PCMJ

Progress in Computer and Mathematics Journal (PCMJ)
volume 2 [August, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

DEVELOPING SAFECONNECT MONITOR DEVICE MONITORING AND ALERT SECURITY SYSTEM IN A LOCAL AREA NETWORK (LAN)

Faiezzatul Huda Abdul Fairuz
College of computing, informatics and mathematics
Universiti Teknologi MARA (UiTM) Cawangan Melaka Kampus Jasin
faiezzatulhuda@gmail.com

Article Info

Received: August 2024
Accepted: March 2025
Available Online:
August 2025

Abstract

Within the realm of network security, several security mechanisms, including firewalls, secure configurations, and authentication protocols, are strategically implemented to prevent potential threats such as Denial of Service (DoS) attacks and viruses. However, a critical aspect often overlooked is the comprehensive monitoring of connected devices, leaving potential vulnerabilities that malicious actors can exploit to infiltrate the network.

While various tools and systems are available for managing devices within a network, their functionality often extends beyond mere device monitoring, resulting in sizable data footprints. Moreover, these tools tend to be complex, demanding a level of expertise typically possessed by professional network administrators. This complexity poses a barrier for wider adoption, restricting their utility to a niche audience.

In response to this gap, a more accessible solution is being developed: SafeConnect Monitor. Positioned as a simplified web-based device monitoring system, SafeConnect Monitor aims to provide a streamlined and user-friendly interface. By prioritizing ease of use, this initiative seeks to democratize device monitoring, making it accessible to a broader user base beyond seasoned network administrators. The development of SafeConnect Monitor represents a paradigm shift towards inclusive network security solutions that balance robustness with user-friendly design, ensuring that vigilance over connected devices becomes a more universally achievable goal.

Keywords: Network; Security; Device Monitoring

INTRODUCTION

Device monitoring can be seen as a security approach to supervise connected devices under a network (Alkenani & Nassar, 2022). Most of the time device monitoring is only one of the features in a network monitoring system instead of a single system. In the existing system, there are other features including equipment management, user management, equipment data

collection, data warehousing, failure receiving, traffic monitoring, and device

performance monitoring (E. Safrianti et al.,2021). Companies with an internal network will hire their own network administrator to control every connected device. Monitoring devices that are connected to a network is important to control device activity and maintain network performance. Besides, unauthorized access by unknown devices can also be avoided by implementing this security procedure (Madi et al.,2019). However, small local area networks (LAN) such as home area network usually does not imply this approach. LAN without correct network configuration and thin firewall open a big opportunity to various types of cyber-attack and many malicious activities being performed by the connected devices. Smart devices in a LAN including smart phone, smart television, and smart door lock make the network even weaker (Mazhar et al., 2022).

A system that consists of device monitoring service usually uses Simple Network Monitoring Protocol (SNMP) to help the system to gather information about detected devices in a network. Based on a journal written by Kijazi (2019), the information that can be collected by SNMP protocol are:

a) Name of the detected devices
b) Location of the devices
c) Timestamp of the devices
d) Number of active devices
e) Operating System (OS) version that run in the devices

This information will be stored in SNMP management information base (MIB) and can be accessed by its agent through an agent such as SNMP4J libraries. Using this collected data, users can observe the device's activity. With help from Java programming, users are also able to eliminate unknown devices. When malicious activity is being performed by any of the devices, the system will send an alert notification through a third-party application such as Telegram or Google Mail (Fikri & Nurhaida, 2021).

There are some web applications that similar to this project on the market. One of the web applications is Zabbix. Zabbix is an open-source application that can be used not only to monitor connected devices but also to observe and control network performance in server and application. This monitoring tool uses its own server which is Zabbix-server. Zabbix-agent will perform the monitoring process and Zabbix-proxy will collect the information from the monitoring process and send it to Zabbix-server (Pradana et al., 2022). It also provides a

dashboard that displays graphs based on the data collected after every monitoring process. Zabbix has ability to support large area of network with big amount of end users and systems (Fikri & Nurhaida, 2021). Other than that, Nagios XI, PRTG Network Monitor, and SolarWinds Network Performance Monitor (NPM) are also some of the web applications that have the same functionality. They provide dashboards for users to observe network activities, notification to know status of their network, and remote monitoring to enable users to manage their network from different places.

LITERATURE REVIEW

There are many topics that have been discussed through researching, reading, and reviewing online databases including articles, journals, and conference papers. From this approach, some information can be retrieved to help in developing this system.

