

Implementation of Authentication Systems on Hotspot Network Users to Improve Computer Network Security

Ellen Dolan¹, Riya Widayanti²

Queensland University¹, Esa Unggul University²

St Lucia QLD 4072¹, Jl. Arjuna Utara No.9, Kb. Jeruk, Kec. Kb. Jeruk, Kota Jakarta Barat²
Australia¹, Indonesia²

e-mail: ellen.dolan@connect.qut.edu.au¹, riya.widayanti@esaunggul.ac.id²



To cite this document:

Dolan, E., & Widayanti, R. (2022). Implementation Of Authentication Systems On Hotspot Network Users To Improve Computer Network Security. *International Journal of Cyber and IT Service Management (IJCITSM)*, 2(1), 88-94. Retrieved from <https://iast-journal.org/ijcitsm/index.php/IJCITSM/article/view/93>

DOI:

<https://doi.org/10.34306/ijcitsm.v2i1.93>

Author Notification

April 2022

Final Revised

April 2022

Published

April 2022

Abstract

Because of the growing number of apps that use client servers, both desktop and WEB applications, each user must learn a large number of user ids and passwords, because each application requires authentication in order to use it for security reasons. Furthermore, the development of network media, both wired and wireless, is accelerating. In the scenarios stated above, RADIUS (Remote Authentication Dial-In User Service) technology is required since the RADIUS approach allows a user to utilize a single user id to access several applications, both desktop and web-based. The RADIUS protocol may be used with both wired and wireless media.

Keywords : wireless, authentication, database, server, client.

1. Introduction

User authentication is often not used in today's network use. When a person joins a network without user authentication, anybody can access the network. Wired Equivalent Privacy is used to authenticate wireless access points for transmission media (WEP) [1]. The WEP key must be put on each access point and each client access point, which makes it cumbersome for administrators to visit each client. Because the WEP key is static, it may be determined by examining other client computers [2]. Several programs now exist that can read the WEP key, allowing unauthorized users to gain access to the network and perhaps harm the machine within. WEP authentication is only given to connection lines for staff, while connection lines for students (hotspots) use wireless access point transmission media without using authentication so that it can be accessed by anyone.

The usage of a HUB (Ethernet hub) as a connection breaker on cable transmission media does not need authentication, so we may join to the network simply by plugging in the cable [3]. As a result, a system for user authentication is developed in this study, which uses both wired and wireless communication mediums.



Copyright © 2022 Ellen Dolan¹, Riya Widayanti².

This work is licensed under a [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/) (CC BY 4.0)

This research will reveal how to create a more effective network security management system as well as how to integrate user management across several apps[4].

2. Network Mode and Route Protocol

Wireless Access Points WLAN stands for Wireless Local Area Network and is a type of wireless network. A WLAN network enables two or more devices to interact using conventional network protocols without the use of a cable transmission line [5]. Electromagnetic waves, which can be in the form of infrared rays, microwaves, or radio waves, are utilized as the transmission channel for communication on the WLAN network (radio frequency, RF). There are a variety of WLAN network modes to choose from, including:

2.1. Ad-Hoc Mode

A peer-to-peer network, also known as a point-to-point network, is a term used to describe ad-hoc mode [6]. Ad-hoc mode allows computers on a WLAN network to connect without passing through an access point.

2.1 Infrastructure Mode

The WLAN network must be configured in Infrastructure mode to link a large number of PCs. In Infrastructure mode, extra equipment in the form of a wireless access point (WAP), also known as an access point, is required [7]. Because an access point functions similarly to a hub or switch on a wired network, it will serve as the hub or switch for the WLAN network. The contrast between ad-hoc and infrastructure mode is depicted in Figure 1.

