet tracer iswell furnished with required components. From the server menu, the IP address is given after choosing the Host. In the Host, the needed settings are all enabled. To them and the wireless router is given a gateway.

The wifi router has WPA2 security enabled, and the radius server has been added to its database. The details of login are required to make any IoT device private. A host IP address and WAP2 Enterprises are setup on IoT devices. Assign an IP address to the laptop's radius server configuration. After entering the IP address, you can check into the web browser. There is a list of connected gadgets that is shown. Any condition you choose can be set, and it will operate according to the criteria you specify.

DESCRIPTIONSERVER

Client- server communication is a technique used by this protocol. Servers and consumers are involved. A router, which connects to a network, or a VPN concentrator, which creates VPN links, are examples of networking devices that are RADIUS clients. By contacting the server, the client requests account authentication.

WPA2

WPA2 is a protocol used to create links between devices and Wi-Fi routers. It offers encryption, which is necessary to maintain the security of the communication channel between the access point and linked devices. Modern routers by default use WPA2 today, which is extensivelyused. However, there are flaws in technology that bad actors are constantly trying to leverage. In comparison to WEP, WPA isbetter because it offers the TKIP encryption scheme to encrypt the encryption key and ensure that it wasn't changed during data transmission. The main distinction between WPA2 and WPA is that WPA2 necessitates the use of a more powerful encryption technique called AES, which enhances network security. Different kinds of WPA2 security keys are available. The keys used by a WPA2 Pre-Shared Key are 64 hexadecimal characters long. Commonly, this approach is employed. WPA2 PSK and WPA2 Personal mode are frequently interchanged by home networks.

IDENTIFICATION

Verification of the user, which can be done by displayingidentification and credentials.

AUTHORIZATION

According to the user's authentication procedure, this refers to the granting of particular services or resources. As a result, users can receive a limited set of rights. Depending on the region, IP address, or time of access, theselimitations may apply.

ACCOUNTING

This is about monitoring how much each individualis using in terms of resources. Host identification isn't required to use this function. Uses for this include administration, planning, billing, etc.

5. RADIUS SERVER MECHANISM

This host ensures the secure access to network resources.In this mechanism the identification will send to thehost. Then it will validate the login details whether to grant or deny access to the user. The host will make the decisions with the help of predefined policies. The identification involves a series of exchange between the user and host. The user will send the request to the host in turn it will send the response whether it is acceptable otherwise it rejects the request. The host will track the activity of the user who loggedin.

RADIUS SERVER AUTHENTICATION METHODS:

Several user identification techniques are supported by this host. It can handle many methods if the login details provided

PAP

PAP setup files and the PAP database are used to set up Password Authentication Protocol (PAP) authentication. Although PAP does not give the user access to the shell, it functions similarly to the UNIX log on programme.

CHAP

It provides the good security in this system. When a server wants to connect to a network resource, the host will send thechallenge message. For the received challenge, user will generate the hash value. This value will be sent to the host foridentification, comparison will take place. The acceptable user alone gain access to use the network resources.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 468-472

MS-CHAP

It uses encryption techniques to guard the host challenge responses.

EAP

Extensible Authentication Protocol (EAP) is an authentication system used in point-to-point connections andwireless networks.

RADIUS PACKET FORMAT :

Key

A RADIUS packet's type is indicated by one octet-long Codefield. Depending on the RADIUS packettype, the value of the code field varies. An Access-Request packet, for instance,would have a value of 1, whereas an Access-Accept packet would have a value of 2.

Identifier

Identifier identifies the user in a network with the help of mac address, username, certificates and ip address. This is done by server to ensure the authentication and authorization of theserver database.

Length

Length means size of the data packets. The length settings in the server must be configured correctly. If incorrect length of packets will result in the failure of the network issues.

Authenticator

It identifies and verifies the user who tries to connectto the network. Whenever the user attempts to connect it sends the request to the authenticator. To the appropriate userlogin will be provided. This ensures the secure access.

Attribute

Access policies are defined by these element. The reporting purpose, network usage and user activity are collected by the attribute. It provides the security to the server.

Type

RADIUS attribute ID is displayed in the Type field,which is one byte long. The number is between 1

and 255.

