JURNAL INFOTEL
Informatics - Telecommunication - Electronics
Website: http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN: 2085-3688; e-ISSN: 2460-0997

A fire suppression monitoring system for smart building

I Ketut Agung Enriko[1,*], Angela Niarapika Nababan[2], Adian Fatchur Rochim[3], Sri Kuntadi[4]
[1,2]Institut Teknologi Telkom Purwokerto
[3]Universitas Diponegoro
[4]PT. Telkom Indonesia
[1,2]Jl. D. I. Panjaitan, No. 128, Purwokerto 53147, Indonesia
[3]Jl. Prof. Sudarto No. 13, Tembalang, Semarang 50275, Indonesia
[4]Jl. Gatot Subroto Kav 52, Jakarta Selatan 12710, Indonesia
[*]Corresponding email: enriko@ittelkom-pwt.ac.id

Received 1 April 2023, Revised 21 May 2023, Accepted 30 May 2023

Abstract — A fire suppression system (FSS) monitoring system is a system to monitor the FSS devices' status since FSS is a critical system for responding to fire disasters. The FSS device to be monitored is the hydrant system, which is a water pump system to spray water at high pressure in case of a fire accident. The monitoring system collects data on important parameters like water pressure, main power status, and backup power status. It is built with an Internet of things (IoT) capability. Data are collected from the FSS module and sent to the IoT platform through Wi-Fi based Internet connection. Then the data will be displayed in a simple dashboard application. In this research, a quality of service (QoS) assessment framework is performed to check the performance of the FSS monitoring system. The framework name is TIPHON, a QoS standard issued by European Telecommunication Standard Institute (ETSI). TIPHON consists of five parameters of assessment: bandwidth, throughput, packet loss, delay, and jitter. For each parameter aspect, this study results as follows: (1) bandwidth performance is "very good" (score = 4), (2) throughput performance is "bad" (score = 1) since typical IoT use cases only send data in small size, (3) packet loss performance is "very good" (score = 4), delay performance is "very good" (score = 4), and jitter is "good" (score = 3). The overall score for the FSS system using the TIPHON standard is 3.2 or categorized as "good".

Keywords – fire suppression system, hydrant monitoring, internet of things, quality of service

I. Introduction

A fire disaster is one of the fatal accidents that should be prevented because it causes death, injuries, and financial loss. A recent study mentioned that in 2019, more than 3 million fire accidents happened, causing 19 thousand deaths and more than 60 thousand injuries [1]. Those accidents happened in various places like forests, peat, buildings, and others, where building fire is one of the main causes. Some causes of fire accidents have been recorded in some studies. For example, from [2], there are several causes of fire: appliances, candles, decorations, electricity, and smoke.

Nowadays, many buildings, especially office buildings, have fire alarm systems that will announce an alert if a fire accident happens. An example of a fire alarm system (FAS) diagram is depicted in Fig. 1 [3]. Typically, a FAS is connected to smoke sensors, heat sensors, and manual call points. A smoke sensor detects the presence of smoke as an early warning system for possible fire occurs [4], and a heat sensor is a device to detect abnormal heat that can be suspected as fire presence [5]. Meanwhile, a manual call point (MCP) is a special button on the wall that should be pressed in case of a fire breakout [6].

A FAS is used to connect to a fire suppression system to make a comprehensive system. A fire suppression system (FSS) is a system to sprinkle water when a fire breakout happens [7], sometimes located indoors or outdoors (hydrant system). A fire suppression system is added to a fire alarm system as an actuator, and it works to sprinkle water when a fire is detected [8]. Fig. 2 describes a complete FAS with an FSS as its actuator, besides other sensors as mentioned in the previous figure.

