Optimation Wireless Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)

Taufik Nur Hidayat
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
One of the main changes in the field of telecommunications is the use of wireless technology. Wireless technology is also implemented in the Ahmad Dahlan University Campus 3 Research Laboratory environment, better known as wireless LAN (WLAN). Each user within the range of campus research laboratory area Ahmad Dahlan University radiates an access point (AP). Another negative impact is that communication that occurs will be easily intercepted between the security of campus network users. The stages performed in this study use the PEAP EAP method to provide security to safer wireless. This security method aims to protect client authentication. PEAP only requires a digital certificate on the authentication side of the server, while the digital certificate on the wireless side of the client will be replaced by using a combination of username and password. Thus, the conclusion of the security implementation using the Freradius Authentication tool by using the PEAP EAP protocol can improve security on the wirelles. Authentication aims to verify the identity of the client so that only registered/valid users can connect to the network and do not need a long time when authentication.

Keywords
(EAP), (PEAP), Protocol, Freradius, IEEE 802.1X.

1. INTRODUCTION
One of the major changes in telecommunications is the use oftechnology wireless.technology is Wireless also applied to computer networks, which is better known as a wireless LAN (WLAN). The conveniences offered by wireless LANs are the main attraction for computer users using this technology to access a computer network or the internet. In the last few years,users wireless LAN have experienced a rapid increase. With Hotspot, internet access becomes easier and more flexible because users will be able to surf the internet without using cables. In the campus environment , this hotspot service is expected to accelerate access to information for students, especially in education, which is known as a barometer of progress in information technology.[1] Many people prefer mobile technology in order to facilitate their activities. So wireless technology was created for area networks that are directly in contact with the person-by-person, namely wireless networks. This technology really supports the level of productivity in the midst of high mobility. This technology is better known as a Wireless Local Area Network (WLAN) or Wireless-Fidelity (Wi-Fi). Wireless has one big problem, especially in public networks, namely data and digital communications that pass through wireless networks can easily be intercepted by irresponsible parties.

Such improvements have led to the demand for a good computer network security system. One security method to resolve this issue is to use an authentication system. The system will perform a user identity authentication process that usually begins with the delivery of a unique code that can be a username and password to ensure a legitimate user[2]. This study aims to optimize the EAP PEAP protocol as an authentication protocol for wireless network users to provide convenience and improve the existing network administration and security aspects.

1.1 Literature Study
1.1.1 Previous Research
The study stage of literature is done to provide a reference to add knowledge in conducting research, there are 4 references cited in this study.

Citra Najih Nurmawanti1, Duddy Soegiarto2 and Umar Al Faruq (2013), with the title Wireless Network Security Using PEAP Ms CHAP V2, can secure data and exchange usernames and passwords from sniffing and bruteforce attacks and to prevent un authenticating clients to be able to access the internet network with a authentication mechanism based on username and password.[3]

Joshua John Muskitta, Banu Wirawan Yohanes and Hartanto Kusuma Wardana (2016) under the title Protected Extensible Authentication Protocol (PEAP) implementation using Remote Access Dial In User Service (RADIUS) case of research results in protection when connection is disconnected: PEAP protects EAP message exchange when connection is disconnected because PEAP sends success/failure messages inside TLS tunnel.[4]

Ichsan Wiratama and Putu Sugiartawan (2019) with the title Enhanced Wireles Security on computer networks at Amikom University using the IEEE Protocol.802.1X Case study results show the configuration performed that will successfully appear web in the destination and Increase the location of wireles in amikom computer network using IEEE Protocol.802.1X.[5].

Muttaqin et al. (2016) titled Hotspot Authentication System Using LDAP and Radius on Wireless Internet Network Prodi Teknik Sistem Komputer case study results in the form of Network server authentication using OpenLDAP and FreeRadius Hotspot [6].

1.1.2 Wireless LAN Components
In building a WLAN network, it takes some hardware for communication between stations to be performed. In general, wireless LAN components consist of the following devices [7].

a. Access Point (AP)
In wireless LAN, the transceiver device is referred to as an access point (AP), and is connected to the network (LAN) via cable. The function of AP is to send and receive data, and serve as a data buffer between wireless LAN and wired LAN.

b. Extension Point
It only works like a repeater for clients in a far away place. The terms of the AP used as extension points are related to the frequency channel used[8].