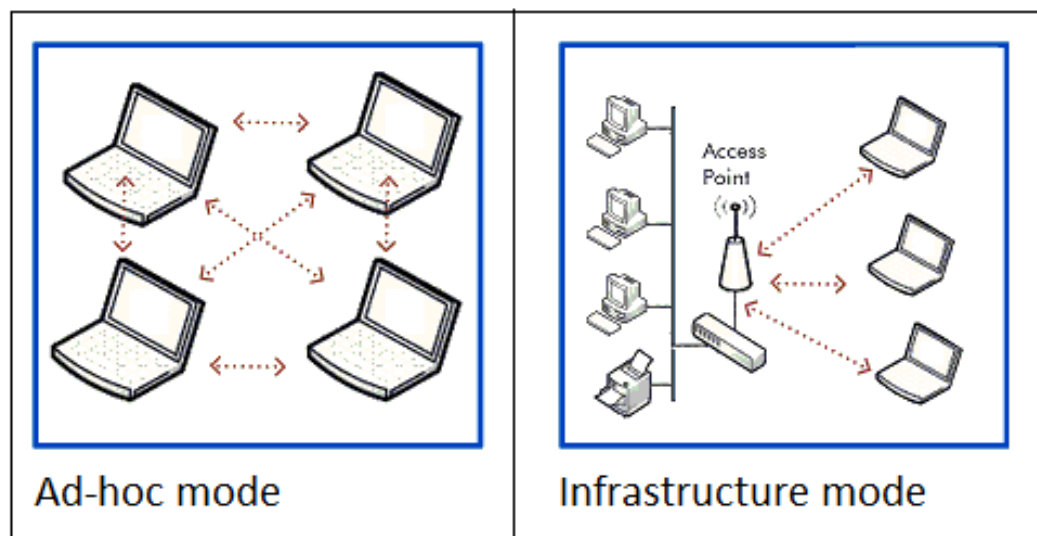


Figure 1. Ad-hoc mode vs Infrastructure mode

WLAN infrastructure networks can link to other networks, such as Ethernet networks. A bridge was necessary to connect to other networks [8]. Access points that circulate in the market can serve as a bridge in most cases.

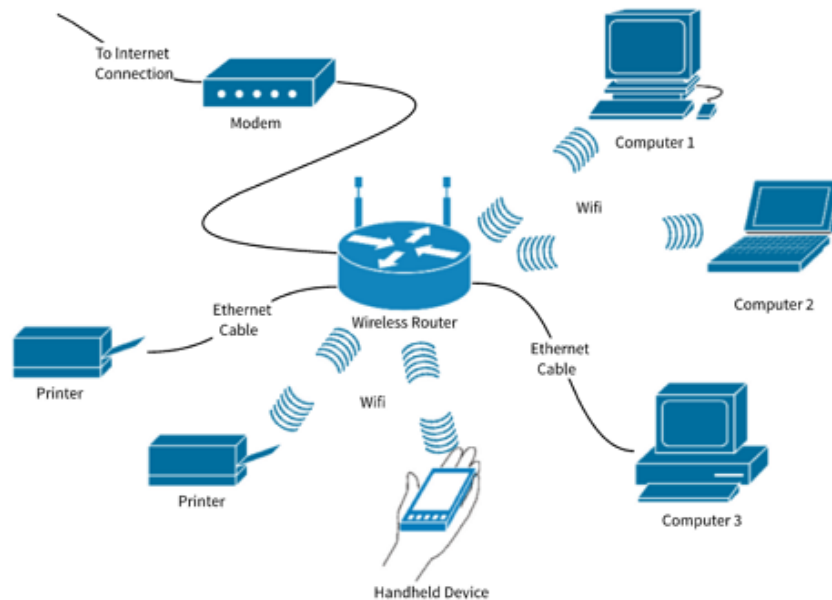


Figure 2. WLAN and Ethernet networks

The process of transporting data packets from one originating host to a destination host via one or more host nodes is known as routing [9]. The routing coordination technique may be separated into two categories: static routing and dynamic routing, as explained below:

a. Static Routing

Static routing involves manually filling and deleting entries in the forwarding routing table, whereas dynamic routing involves changes made via the routing protocol. Static routing is the most basic type of routing that may be used on a computer network. In a network, using 100% static routing involves populating every item in the forwarding table on every router [10]. In a small network, using static routing is not a problem; all that is required is a few entries in each router's forwarding table. On the other hand, completing the forwarding table in each router, which is not trivial in a big network, is a time-consuming task.

b. Dynamic Routing

Dynamic routing eliminates the need to manually populate forwarding table entries. Routing protocols govern how routers connect with one another and exchange routing information, which might vary the contents of the forwarding table based on the network's status [11]. As a result, routers are aware of the present condition of the network and are able to route datagrams appropriately.