Local Area Network (LAN) Architecture

LAN can be divided into two types of architectures which are client-server and peer-to-peer. The classification for these two architectures is based on network traffic dichotomization technology which can be seen through network traffic behavior. It is important to know which LAN layout is being monitored so that the best security strategy can be implemented correctly (D. Yang & M. Chen, 2022).

Client-Server LAN

In a client-server LAN, documents and resources that want to be shared within all client devices will be stored on a centralized device which is also known as a server. In the context of Hypertext Transfer Protocol (HTTP), the client communicates with the server by sending a request message that contains method, content information, and current connection state. After converting the requested domain name into IP address, the server returns a response message that includes the location of requested document (Maschi, Alonso, 2023).

There are a few reasons why this type of LAN architecture is usually applied in small companies and most households. Firstly, this network has faster access speed compared to Peer-to-Peer (P2P) LAN (Slone, 2020). This statement has been proved by A. A. Tuifaiga et al. through a performance comparison between client/server and peer-to-peer in Wireless LAN. Based on figure 1 that shows UDP throughput for both client-server and P2P, IPv4 for

client/server is clearly higher than IPv4 P2P. Client-server LAN architecture has higher bandwidth due to high overheads in sharing packets between client and server.

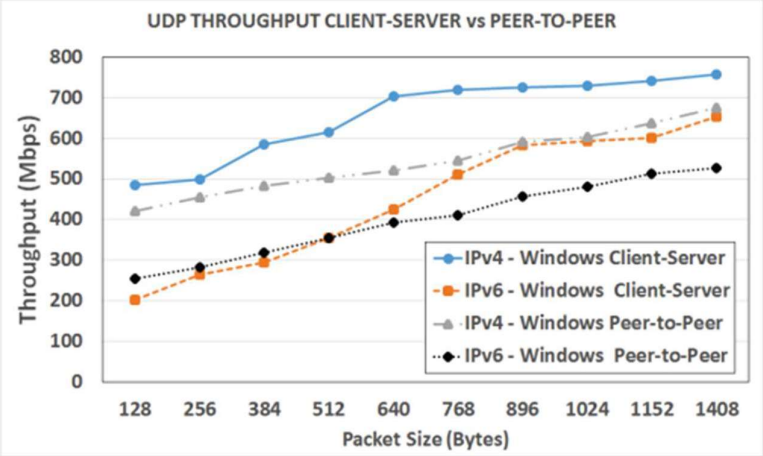

Figure 1: Comparison UDP Throughput between client/server and P2P

(Source: A. A. Tuifaiga et al., 2021)

Furthermore, the centralized routing services allow all activities that have been performed within the network to be tracked and easy to monitor. This also makes upgrading software a simple task. The network administrators can simply upgrade the applications stored on the file server rather than having to physically upgrade each client's device (Slone, 2020).

In the other hand, this centric network also gives an easy gateway access to outsider. Once the server can be accessed, the other connected devices can also be reached. This unauthorized access can bring various threats into the interconnected devices including malicious file injection, unwanted configuration setting modification, and sudden disconnection. With the thin layer of security system, this architecture enhances the attacker to do unwanted activities within the local connection.

Peer-to-Peer LAN

A local area network can be characterized as Peer-to-Peer (P2P) LAN when the users communicate directly with one another through their devices using handshaking process where all devices in the network need to initiate the connection and begin to exchange messages to (K. Kwan et al., 2019). P2P LAN is a distributed LAN architecture that has components or

nodes distributed across various locations rather than being centralized, with users contributing and sharing resources crucial for network services like file sharing. The users contribute and share their own resources, which are essential for providing services and content within the network. Notably, participants can access these shared resources directly from one another without the need for intermediaries or central servers (W. Tushar et al., 2020).

One of the advantages of P2P networks exhibit robustness, as the removal of any single participant does not significantly impact overall network service. This inherent resilience ensures that the departure of individual participants does not cause any significant loss, and the shared services can persist without disruptions. This characteristic highlights the decentralized and self-sustaining nature of P2P architectures, making them well-suited for dynamic and evolving network environments (W. Tushar et al., 2019). Furthermore, this type of LAN is inexpensive and easy to handle. An illustrative example of this efficiency is observed when participants desire to use a common application on their devices. In a P2P connection setup, the application only needs to be installed on one of the devices, and the configured sharing options enable seamless resource utilization among participants. This streamlined approach to resource sharing enhances the user experience and simplifies network management (Slone, 2020).