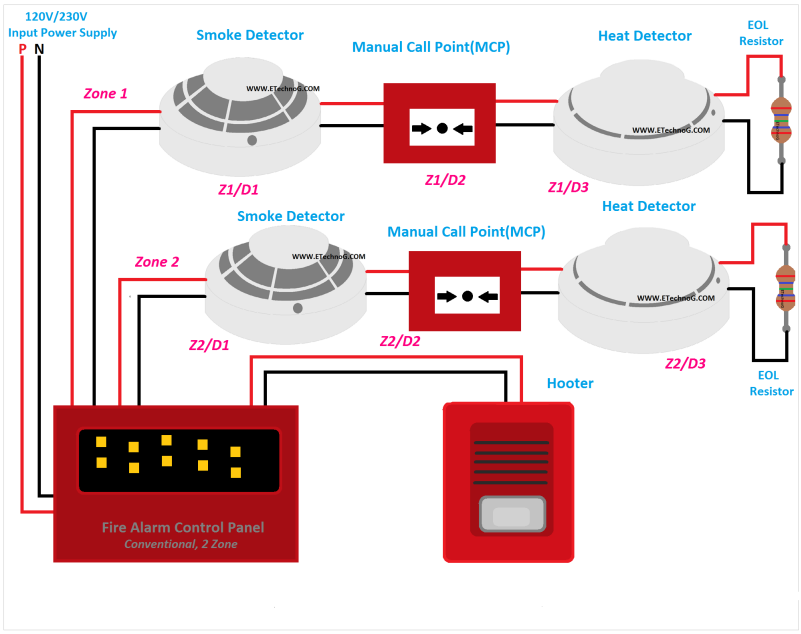

Fig. 1. A typical fire alarm system wiring diagram.

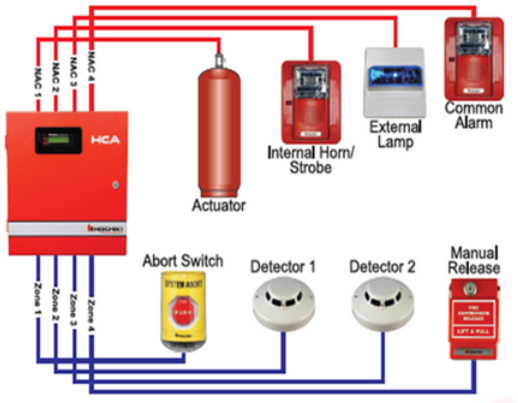

Fig. 2. A complete fire alarm system with a fire suppression system as an actuator [9].

FAS technology is also enhancing in line with the advancements in electrical engineering and information systems technologies. A FAS is no longer a conventional wired-based system but already improved with an addressable system. An addressable FAS operates digitally, where every device is connected to a fire alarm control panel with digital signals [10]. Meanwhile, traditional fire alarms work based on electrical currents. Basically, they have only two states: normal or fire, without knowing where the fire occurs [11].

With digital systems, addressable FAS has some benefits: (1) The exact location of an alarm can be determined as an individual sensor has its address, (2) The use of digital signal gives better speed and accuracy, (3) It has an isolation module to prevent a part damaging other parts, and (4) There is a communication protocol between the control panel and each sensor [3]. The addressable FAS also provides the possibility to be enhanced with an automatic monitoring system, for instance.

One important part of the FAS is the fire suppression or sprinkler systems. If a fire accident happens, it reacts with sprinkling water in the alarm area. If it fails to react, the fire can spread quickly and burns the entire building. To check the condition of a sprinkler system, a safety officer should monitor it regularly by inspecting the parameters in the control panel, usually in the basement. Some important parameters that should be checked are water pressure and the supporting facilities to maintain the water pressure [12].

This study aims to develop a monitoring system for an FSS using the Internet of things (IoT) technology. With this feature, the status of an FSS can be monitored in real-time, thus giving more safety and reducing the dependency on human resources works. The monitoring system collects data from the FSS control panel, sends them to an IoT platform through internet access, and visualizes the result on a website application. With this IoT-based monitoring system, the building management can monitor the FSS status in real-time, and detect problems as soon as possible, so they can guarantee the FSS system is reliable and in good condition.