1.1.3 Extensible Authentication Protocol (EAP)

EAP or Extensible Authentication Protocol is an authentication framework that provides transport services and uses keying material and parameters generated by EAP methods. EAP was originally developed for Point-to-Point or PPP connections. However, nowadays EAP is also implemented and widely used for user authentication on wireless networks[9]. EAP is used in three-tier authentication, so in the communication process EAP will use a different transport protocol

1.1.4 Protokol IEEE

Security is very important in wireless networks. On wireless networks, IEEE supports the 802.1X standard to improve data transmission security [10]. The IEEE 802.1X architecture scheme is shown in Figure 1.

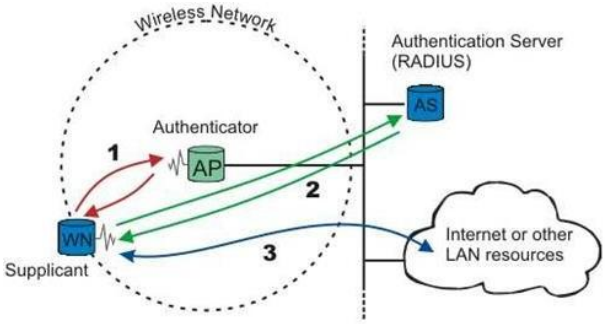

Figure 1. IEEE architectural scheme

Supplicant is a device used by users, can be laptop, mobile phone, PDA and also other gadgets will connect themselves to authenticator devices in the form of access points. From the connection between the supplicant and the authenticator then on the supplicant side will appear a menu that asks to enter data in the form of user data and password for the connection to the network, then authenticator will forward the data from that user to the authentication server in the form of RADIUS server [11].

1.1.5 Protected Extensible Authentication Protocol (PEAP)

Protected EAP (PEAP) is one of the EAP methods. PEAP is a username and password based authentication protocol type to secure the authentication process. PEAP is mostly used on wireless LAN networks, but can also be used with i access rights. cable authentication. PEAP uses server-side public key certificates to authenticate the server. Then create a TLS tunnel between the client and the authentication server. PEAP is a good choice for an authentication protocol because it is compatible with multiple hardware devices from various vendors, such as Microsoft, CISCO [12]. and Funk. As in the following figure 2.

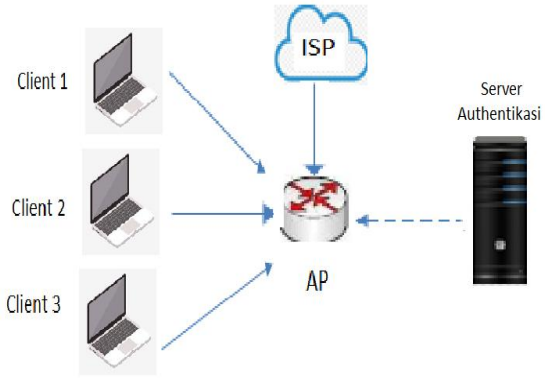

Figure 2. PEAP Topological Design

The details of the figure 2. design topology of the wireless network system above are as follows:

1. The type of topology that is applied is the wireless network mode of the infrastructure.
2. All client IP addresses and access points used using class C (subnet-mask 255.255.255.0); represented in CIDR (/24) format.
3. In the network segment there are:
   A. Client : defines the client of the internal WLAN.
   B. Server : Defines and represents a server engine on a computer's network system
   C. Access point (AP) : defines as a device that becomes an intermediary between cable and air-based communication.

1.1.6 RADIUS

RADIUS stands for Remote Acces Dial in User Service. First developed by Livingston Enterprises. It is a computer security protocol network used to create controlled access management on a large network. RADIUS is defined in RFC 2865 and RFC 2866. RADIUS is commonly used by companies to regulate access to the internet for clients.[13]. RADIUS authenticates, authorizes, and registers user accounts centrally to access network resources.