However, since the devices in P2P LAN need to stay connected to access point (AP) to get the Internet access and other devices in the network at the same time, the users will encounter a few flaws. The devices need to stay in the coverage area otherwise the channel speed will be slow. When a device chooses to stay connected to its current AP despite the availability of a stronger signal from another AP, a sticky client could be created. The absence of centralized technology makes it hard to control and monitor device activities, performance, and security. Additionally, this network layout has throughput limitation. Downlink oversubscription can occur when the required throughput for all users exceeds the channel's maximum capacity, impacting performance. The absence of centralized technology also makes it hard to control and monitor devices' activities, performance, and security (N. D. Mickulicz & P. Narasimhan, 2020).

Devices

There are several methodologies in categorizing types of devices. In a research article written by Hirofumi Noguchi, Misao Kataoka, and Yoji Yamato, they identify the types of a device based on its network information. Different types of devices will communicate differently according to their usage of network. Thus, communication details between the device and Internet can classify devices into their type. There are techniques for device identification based on hardware fingerprints, including radiometric fingerprints. While these methods prove effective in identifying Network Interface Cards (NICs), they require specialized equipment like a radio sensor. Consequently, they may not be practical for cost-effective management of a substantial number of devices (H. Noguchi et al., 2019). Thus, a latest device classification method has been implemented in this project. This new approach uses two methods in categorizing the connected devices which are analysis based on database and analysis based on its network traffic. The proposed method can divide the devices into three categories which are Internet of Things (IoT), Not IoT, and Router (C. Takasaki et al., 2023).

Internet of Things (IoT)

IoT applications require both software and hardware to work well on various devices with different abilities and conditions. They help humans to interact with devices and usually involve sending and analysing big amount of data. As shown in figure 2, the data that has been gathered from IoT devices and sensors need to go through four cross-layers before reach to user's interface. This case can bring to the first security issue of IoT devices which is the data that has been stored in a third party's server will be invisible to users and developers. This can cause unauthorized access to users' private data without they realize (Nada Alhirabi et al., 2021).

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 2 [August, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

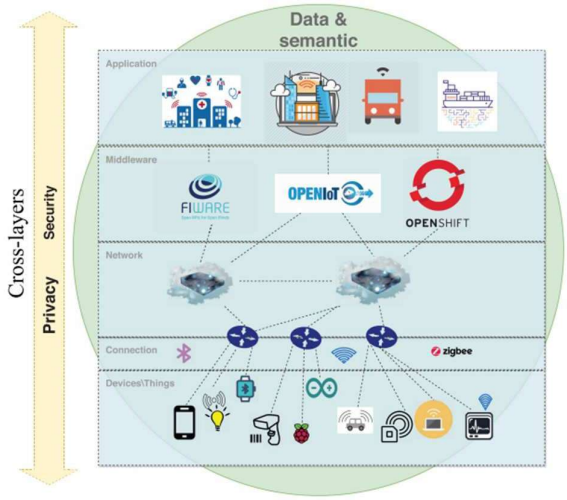

Figure 1: Heterogeneous IoT Framework

(Source: Nada Alhirabi et al., 2021)

Network Monitoring Protocol

The network security of a device monitoring system is considered a critical point in the overall network safety infrastructure. Given the potential threats of cyber warfare, hacking, network intrusion, and various illegal activities, security protection for the devices within the network faces significant pressure. Therefore, it is crucial to implement an efficient protocol that incorporates appropriate technical elements for the monitored network. (Q. Meng et al., 2019).

Simple Network Management Protocol (SNMP)

Device network management is accomplished via the OSI model layer 7 protocol known as Simple Network Management Protocol (SNMP). Network administrators can use this protocol to find and fix device faults and obtain device status information. These days, SNMP allows administrators to manage an enormous number of devices, including workstations, printers, servers, routers, switches, and more. The protocol is made to be able to manage hardware made by different manufacturers and set up on different kinds of physical networks. Stated differently, SNMP spares management duties from considering the physical attributes of devices under its control as well as the fundamentals of networking technology (A. Boyko et al., 2019).

Internet Control Management Protocol (ICMP)

ICMP, also can be referred as RFC 792, serves the purpose of reporting internet errors and sending notification messages. Its lightweight nature makes it convenient for identifying network issues, and the well-known application Ping is implemented based on ICMP, available on all operating systems. Numerous research endeavours leverage this protocol to assess the status of network devices for security purposes. Specifically, ICMP is employed to create a notification system for detecting the status of wireless access points used in the public internet service provided by Sansai municipality (K. Kantawong et al., 2022).