Some previous studies have been done related to this topic. The first is from [13] where the authors investigated the performance of fire suppression systems in shopping centers in Australia. Another research is [14], where an automated monitoring system for a fire alarm in certain buildings is presented. The system is developed with Zigbee communication, and the alarm can be sent to the fire department for quick response. Meanwhile, using Bayesian Network analysis, [15] discussed the modeling (systematic review) of fire risk regarding the technical, human, and organizational aspects. The last paper to be discussed

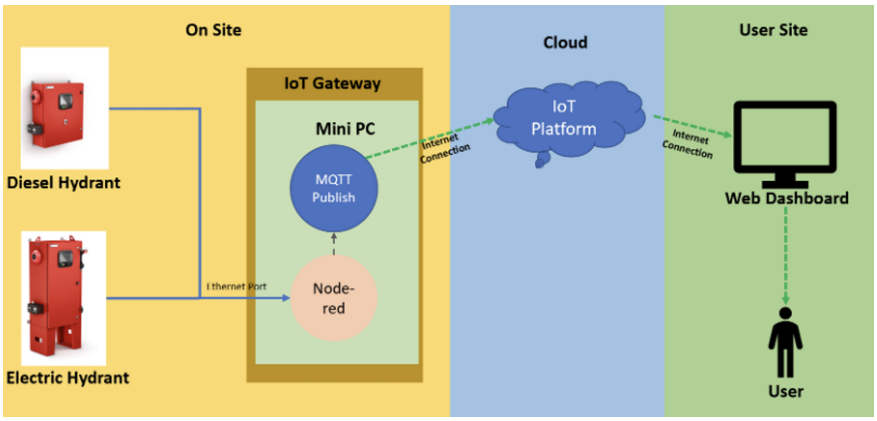

Fig. 3. Architecture of the IoT-based FSS monitoring system.

here [16] focused on developing an Arduino-based fire alarm system using GSM connectivity. The system had already been successfully deployed as a prototype.

This paper is organized as follows: the introduction is in section I, the research method is in section II, the result is in section III, the discussion is in section IV, and the conclusion is in section V.

II. Research Method

This section discusses the system architecture and the flowchart of IoT-based FSS monitoring system.

A. System Architecture

The basic architecture of the fire suppression system follows the common IoT architecture or value chain, which consists of four elements: device, network, platform, and application. The architecture of FSS monitoring in this study is depicted in Fig. 3. On the device side, an IoT gateway (mini-PC) is connected to the FSS panel for data collection purposes. In this research, an FSS panel from the Tornatech brand is used. The data collected are water pressure, main power status, and backup power status (diesel generator). These data are collected and processed using Node-RED software.

Then the data will be sent using the MQTT protocol using a Wi-Fi connection. MQTT protocol is used since it is lightweight, bandwidth efficient, and commonly used in IoT applications [17]. This is where the network element works in a typical IoT system, including in this research. Hereafter, the data will be received on the IoT platform, which is the platform element of the IoT value chain. The IoT platform is an MQTT broker that gathers all data, stores it in a data base, and creates the application programming interface (API) to be consumed by a website/mobile application. The last element is the application, a user interface for people who use the IoT application. Authorized officers will use the website application created in this project to monitor the FSS status, and it also provides certain notifications if there is an abnormal status.

B. Flowchart

Fig. 4 explains how this FSS monitoring system works. First, the IoT gateway or mini-PC requests data from the FSS control panel, which consists of water pressure, main voltage, and backup voltage. If the request is fulfilled, those data will be coded into a string format and joined together. Then the IoT gateway will try to connect to the IoT platform (MQTT broker) through the MQTT protocol. If it succeeds, it sends all the data through the Internet cloud. The last process is where the website application consumes the data from the IoT platform to be visualized for monitoring.