Length

The RADIUS attribute's length is displayed in the Lengthfield, which is one octet long.

Data Exchange Fields

These fields can be up to Two hundred and fifty three bytes in length. Specific RADIUS attribute information is contained in theValue field. The Type and Length fields control how theValue field is formatted and how long it should be.

6. RADIUS AUTHENTICATION PACKETS

Step 1

The login details are attached to the first packet will besent from the user to host. This packet helps to decide whether to grant or deny unique services requested.

Step 2

The response message from the server to the user is like verifying the login details. The network access has been provided to connect to that. The message consists of session id,the time that they spent in the network.

Step 3 :

If this message is received from the host indicates that the user who attempts to connect to the server are failed to connect network and their login details are denied. The server will ensures this by verifying with the directory or database. The rejection of identification may be entering of incorrect login details.

Step 4 :

To make the server more secure before providing denial or granting additional challenge message will be sent to the server.

To determine the secureness the one time logindetails, a token will be included. This message ensures only authorized users are able to connect to network resources.

PACKETS FOR RADIUS ACCOUNTING

These packets collects details regrading the user'snetwork usage. It is the collection of session usage, data usage.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 468-472

Reply for Accounting (Start)

If a user uses accounting, it sends this packet to a hostbefore gaining access to network resources.

Accountant Response (Begin)

The host must then send a Start packet aftersuccessfully receiving and records the packet.

Reply for Accounting (Interim Update)

Real-time accounting can be configured to halt useraccounting if the Accounting-reply(Stop) packet is not received by the RADIUS server.

As a result, by routinely delivering Accounting- reply(Interim-update) packets to the server, the client reduces accounting variation.

Accounting Reply (Interim-update)

The device will sent a message to the user regarding the usage information. This data will be stored in database. Message will be sent periodically to the server know how much data is transmitted and used. By analyzing the generated reports by the host we can easily detect the abnormalities easily. This helps to maintain the security and control over the network resources.

Reply accounting, stop

This packet is sent by the user, demanding that the host discontinue accounting when a user intentionally logs out or is forcibly disconnected by the NAS, containing data on network resource usage (such as the online duration and quantity of incoming/outgoing bytes).

STEPS TO I MPLEMENTATION OFIDENTIFICATION (LOG IN)

- Using its user credentials, the user tries self- authentication in the first stage.
- The user then sends an Access-Reply message to the host with a username and password.
- Using the data in the request, the host performs user authentication against a third-party database. (for instance, Active Directory). If a same is found, the hostaccesses its database to get more details about the user in question. The RADIUS
- server looks for a data or access policy to get the samethe user's security. If enabled, a request will be submitted along with an access challenge if necessary is identified.
- In the event that the host is able to validate the reply, itsends an Access-Allow message back to your gadgets.
- If the host resply is invalid or does not follow the rules, the transaction is abandoned and an Access- decline message is sent back by the host. The user won't
- be able to use it if the system is locked out. The Access-Allow message has two attributes: a sharedconfidential and a purified ID. If the user cannot locatethe Shared confidential , messages are denied.
- If the shared confidential exact, the user gets the valueof the purified ID attribute. The user then uses this purified ID to join the user to a specific RADI host Group.
- At this point, the user can create a network connection.

Can you trust the host?

It's impossible to imagine that issues pertaining to cybersecurity may be important for degrading. Its age and the fact that cyberthreats are now much more common, it is sense to be concerned about the security of host. The very best thingis host continue to be very secure when configured properly. When combined with x.509 digital certificates, they has operate better than when using user credentials, which are frequently susceptible will be taken as C.

Can we use the host?

A breach in the network infrastructure of your business is among the bad things that may happening today. It could have severe implications on your daily operations as wellas your reputation among clients and customers. In light of this, it is crucial to maintain compliance with security good practices, and this includes the method you employ for user authentication on your resources. You don't want unauthorizedentrance to occur, thus the host can help you prevent it.

To ensure that only allowed users are accessing corporate resources, the Identity Provider can validate a user's credentials or a host can confirm a certificate is still valid by comparing it to a Certificate Revocation List.