RADIUS is a computer security protocol that allows users to authenticate, authorize, and register for network access from a central location. RADIUS was first used to authenticate remote network access over a dial-up connection, as described by RFC 2865 and RFC 2866. RADIUS is currently used to verify network access across a variety of connections other than dial-up, including VPN (Virtual Private Networking), wireless access points, Ethernet switches, and other devices [12].

By managing authentication and authorisation of user connections, the RADIUS server offers a security mechanism. When a client computer connects to the network, the RADIUS server requests the user's identification (username and password), which is then compared to data in the RADIUS server database to decide whether the user is permitted to utilize network services [13]. If the authentication and authorisation processes are successful, the reporting process begins, which includes logging all user connection activities, computing the time length, and counting the number of data transfers the user has made. The reporting process carried out by the RADIUS server can be in the form of time (seconds, minutes, hours) or in the form of large data transfers (Bytes, KBytes, Mbytes).

WEP (Wired Equivalent Privacy), often known as Shared Key Authentication, is a way of safeguarding wireless networks. Shared Key Authentication (SKA) is a type of authentication that necessitates the usage of WEP [14]. WEP encryption employs a key that is inserted into the client or access point (by the administrator). This key must match the one given to the client by the access point and the one used by the client to authenticate with the access point.

3. System Design

Hardware (Minimum) required are as follows:

1. x86 300 MHZ Pentium Motherboard
2. RAM 64 MB
3. Hard disk 40 GB

Hardware requirements to install Router OS, in this case using MikrotikOS

1. CPU and motherboard 100 MHz Pentium.
2. RAM 32MB
3. 1GB ATA/IDE hard disk.

The Linux Ubuntu and MikroTik installation media are:

1. Ubuntu Server 8.04 LTS Linux CD
2. MikroTik CD
3. FreeRADIUS Server Software
4. Software LAMP (Linux Apache MySql Php)

Users notice that the needed network is straightforward and uncomplicated. This is because the client just sees the network as a place to share generic information and connect to the internet.

A desktop application is a program that may operate on its own or without the need of a browser on a computer with a certain operating system [15]. By putting this program on each user's desktop, they may use desktop apps. Administrative operations are carried out using desktop software.

In the laboratory, some WEB-based apps may access desktop and e-learning programs, as well as WEB applications, whereas the hotspot can only access ebooks, e-journals, WEB mail clients, and WEB applications. SIAKAD is a line that may be accessed via a local network or the internet. Database servers, mail servers, FTP servers, DNS servers, proxy servers, and firewalls all employ application servers on WEB servers.

For administration and access to the internet. The cable used to connect the buildings is STP (Shielded Twisted Pair). UTP (Unshielded Twisted Pair) and wireless cable transmission medium are used to link customers in a single room. The transmission media, on the other hand, is for hotspot locations [16]. A HUB is used to divide clients and is put in each building or space depending on the quantity of clients.

With RADIUS Server, a simple topology may be created. The RADIUS server is responsible for centrally storing users and passwords [17]. The user enters the username and

password through the NAS's interface, and the NAS checks with the RADIUS server to see if the username and password are stored in the database. If the user has a username and password, he or she will be able to access the network [18].

According to the architecture of the authentication system as described in explaining the architecture of the authentication system, the user must connect to the network through a PC or laptop. If a user has a username and password on the RADIUS server, they may access the network. The user can connect to the network after he or she has properly logged in. The Bits application's username and password are the same as the user and password used to log in.

Name	Parent	Packet	Limit At (p...	Max Limit	Avg. R...	Queued Bytes	Bytes
Hotspot Total Download	global			2M	2.0 Mbps	0 B	3764 2...
HS-Download	Hotspot Total	Paket...	1M	2M	2.0 Mbps	18.7 KB	3782 9...
Hotspot Total Upload	global			2M	0 bps	0 B	0 B
HS-Upload	Hotspot Total	Paket...	1M	2M	0 bps	0 B	0 B

4 items 18.7 KB queued 30 packets queued

Figure 3. User Importer Tool Test Results

4. Conclusion

The RADIUS (Remote Authentication Dial In User Service) Server is a network server that provides Authentication, Authorization, and Accounting (AAA) services. In summary, this RADIUS Server maintains a user database that may be accessed by clients or users on the same network as the RADIUS Server.