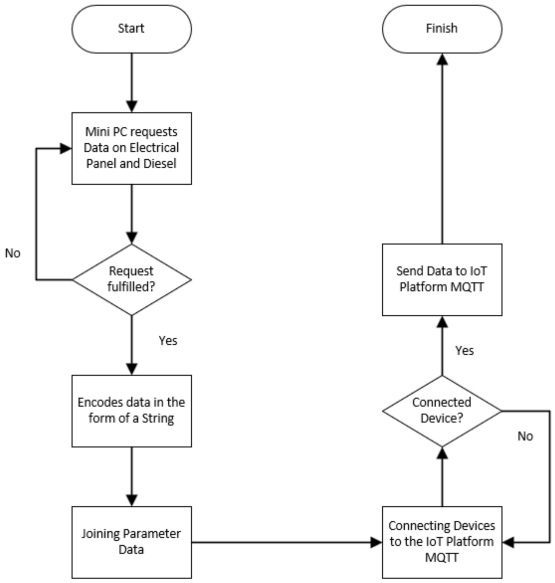

Fig. 4. Flowchart of the IoT-based FSS monitoring system.

III. Result

The FSS monitoring system has been successfully developed completely from data colthe lection process to a website application. Fig. 5 depicts the physical look of FSS monitoring's device implementation. The IoT gateway has been connected to the FSS pamain and backup.

Fig. 5. Physical look of an FSS monitoring device (A: FSS main panel, B: IoT gateway, C: FSS backup panel).

The device can already send the FSS status from the FSS panel to the IoT platform through an internet connection, and a website application is already created. A screenshot of the FSS monitoring website is drawn in Fig. 6.

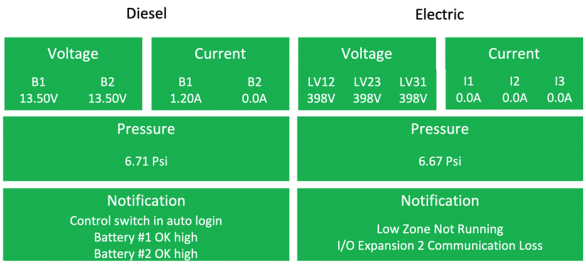

Fig. 6. A screenshot of the FSS monitoring website application.

In the picture, it can be seen all the status of important parameters in FSS like the voltage, current, and pressure from the main power ("Electric") and backup ("Diesel"). At the bottom side, the "Notification" menu is displayed to inform the overall status of the FSS, like, the control switch and battery status.

IV. Discussion

For analysis purposes, the TIPHON (which stands for Telecommunication and Internet Protocol Harmonization Over Networks [18]) standard is used to quantify whether the FSS monitoring works well from the quality of service (QoS) aspect. TIPHON standard consists of five parameters: bandwidth, throughput, delay, packet loss, and jitter [19]–[21]. TIPHON's measurements are concluded in the QoS parameter index in Table 1.

Table 1. TIPHON QoS Parameter Index

Value	Percentage (%)	Index
3.8 - 4	95 - 100	Very Good
3 - 3.79	75 - 94.75	Good
2 - 2.99	50 - 74.75	Not Good
1 - 1.99	25 - 49.75	Bad

This table can be filled after all parameters' quality has been investigated.

First, Table 2 is the reference for the bandwidth parameter to determine the QoS for this aspect. Nonetheless, the bandwidth parameter, in many cas can be ignored since, nowadays, internet access quality is already good.