ICMP operates in conjunction with IP protocols to report error messages encountered while sending packets to native hosts. It encompasses various types, and Ping is an application that utilizes ICMP. The ICMP Echo service header has a packet size of 8 bytes, and the Type field distinguishes between an echo request (Type 8) and an echo reply (Type 0).

METHODOLOGY

For this project, Agile model has been chosen to be implemented. Agile models, also referred to as the change-driven life cycle, are characterized as a fast and incremental iterative model. In this approach, the scope of the software project takes shape during its execution. The strategy involves creating the minimum viable product (MVP) in the initial iteration and progressively incorporating additional features and functionality in subsequent iterations (Almazaydeh et al., 2022). This model consists of five stages which start with design, develop, test, release, and plan and it continually repeated as the requirements change.

Table 1: Project formulation table

Stage	Activities	Deliverables
Plan	• Planning the software features with its functionality. • Analyzing requirements needed through articles reading.	• Network monitoring protocol. • Local Area Network (LAN) characteristics. • Device behavior in LAN. • Comparison between existing similar applications. • Development methodology. • Use case diagram.

Design	• Mapping out flowchart and entity relationship diagram (ERD).	• Flowchart diagram • ERD • UI design
Develop	• Designing user interface. • Developing functional user interface. • Building module and functions. • Developing device monitoring system. • Developing real-time database system.	• Device monitoring system.
Test	• Running system testing on the developed application. • Correcting the detected error. • Identifying if the stated monitoring protocol works well.	• System testing result.
Release	Letting users use the application and ask for feedback from the users.	

RESULT AND DISCUSSION

After going through the planning, designing, and developing phases, the user interface of SafeConnect Monitor was successfully being built. This system consists of nine interfaces which are:

a) Landing Page
b) Registration Page
c) Login Page
d) Network Registration Page
e) Network Information Form
f) Dashboard Page
g) Connected Devices Page
h) Alert Notification Page
i) Profile Page

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 2 [August, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

System Testing

System testing aims to evaluate both functionality and performance of complete software. There are eight steps that need to be taken to make sure the tested software can be analyzed.

Build a Test Environment

The test environment consists of one wireless router and three devices which are a mobile phone, a tablet, and a laptop. For the router, the firewall for IPv4 already has been disabled to make the information from the MIB is transparent.

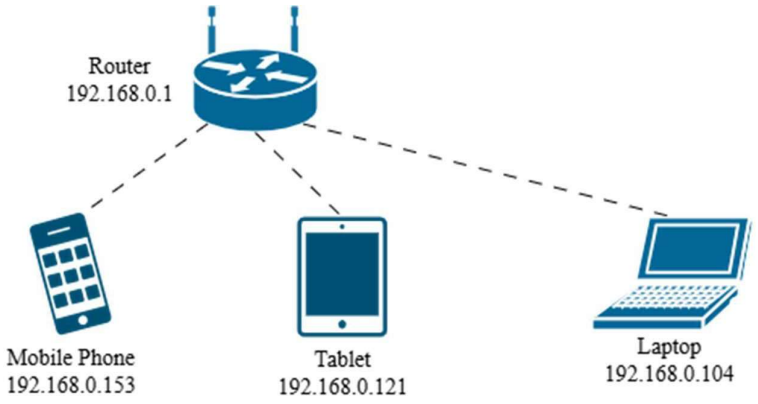

Figure 3: Network Diagram of Test Environment

Create Test Data

The following table is the information that was being collected from the devices in the test environment. This information is supposed to be received by the system, saved into the database, and displayed in the user interface.

Table 2: Network Information Test Data

	Test Data
Name (SSID)	TP-Link_E09A
MAC Address	90-0F-0C-E5-57-BD
IP Address	192.168.0.1
Type	Public
Speed	30Mbps

PCMJ
Progress in Computer and Mathematics Journal (PCMJ)
volume 2 [August, 2025]
e-ISSN: 3030-6728
Website: fskmjebat.uitm.edu.my/pcmj

Table 3: Devices Information Test Data

Devices' name	IP address	Type	Status
DELL Inspiron	192.168.0.104	Laptop	Online
Huda's A51	192.168.0.123	Mobile	Online
iPad	192.168.0.121	Mobile	Online

Run the Test

This testing will run automatically in Nagios XI using a provided configuration wizard, 'Website URL'. This service requires the user to fill in a form with the URL of the system (http://safeconnect2.test/), the host name (localhost) and the IP address of the host (127.0.0.1). After filling in this form, Nagios XI will take some time, in this case, nearly an hour, to produce an overview with a summary of the system's performance. In figure 4, the status of the website is stated a 'OK' with 0% of lost services.