Based on the testing and installation of the system, it can be concluded that users may be authenticated on the network using RADIUS with free RADIUS software linked to Mikrotik as a network access server. It is predicted that user authentication would increase computer network security.

References

- [1] Y. Chandra, N. A.-J. I. System, and undefined 2021, "Wireless Network Security Using WEP (Wired Equivalent Privacy) Method With RC4 Stream Cipher Encryption," *journal.teknikunkris.ac.id*, 2021, Accessed: Mar. 02, 2022. [Online]. Available: <http://journal.teknikunkris.ac.id/index.php/jis/article/download/139/119>
- [2] D. Cahyadi, A. Faturahman, H. Haryani, E. Dolan, and S. millah, "BCS : Blockchain Smart Curriculum System for Verification Student Accreditation," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 65–83, Apr. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/20>

- [3] G. D.-R. energy and undefined 2020, "A survey on smart grid technologies and applications," *Elsevier*, Accessed: Mar. 02, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0960148119312790>
- [4] D. Immaniar, N. Azizah, D. Supriyanti, N. Septiani, and M. Hardini, "PoTS: Proof of Tunnel Signature for Certificate Based on Blockchain Technology," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 101–114, May 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/28>
- [5] T. Ayuninggati, N. Lutfiani, and S. Millah, "CRM-Based E-Business Design (Customer Relationship Management) Case Study: Shoe Washing Service Company S-Neat-Kers," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 216–225, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/58>
- [6] G. Maulani, G. Gunawan, L. Leli, E. Ayu Nabila, and W. Yestina Sari, "Digital Certificate Authority with Blockchain Cybersecurity in Education," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 136–150, May 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/40>
- [7] T. Nurhaeni, N. Lutfiani, A. Singh, W. Febriani, and M. Hardini, "The Value of Technological Developments Based on An Islamic Perspective," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 1–13, Apr. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/4>
- [8] B. Rawat and S. Purnama, "MySQL Database Management System (DBMS) On FTP Site LAPAN Bandung," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 173–179, 2021.
- [9] P. Edastama, A. Dudhat, and G. Maulani, "Use of Data Warehouse and Data Mining for Academic Data: A Case Study at a National University," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 206–215, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/55>
- [10] P. Edastama, A. S. Bist, and A. Prambudi, "Implementation Of Data Mining On Glasses Sales Using The Apriori Algorithm," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 159–172, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/46>
- [11] Y. Durachman, A. Sean Bein, E. Purnama Harahap, T. Ramadhan, and F. Putri Oganda, "Technological and Islamic environments: Selection from Literature Review Resources," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 37–47, Apr. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/12>
- [12] D. Apriani, A. Williams, U. Rahardja, A. Khoirunisa, and S. Avionita, "The Use of Science Technology In Islamic Practices and Rules In The Past Now and The Future," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 48–64, Apr. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/16>

- [13] I. Y. Ruhawati, A. P. Candra, and S. N. Sari, "Design and Build a Multimedia System for Indonesian Religious Activities Based on Android," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 233–239, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/64>
- [14] M. R. Anwar, R. Panjaitan, and R. Supriati, "Implementation Of Database Auditing By Synchronization DBMS," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 197–205, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/53>
- [15] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation Of E-Business Information System In Indonesia : Prospects And Challenges," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 180–188, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/49>
- [16] S. Watini, T. Nurhaeni, and L. Meria, "Development Of Village Office Service Models To Community Based On Mobile Computing," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2 SE-Articles, pp. 189–196, Oct. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/51>
- [17] A. Alwiyah, S. Husin, P. Padel, M. Anggaraeni, and S. Sulistiawati, "Alignment of Science and Technology With Islamic Principles Using Quantum Theory," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 115–120, May 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/32>
- [18] T. Ramadhan, Q. Aini, S. Santoso, A. Badrianto, and R. Supriati, "Analysis of the potential context of Blockchain on the usability of Gamification with Game-Based Learning," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 84–100, Apr. 2021, [Online]. Available: <https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/24>