Table 2. Bandwidth Parameter Index

Bandwidth (Mbps)	Category	Index
$>$ 2.1	Excellent	4
$>$ 1.2 - 2.1	Good	3
$>$ 0.7 - 1.2	Fair	2
0 - 0.7	Bad	1

Next, for the throughput parameter, the throughput formula is shown in (1).

$$\text{Throughput}(Kbps) = \frac{\text{Packet received}(Kb)}{\text{Transmit time}(s)} \quad (1)$$

The throughput value from (1) can be converted to a percentage compared to the bandwidth available in the network, as seen in (2).

$$\text{Throughput}(\%) = \frac{\text{Throughput}(Kbps)}{\text{Bandwidth}(Kbps)} \times 100\% \quad (2)$$

From the throughput formula, it can be inferred that if the data sent to the internet bandwidth is relatively small (typical in IoT use cases), the throughput result will always be small. The standard of throughput for the QoS index is shown in Table 3.

Table 3. Throughput Parameter Index

Throughput (%)	Category	Index
76 - 100	Very Good	4
51 - 75	Good	3
26 - 50	Fair	2
0 - 25	Bad	1

Next, for the packet loss parameter, the standard is shown in Table 4.

Table 4. Packet Loss Parameter Index

Packet Loss (%)	Category	Index
0 - 2	Very Good	4
3 - 14	Good	3
15 - 24	Fair	2
$\geq$ 25	Bad	1

Meanwhile, the delay parameter standard is shown in Table 5.

Table 5. Delay Parameter Index

Delay (ms)	Category	Index
$<$ 150	Very Good	4
150 - 300	Good	3
300 - 450	Fair	2
$>$ 450	Bad	1

Last, the jitter parameter standard is shown in Table 6.

To check the QoS of the system, the first parameter to be checked is bandwidth. Since the system uses 10 Mbps internet access, the index value for this parameter is "4" or excellent.

The next parameter is throughput, which for evaluation purposes, 100 data have been collected and processed with Wireshark. The data sample for throughput parameters are shown in Table 7.

Table 6. Jitter Parameter Index

Delay (ms)	Category	Index
< 150	Very Good	4
150 - 300	Good	3
300 - 450	Fair	2
> 450	Bad	1

Table 7. Throughput Measurement Result

Data	Data Sent (Kb)	Transmit Time (s)	Throughput (Kbps)
1	3.87	0.18	21.46
2	3.48	0.18	19.32
3	3.04	0.18	16.87
4	3.73	0.18	20.63
5	3.55	0.18	19.70
6	3.89	0.18	21.56
7	3.78	0.18	21.05
8	4.63	0.18	25.70
9	6.25	0.18	34.67
10	3.56	0.18	19.72
...	...	...	...
100	2.89	0.18	16.06

The average of 100 throughput data is 19.54 Kbps, or compared to the bandwidth is 0.2 %. Thus, this result falls into the "bad" category or index = 1. Nonetheless, this parameter can sometimes be ignored in IoT use cases since, usually, the IoT sensors send a very small data payload.

Next, for packet loss evaluation, the packet loss data have been collected and shown in Table 8.

Table 8. Packet Loss Measurement Result

Data	Data Sent (Bytes)	Data Received (Bytes)	Packet Loss (%)
1	2764	2764	0
2	2467	2467	0
3	2279	2279	0
4	3041	3041	0
5	2455	2455	0
6	2664	2664	0
7	2878	2878	0
8	2959	2959	0
9	3666	3666	0
10	2471	2471	0
...	...	...	...
100	2512	2512	0

From Table 8, packet loss for all 100 data is 0, or there is no packet loss in all transactions. This performance is achieved since, for the internet connection, a fiber optic broadband network is used to assure network reliability. Therefore, this is a perfect condition for IoT data transmission, which yields an index = four or very good for the packet loss parameter.

The next QoS parameter to be analyzed in this research is a delay. The data for delay measurements are shown in Table 9.

From delay measurement results the delay time for all 100 measurements is 74.76 ms in average. This yields a very good result for IoT data transmission, ince it is below 150 ms as the threshold of very good category (index = 4) in the delay parameter.