Service Status for this Host Last updated: 2024-07-17 05:15:45

Service	Status	Duration	Attempt	Last Check	Status Information
Current Load	Ok	3d 6h 27m 26s	1/4	2024-07-17 05:11:00	OK - load average: 0.23, 0.80, 0.99
Current Users	Ok	3d 7h 8m 7s	1/4	2024-07-17 05:11:43	USERS OK - 0 users currently logged in
HTTP	Ok	3d 7h 7m 42s	1/4	2024-07-17 05:12:18	HTTP OK: HTTP/1.1 200 OK - 2798 bytes in 0.003 second response time
Memory Usage	Ok	3d 7h 7m 15s	1/4	2024-07-17 05:13:08	OK - 835 / 1743 MB (47%) Free Memory, Used: 1199 MB, Shared: 143 MB, Buffers + Cached: 433 MB
PING	Ok	3d 7h 6m 52s	1/4	2024-07-17 05:14:14	PING OK - Packet loss = 0%, RTA = 0.30 ms
Root Partition	Ok	3d 7h 6m 27s	1/4	2024-07-17 05:14:48	DISK OK - free space: / 32546 MiB (85.99% inode=99%):
SSH	Ok	3d 7h 6m 2s	1/4	2024-07-17 05:15:11	SSH OK - OpenSSH_8.7 (protocol 2.0)
Service Status - crond	Ok	3d 7h 5m 37s	1/4	2024-07-17 05:10:51	• crond.service - Command Scheduler
Service Status - httpd	Ok	3d 7h 5m 12s	1/4	2024-07-17 05:11:19	• httpd.service - The Apache HTTP Server
Service Status - mysqld	Ok	3d 7h 4m 47s	1/4	2024-07-17 05:12:12	• mysqld.service - MySQL 8.0 database server
Swap Usage	Ok	3d 7h 4m 20s	1/4	2024-07-17 05:12:39	SWAP OK - 87% free (1794 MB out of 2067 MB)
Total Processes	Ok	3d 7h 4m 5s	1/4	2024-07-17 05:13:23	PROCS OK: 95 processes with STATE = RSZDT

Figure 4: Result from System using Nagios XI

Identify System Defect

Despite the successful result of the system's performance, the SNMP protocol still cannot be implemented correctly. The network information that saved in the database is not match with the created test data. The comparison can be seen in table 4.

Table 4: Comparison between Test Data and Received Data

	Test Data	**Received Data**
Name (SSID)	TP-Link_E09A	TP-Link_E09A
MAC Address	90-0F-0C-E5-57-BD	90-0F-0C-E5-57-BD
IP Address	192.168.0.1	192.168.0.1
Type	Public	Public
Speed	30Mbps	null

Regression Testing

The system is being tested by running the system with the mentioned defect. The side effect of the defect is the field for speed in the network information table is blank.

Log Defects

This step allows the developer to fix the defect. This system will use an API from Nagios XI through a configuration wizard, 'SNMP Walk'. This service will send 'snmpwalk' command remotely through the API that will be implemented in SafeConnect Monitor system.

Retest

After applying the solution, the system needs to be tested again by comparing the output from the system and the test data to make sure the received information is accurate.

CONCLUSION

Most people are aware of the importance of security mechanisms implementation in their network, but they did not know what to do. SafeConnect Monitor, a device monitoring system provides a straightforward solution that comes with a use-friendly interface. This system utilizes SNMP protocol, enabling it to serve formative details about devices under a network that is being monitored. By leveraging the SNMP protocol, it not only monitors network devices but also facilitates proactive device management. Users can easily view and resolve

problems, ensuring their network remains secure and efficient. The ability to terminate device connections remotely is particularly valuable for maintaining network integrity and preventing unauthorized access.

Furthermore, there is a dashboard that is designed to provide users with real-time insights into the collected data including the number of devices and the number of issues that currently occur. This feature allows users to quickly analyze the level of security of their network and take immediate action if any issues arise. Detailed information about connected devices and current issues that also provided in the system helps users stay informed and make data-driven decisions to enhance their network security.