1.1.7 Wireless LAN Standard

The standard commonly used for WLAN is 802.11 set by IEEE at the end of 1990. standard 802.11 there are 3 namely IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.[14].

1.1.8 AAA Security Protocol

The concept of working authentication server is known as AAA (authentication, authorization, and accounting). That consists of Authentication, Authorization, and User Account Registration. Aaa concept has functions that focus on three aspects in user access control including Authentication, Authorization, and Accounting[15].

1.1.9 Authentication Protocol

Protocol is a set of rules relating to data communication between communication tools so that data communication can be done correctly. Authentication is a verification process for declaring an identity. A common form commonly used to authenticate using a combination of logon ID/username and password, if the combination of the two is correct then the client can access to certain network resources.[16].

1.1.10 EAP Over RADIUS

EAP over RADIUS is an authentication mechanism

performed by the access server (access point) to pass EAP messages of any type of EAP to the RADIUS server to perform the authentication process. An EAP message is sent between the access client and the access server using the EAP Message RADIUS attribute format and is sent as a RADIUS message between the access server and the RADIUS server. The access server is only a device that misses EAP messages between the client and the RADIUS server. RADIUS, not done by the access server. EAP over RADIUS is used in environments where RADIUS is the provider of authentication mechanisms. The advantage that can be gained by implementing EAP over RADIUS is that the type of EAP does not need to be installed on every access server, simply done on radius server. However, the access server must support EAP as a protocol for performing authentication activities and passing EAP messages to radius servers. Because EAP is part of the 802.1x standard, it must enable 802.1x authentication to enable AP in order to use EAP[17].

1.1.11 Wireless LAN

Wireless uses radio waves (RF) or microwaves to form communication channels between computers[18].Wireless networks are a more modern alternative to cable networks that rely on copper and fiber optic cables between networks. LAN or Local Area Network is a computer network that covers a relatively small geographic area in one floor or building[19].

2. RESEARCH METHODS

2.1 Research Methods

2.1.1 Observation

As a scientific method of observation can be interpreted as observation, so observation is a data collection technique that is done systematically and deliberately, which is done through observation and recording of symptoms investigated by using sensory tools especially the eye against ongoing events. In this study, the authors made observations of network data objects and security in the Research Laboratory.

2.1.2 Literature

With a lot of studying the littarature related to network security, FreeRadius, EAP – PEAP. So the source of literature is widely obtained from books, papers or journals, scientific works and supporting sites.

2.1.3 Identification of Needs

Tools and materials used in this study are divided into two types, namely software and supporting *Software* in conducting research. Research tools and materials as shown in, among others : Ubuntu /10.10/The operating system is used as the OS installe Ubuntu Kalilinux for authentication user centralized. Windows 7/7/Foroperating systems client / user. Winbox/V3.19/As a configuration access point.[20].

Tools and materials used in this study are divided into two types, namely software and supporting hardware in conducting research. Research tools and materials:

1. AAA/ RADIUS Server Computers Server /Produc : HP Prosesor : Intel I3,Harddisk : 1 TB, RAM : 4 GB,OS : Window 10 64 bit/ Used as a centralized authentication server using FreeRADIUS, as well as centralized user database management and management.
2. Access Point (AP)/Mikrotik Hub Mini Series : R8931-2ND/ As an access server / device that delivers EAP packets between the client and authentication server
3. Computer Client/ Produk : LENOVO 140 Prossesor : Core2Duo T5800 2,0GHz, RAM : 3 GB, Harddisk : 250 GB WLAN card : Broadcom 802.11 g Function :clientterotentikasi/Used as an authenticated client computer and has permissions

3. RESULTS AND DISCUSSIONS

In the study designed a wireless network using the campus network of Campus Research Laboratory that is already available to detect ip addresses. It takes 2 laptops as detectors and . 1 Acces Point . On one laptop as FreeRadius to save the user as Authentication from username and password with ip 192.168.88.2. Laptop one as a client has an ip address 192.168.88.3 as a user who will be log in on the network. For Acces Point is used as sending and receiving data and can grant Access rights, ip address 192.168.88.1

As in the following figure 4.