The last QoS parameter to be checked is jitter. The jitter measurement is done for 100 data collection, and

Table 9. Delay Measurement Result

Data	Payload (Bytes)	Delay (ms)
1	2764	65.24
2	2467	73.10
3	2279	78.99
4	3041	59.40
5	2455	73.45
6	2664	67.81
7	2878	62.44
8	2959	60.94
9	3666	49.19
10	2471	73.10
...	...	...
100	2512	71.80

the data samples are shown in Table 10.

Table 10. Jitter Measurement Result

Data	Payload (Bytes)	Jitter (ms)
1	2764	65.26
2	2467	73.12
3	2279	79.03
4	3041	59.42
5	2455	73.48
6	2664	67.83
7	2878	62.47
8	2959	60.96
9	3666	49.20
10	2471	73.13
...	...	...
100	2512	71.83

From 100 collected data, the average jitter value is 74.79 ms or categorized as good (index = 3).

The resume of QoS measurements for this FSS monitoring system is shown in Table 11.

Table 11. FSS QoS Mesurement Results

Parameter	Result	Index	Category
Bandwidth	10 Mbps	4	Very Good
Throughput	0.2 %	1	Bad (can be ignored)
Packet Loss	0	4	Very Good
Delay	74.76 ms	4	Very Good
Jitter	74.79 ms	4	Good

The average value for TIPHON parameters is 3.2 (or "good"), while if the throughput parameter is ignored, the average will be 3.75 (still "good").

V. Conclusion

A fire suppression system (FSS) monitoring system is needed to monitor the device's status since FSS is a critical system to rfor respondingfire disasters. The monitoring system collects data on important parameters: water pressure, main power status, and backup power status. The FSS monitoring system is built with an IoT capability. Data are collected from the FSS module and sent to the IoT platform through Wi-Fi based Internet connection. Then the data will be displayed in a dashboard application. A QoS assessment framework is referred to and performed to check the performance of the FSS monitoring system, namely the TIPHON framework. The results of TIPHON QoS with 100 data samples for each measurement are (1)

Bandwidth = 10 Mbps or QoS Index = 4 (categorized as "very good"), (2) Throughput = 0.2 % or QoS Index = 1 ("bad", but in IoT use cases this parameter sometimes is ignored), (3) Packet loss = 0 or QoS Index = 4 ("very good"), (4) Delay = 74.76 ms or QoS Index = 4 ("very good"), and (5) Jitter is 74.79 ms or QoS Index = 3 ("good"). The overall grade of the FSS monitoring system performance is 3.2 (or 3.75 if the throughput parameter is omitted), categorized as "good".

For future work, the study should discuss other paranother partSS system, for example, fire alarm control panel. With this feature, the FSS monitoring system will be more comprehensive, making the building safety system more reliable.

ACKNOWLEDGMENT

This work is supported by a grant from PT. Telkom Indonesia and The Indonesia Telecommunication and Digital Research Institute (ITDRI) task force.

REFERENCES

[1] N. N. Brushlinsky, M. Ahrens, S. V. Sokolov, and P. Wagner, *World Fire Statistics*. Technical report 21. Center of Fire Statistics, Int. Assoc. of Fire and Rescue Services, 2016.

[2] Eastern Kentucky University, "The 10 Most Common Causes of House Fires," EKU Online, 2022.

[3] ETechnoG, "What is Addressable Fire Alarm System? Wiring Diagram," ETechnoG Online, 2022.

[4] S. Wang, X. Xiao, T. Deng, A. Chen, and M. Zhu, "A Sauter mean diameter sensor for fire smoke detection," *Sensors and Actuators, B Chem.*, vol. 281, no. May 2018, pp. 920–932, 2019, doi: 10.1016/j.snb.2018.11.021.

[5] S. Antonov and K. Grozdanov, "Investigation of operation of heat sensor located on the ceiling," in *Proc. 2021 6th Int. Symp. Environ. Energies Appl. EFEA 2021*, pp. 0–3, 2021, doi: 10.1109/EFEA49713.2021.9406227.