Hence, SafeConnect Monitor offers a comprehensive and user-friendly solution for network monitoring and management. Its use of the SNMP protocol, combined with a clear and informative dashboard, empowers users to maintain a secure and efficient network. By providing both detailed device information and remote management capabilities, this system addresses the common challenge of network security implementation, making it an invaluable tool for users seeking to protect their digital infrastructure.

REFERENCES

A. A. Tuifaiga, P. A. Ram and S. S. Kolahi, "Performance Comparison of IPv6 in 802.11ac WLAN in Windows and Linux Environment," TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON), Auckland, New Zealand, 2021, pp. 799-804, doi: 10.1109/TENCON54134.2021.9707449.

A. Boyko, V. Varkentin and T. Polyakova, "Advantages and Disadvantages of the Data Collection's Method Using SNMP," 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2019, pp. 1-5, doi: 10.1109/FarEastCon.2019.8934069.

Alkenani, J., & Nassar, K. A. (2022). Network Monitoring Measurements for Quality of Service: A review. Iraqi Journal for Electrical and Electronic Engineering, 18(2). https://doi.org/10.37917/ijeee.18.2.5

Almazaydeh, L., Alsafasfeh, M., Alsalameen, R., & Alsharari, S. (2022). Formalization of the prediction and ranking of software development life cycle models. International Journal of Power Electronics and Drive Systems, 12(1), 534. https://doi.org/10.11591/ijece.v12i1.pp534-540

C. Takasaki, T. Korikawa, K. Hattori and H. Ohwada, "Traffic Behavior-based Device Type Classification," 2023 International Conference on Computing, Networking and

Communications (ICNC), Honolulu, HI, USA, 2023, pp. 353-357, doi: 10.1109/ICNC57223.2023.10074041.

D. Yang and M. Chen, "A Classification Method for Network Applications using BP Neural Network," 2022 International Conference on Informatics, Networking and Computing (ICINC), Nanjing, China, 2022, pp. 233-237, doi: 10.1109/ICINC58035.2022.00054.

E. Safrianti, L. O. Sari and N. A. Sari, "Real-Time Network Device Monitoring System with Simple Network Management Protocol (SNMP) Model," 2021 3rd International Conference on Research and Academic Community Services (ICRACOS), Surabaya, Indonesia, 2021, pp. 122-127, doi: 10.1109/ICRACOS53680.2021.9701973.

Fikri, M.H., & Nurhaida, I. (2021). Pemantauan Jaringan Menggunakan Nagios Dan Zabbix Dengan Notifikasi Telegram Messenger Dan Google Mail. Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer. Hayyy

H. Noguchi, M. Kataoka and Y. Yamato, "Device Identification Based on Communication Analysis for the Internet of Things," in IEEE Access, vol. 7, pp. 52903-52912, 2019, doi: 10.1109/ACCESS.2019.2910848.

K. Kantawong, S. Chaichumpa, S. Pravesjit and M. Yaibuates, "A Lightweight Framework for Retrieve IP Device Status Based on MQTT Protocol," 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Chiang Rai, Thailand, 2022, pp. 46-49, doi: 10.1109/ECTIDAMTNCON53731.2022.9720332.

K. Kwan and B. Greaves, "FileLinker: Simple Peer-to-Peer File Sharing Using Wi-Fi Direct and NFC," 2019 IST-Africa Week Conference (IST-Africa), Nairobi, Kenya, 2019, pp. 1-9, doi: 10.23919/ISTAFRICA.2019.8764840.

Nada Alhirabi, Omer Rana, and Charith Perera. 2021. Security and Privacy Requirements for the Internet of Things: A Survey. ACM Trans. Internet Things 2, 1, Article 6 (February 2021), 37 pages. https://doi-org.ezaccess.library.uitm.edu.my/10.1145/3437537

Pradana, A., Widiasari, I.R., & Efendi, R. (2022). Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix Berbasis SNMP. AITI.

Q. Meng, D. Li and Y. Ma, "Research and Application Based on Network Security Monitoring Platform and Device," 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), Chengdu, China, 2019, pp. 716-719, doi: 10.1109/ISGT-Asia.2019.8881520.

W. Tushar, T. K. Saha, C. Yuen, D. Smith and H. V. Poor, "Peer-to-Peer Trading in Electricity Networks: An Overview," in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3185-3200, July 2020, doi: 10.1109/TSG.2020.2969657.

Slone, J. P. (2020). Local Area Network Handbook, Sixth Edition. CRC Press.