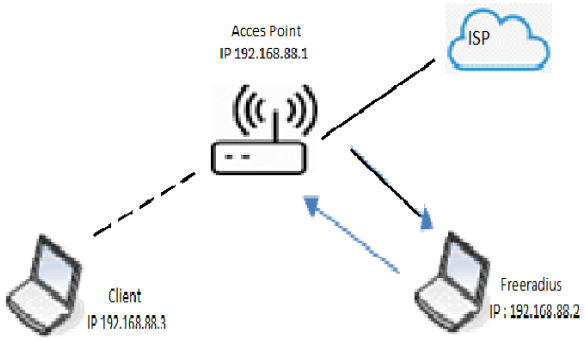

Figure 3. Research Scenarios

The details of figure 3 above are the stages of research that will be.

3.1 RADIUS server configuration

3.1.1 Configure radiusd.conf.

aim to activate radiusd protocol, More can be seen in the settings As in the following figure 4.

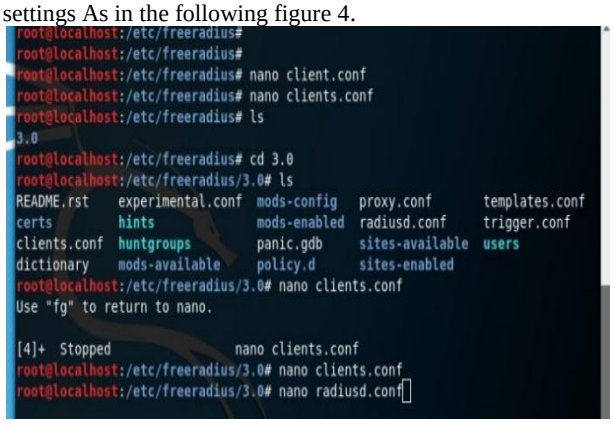

Figure 4. Radiusd conf result configuration view

In figure 4.if there is still a "#" sign in front of it then the script is not active

3.1.2 Configuring clients.conf

This file aims to configure in the form of adding and subtraction of new clients, We type a command line in linux Terminal as follows: With this file above will determine the RADIUS Client device that will be connected to FreeRadius as shown in figure 5.

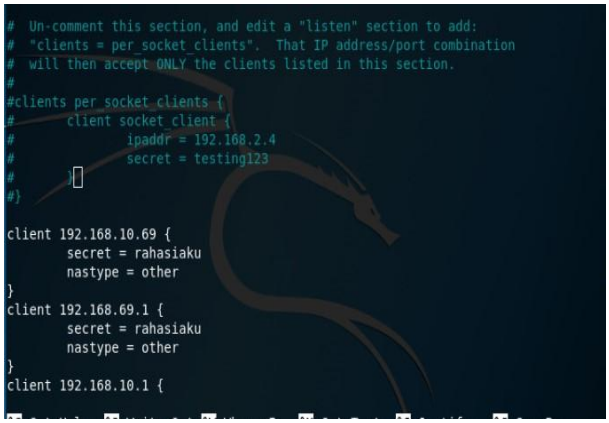

Figure 5. Configuration View on *clients.cof*

In figure 4.above add a script in the form of ip address from RADIUS Client (Mikrotik) and also Secret that will be used by RADIUS Client connected to FreeRadius. Both types of parameters are the main. such as the topology above already fill ip address of Mikrotik 192.168.69.1and secret ie "rahasiaku"

3.1.3 Configuring users.conf

At this stage add an account in the form of username and password used to login hotspot. add a combination of user and password to the Users file. Type in linux terminal a command line as follows: In the file a script tries to add username=try and password=12345, and the second username=taufikradius and password=testingradious Can be seen in figure 6:

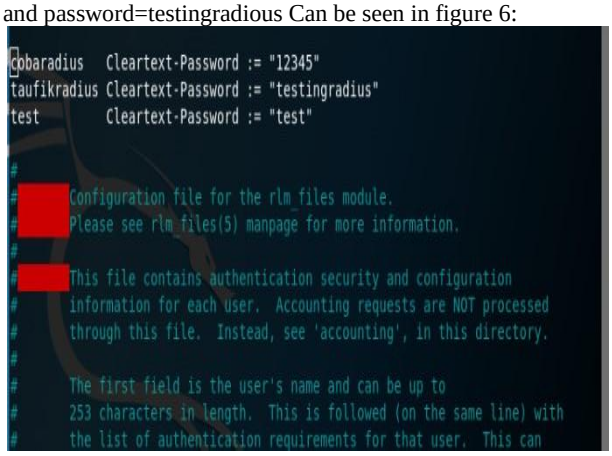

Figure 6. User.conf Addition view

In figure 6 above use the username and password to register the user as the username and password to be used for authentication at Acces Point.