[6] S. Granda and T. M. Ferreira, "Assessing vulnerability and fire risk in old urban areas: Application to the historical centre of guimarães," *Fire Technol.*, vol. 55, no. 1, pp. 105–127, 2019, doi: 10.1007/s10694-018-0778-z.

[7] M. Rashid, R. P. Dhakal, and T. Z. Yeow, "Automatic fire sprinkler systems: An overview of past seismic performance, Design Standards & Scope for Future Research," in *2018 NZSEE Conference*, 2018.

[8] W.-Y. Liu, C.-H. Chen, Y.-L. Shu, W.-T. Chen, and C.-M. Shu, "Fire suppression performance of water mist under diverse desmoking and ventilation conditions," *Process Saf. Environ. Prot.*, vol. 133, pp. 230–242, 2020, doi: 10.1016/j.psep.2019.10.019.

[9] M. Engineering, "Fire supression system," MIS Engineering Online, 2020.

[10] High Rise Security Systems LLC, "Fire alarm systems: How does an addressable fire alarm system work," HRSS Online, 2021.

[11] P. J. Y. Piera and J. K. G. Salva, "A wireless sensor network for fire detection and alarm system," in *2019 7th Int. Conf. Inf. Commun. Technol. ICoICT 2019*, pp. 1–5, 2019, doi: 10.1109/ICoICT.2019.8835265.

[12] S. A. Abdulrahman, K. Chetehouna, A. Cablé, Ø. Skreiberg, and M. Kadoche, "A review on fire suppression by fire sprinklers," *J. Fire Sci.*, vol. 39, no. 6, pp. 512–551, 2021, doi: 10.1177/07349041211013698.

[13] K. A. M. Moinuddin, J. Innocent, and K. Keshavarz, "Reliability of sprinkler system in Australian shopping centres –A fault tree analysis," *Fire Saf. J.*, vol. 105, no. February, pp. 204–215, 2019, doi: 10.1016/j.firesaf.2019.03.006.

[14] C. Xinhao, W. Siqi, and H. Chenghao, "Design of fire alarm system with automatic position," in *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, 2020, pp. 141–144.

[15] S. Tan and K. Moinuddin, "Systematic review of human and organizational risks for probabilistic risk analysis in high-rise buildings," *Reliab. Eng. Syst. Saf.*, vol. 188, no. February, pp. 233–250, 2019, doi: 10.1016/j.ress.2019.03.012.

[16] N. N. Mahzan, N. I. M. Enzai, N. M. Zin, and K. S. S. K. M. Noh, "Design of an arduino-based home fire alarm system with GSM module," in *J. Phys. Conf. Ser.*, vol. 1019, no. 1, 2018, doi: 10.1088/1742-6596/1019/1/012079.

[17] A. P. Haripriya and K. Kulothungan, "Secure-MQTT: An efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things," *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1402-8.

[18] E. Setyaningsih, S. D. Hariyanto, D. Wahyuningtyas, and S. Kristiana, "Performance improvement of the shredder machines using IoT-based overheating controller feature," *J. Infotel*, vol. 14, no. 4, pp. 329–337, 2022, doi: 10.20895/infotel.v14i4.812.

[19] A. Hafiz and D. Susianto, "Analysis of internet service quality using internet control message protocol," in *J. Phys. Conf. Ser.*, vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012055.

[20] A. Charisma, A. D. Setiawan, G. M. Rahmatullah, and M. R. Hidayat, "Quality of Service (QoS) on 4G telkomsel networks in Soreang," in *2019 IEEE 13th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2019, pp. 145–148.

[21] R. Ratnasih, D. Perdana, and Y. G. Bisono, "Performance analysis and automatic prototype aquaponic of system design based on internet of things (IoT) using MQTT protocol," *J. Infotel*, vol. 10, no. 3, p. 130, 2018, doi: 10.20895/infotel.v10i3.388.