A host will Identity a mistake, such as SecureW2's Cloud host, can go above and beyond by cross-referencing certificates with your identification during authentication, giving you access to a variety of attribute-based policy enforcement options.

Another crucial consideration is role-based access control, which we briefly covered before. By granting each user, the

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

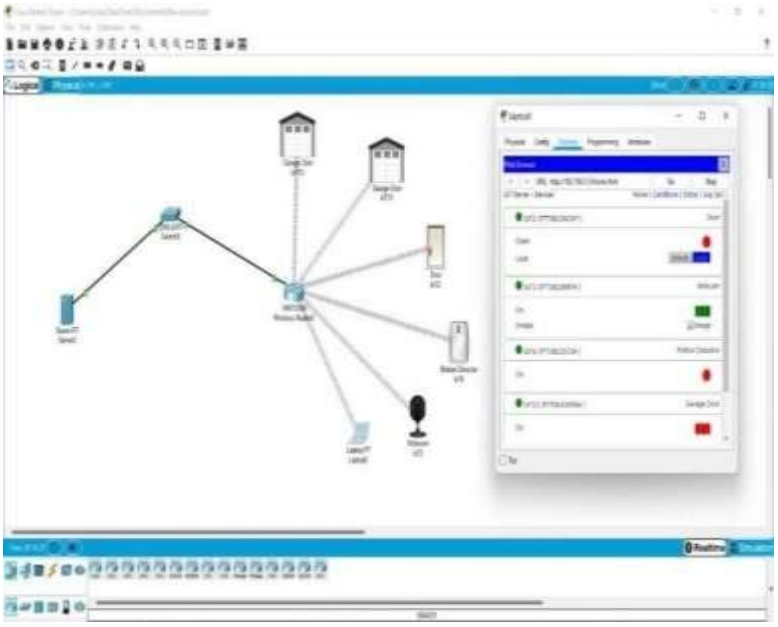
Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 09, September 2023, pp : 468-472

appropriate level of network access based on their credentials or certificate (or directory entry, in the case of ID Lookup), a RADIUS can help your company make the moveto a mature ZTNA model. Additionally, RADIUS servers provide your IT team with more visibility through their event.logs. As a result, IT professionals can quickly respond to anyquestionable behavior by reviewing the logs. Briefly, a host is a fantastic addition to the network security strategy

7. SIMULATION RESULTS



8. CONCLUSION

Comparing the encrypted text of five hundred and twelve and one hundred and twenty eight, suggested approach are strong enough to withstand hacking. These servers are applicable for to provide the reliable infrastructure for large companies. The involvement of handshaking mechanism in this server makes it secure and efficient means of managing network. The main advantage of using this server is providing centralized security to the user accounts because of security policies and for its scalability and flexibility of the users.

9. REFERENCES

[1] Aqeel-ur-Rehman, K.M. and Ahmed, B. (2013) Communication Technology That Suits IoT—A Critical Review. CCIS Springer-Verilag, Heidelberg.

[2] Taskin, M. (2008) WEP Post Processing Algorithm for Robust 802.11 WLAN Implementation.Science Direct: Computer Communication Journal, 31, 3405-3409.

[3] Sheila, F. (2007) Establsihing Wireless Robust Security Networks. NIST Special Publication, Gaithersburg.

[4] The Wi-Fi Alliance (2012) The State of Wi-Fi ®Security.https://davidhoglund.typepad.com/files/20120229_state_of_wi-fi_security_09may2012_updated_cert.pdf

[5] John, L.M. (2005) Auditing Wi-Fi Protected Access (WPA) Pre, Shared Key Mode. Linux Journal3. https://www.linuxjournal.com/article/8312

[6] Arash, H.L., Mir, M.S.D. (2009) A Survey onWireless Security Protocols (WEP,WPA and WPA2/802.11i). 2009 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, 8-11August2009.https://doi.org/10.1109/ICCSIT.2009.5234856

[7] Mina, M., Abdul, A., Zunata, A. and Zaton, M. (2007) Security Improvement for Management Frames in IEEE 802.11 Wireless Networks. International Journal of Computer Science and Network Security, 7, 276-284.