3.2 Configure Access Points

The first step should be in the Wirelles menu section of the Security Profile section. one of the features on microtics used to add authentication methods using dynamic key encryption: WPA/WPA2 and static key: WAP. The most widely implemented security feature is wireless authentication using WPA/WPA2 Pre-Shared-Key set on the wireless Security profile. Shown in figure 7

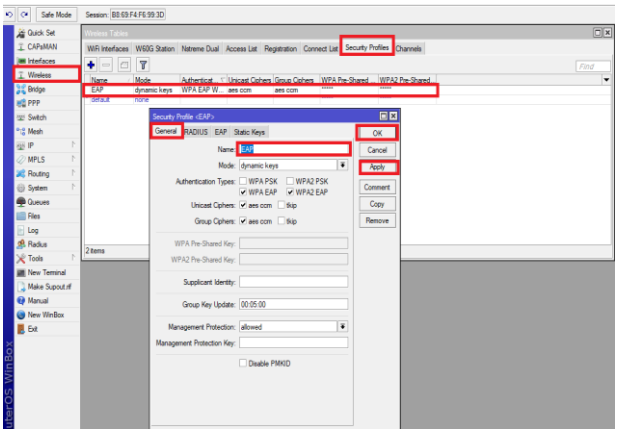

Figure 7. Display settings from the Security Profile

In figure 7 above, security applies to authentication types using wpa EAP which is better security and in dynamic keys mode is used to determine the combination of authentication in the form of username and paswword. enter in the example name section above use "EAP", to be in node iskan "dnyamic key" meaning it does not require a passwor set on the microtic part and for authentication type ceklist WPA EAP and WPA2 EAP section. For the next stage the configuration of EAP Methods for PEAP can be seen in figure 8

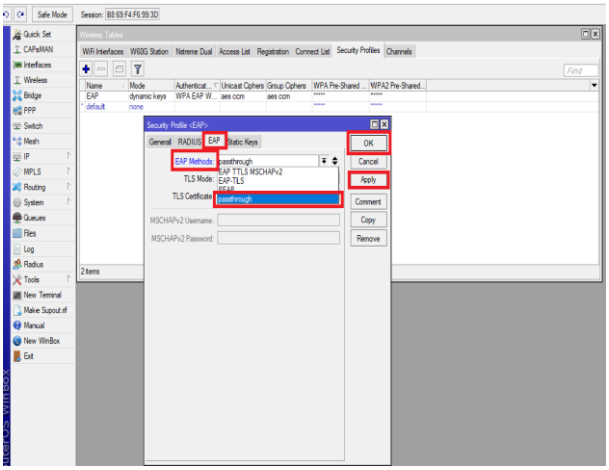

Figure 8. EAP settings display

Figure 8 is used for the choice of wirelles authentication method using IEEE 802.1X/EAP as a confucius step. EAP is used for cable verification method options using IEEE 802.1X/EAP as a confucius step. in the picture above divide the EAP Security Profile in the EAP Method section select "Passtrough" for others to go. The next step is to install the Wirelles Menu section. The next step is to set the wlan interface menu section as in figure 9.

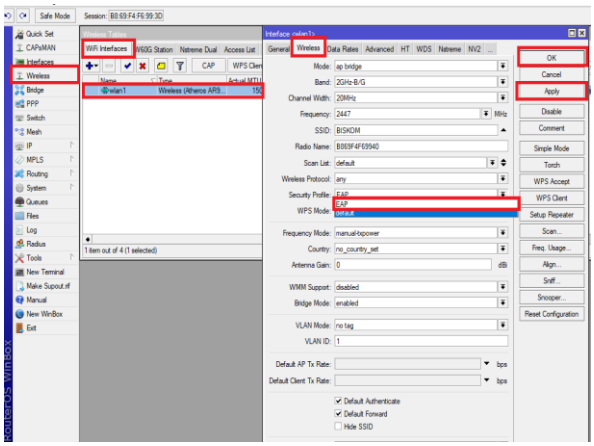

Figure 9. WLAN Interface settings display

In figure 9 above, configure the wlan section to be used as the SSID for the Wirelles name for the client. For configuration on the WLAN1 Interface in the Wireless submenu, in the mode select "ap-bridgge, next on the SSID when "BISKOM" matches the example above, and finally the Security Profile section select "EAP' which was before it was created in the Security Wireless sub menu. and the next step of setting the Radius Server on the figure 10.

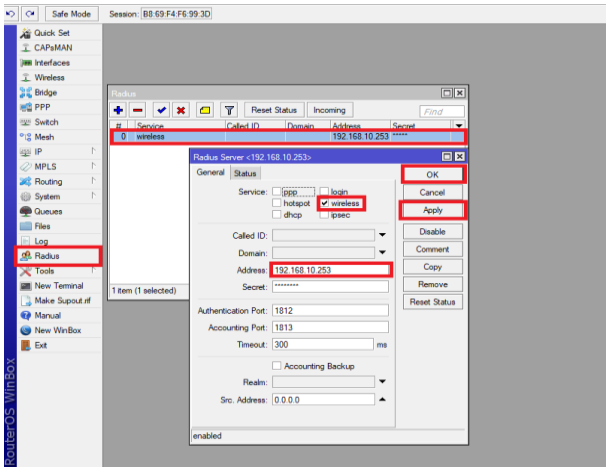

Figure 10. Radius Server settings display

In figure 10 above is the Radius Sever menu used to connect the IP client to be connected with Mikrotiknya and previously the server IP has been added to the client.

3.3 Implements

After finishing the simulation stage, the author then implements this solution on the actual device. . On the authenticator side, this device must know the IP address of the RADIUS server and the combination of shared secrets used to be able to communicate with the RADIUS server. While on the supplicant side, this device first installed a digital certificate for the CA or digital certificate from radius server. seen in figure 11.

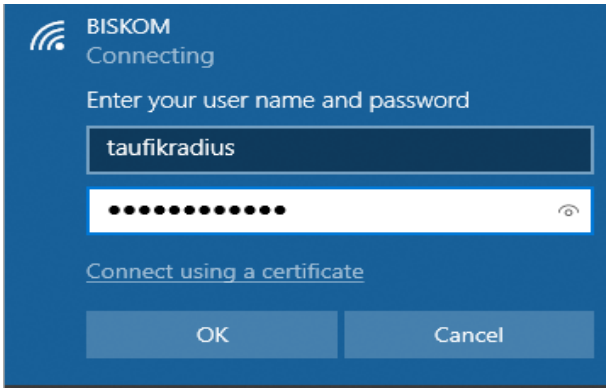

Figure 11 Login view

In figure 11 above is the login view in window 10 with SSID "BISKOM" and enter username" taufikradius" and password "taufiktesting" that has been registered on the user side in Freeradius Configuration. This digital certificate ensures that the applicant is connected and authenticates to the actual RADIUS server. This mechanism is also called server authentication. Once the configuration on the applicant and authenticator is complete, the user has been able to access the wireless network using their respective accounts. when the user whose account is not registered, the authenticator cannot give access to the user, so the user must be registered first, for more details see Table 1

Table 1. Results from the experiment

No	Client	before PEAP conditions	after PEAP conditions
1	Security Wireles Mode	-	✓
2	Capture username and password	-	✓

From table 1 it can be concluded that the application of PEAP method is safer in terms of security wirelles.

4. CONCLUSION

Conclusions obtained during the implementation of Wireless security using the PEAP EAP centrally monitoring user permissions. the Implementation of Protected EAP (PEAP) can improve security on the wirelles. Authentication aims to verify the identity of the client so that only registered/valid users can connect to the network and do not need a long time when authentication.

5. REFERENCES

[1] Supriyanto, A. (2006). Technical Overview of Wireless Device Technology and Security Standards. XI (2), 75–83.

[2] Supriyanto, A. (2006). Technical Overview of Wireless Device Technology and Security Standards. XI (2), 75–83.

[3] Citra Najih Nurmawanti1, DS (2013). Wireless Network Security Using PEAP Ms CHAP V2. Journal of Information Technology, 1 (1), 214-219.

[4] Yosua John Muskitta1, Banu Wirawan Yohanes2, Hartanto Kusuma Wardana3. 2016. " Implementation of Protected Extensible Authentication Protocol (PEAP) use Remote Access Dial In User Service (RADIUS)." *Techné*

Jurnal Ilmiah Elektroteknika 91-99.

[5] Ichsan Wiratama*1, Putu Sugiartawan2. 2019. " Improved Wireless Security on Computer Networks at Amikom University Using IEEE802.1X Protocol." *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)* 21-30.

[6] Dkk., Muttaqin. 2016. " Hotspot Authentication System Using LDAP and Radius on Wireless Internet Network Computer System Engineering Program."

[7] (Aristiara & Budihartanti, 2014) Analysis of Wireless LAN (WLAN) Network Security at PT. PLN (Persero) Region P2B Area Sorong Sonny Rumalutur. (nd). 19 (100), 48–60.

[8] Aristiara, D., & Budihartanti, C. (2014). Network User Authentication Using Radius Windows 2008 Server At Pt Pertamina. Journal of Techno Nusa Mandiri, XI (2), 118–128.

[9] Krisnawan, A. (2015). Room Security System Design Using the Raspberry Pi. Faculty of Electrical Engineering, Telkom University, 2 (2), 3743–3754.

[10] Muskitta, YJ, Yohanes, BW, & Wardana, HK (2016). Implement Protected Extensible Authentication Protocol (PEAP) using Remote Access Dial In User Service (RADIUS). Techné: Scientific Journal of Electrotechnics, 15(02), 91–99.

[11] Purwanto, TD, & Cholil, W. (2013). Performance Analysis of Wireless Radius Server on Access Point 802 Devices. 11g (Case Study at Bina Darma University). 2013 (November), 371–376. [7] ISACA. 2012a. Trust And Partnership A Business Framework for the Governance and Management of Enterprise IT.

[12] Riadi, I., Studies, P., Information, S., & Dahlan, UA (2011). Network Security Optimization Using Mikrotik-Based Application Filtering Introduction Theory Basis. 1 (1), 71–80. [9] ISACA. 2012c. Isaca COBIT 5 Implementation.

[13] Supriyono, A. (2013). Hotspot System Design Usin Captive Portal. Journal of Bachelor of Informatics Engineering,1(1),172–180.

[14] Primary, Rifky Wahyu. 2019. "Implementation Of User Authentication System Using Radius Server And Active Directory On Wireless Network In Pt. Kudo Teknologi Indonesia." Jakarta State Polytechnic..

[15] Purnama, Rachmat Adi. 2019. "Wireless Network Security Optimization Using MAC Address Firewall Filtering." Indonesian Journal on Networking and Security 43-47.

[16] Denda Aristiara[1], Cahyani Budihartanti2. 2014. "Network User Authentication Using Windows 2008 Radius Server At Pt Pertamina." Journal of Techno Nusa Mandiri 118-128.

[17] Baihaqi1, Yeni Yanti2, Zulfan3. 2018. "Implementation of WPA2-PSK Security System." Foyer Engineering 248-254.

[18] Internet Draft. Protected EAP Protocol (PEAP)Version 2 [Online]: -10 [25 Agustus 2010].

[19] Dirk van der Walt, "FreeRADIUS Beginner's Guide Manage your network resources with FreeRADIUS", PACKT publishing, Birmingham –Mumbai, 2011.

[20] Teuku yuliar Arif, Syahrial, and Zulkiram, "Study Protocol Authentikasionon internet service service (ISP)". Journal of Electrical Engineering: Volume 6 No. 1 / Agustu 2011.