Comparative analysis on virtual private network in the internet of things gateways

Mohd Idzaney Zakaria[1,2], Mohd Natashah Norizan[1,3], Muammar Mohamad Isa[1,2], Mohd Faizal Jamlos[4], Muslim Mustapa[1]
[1]Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia
[2]Advanced Communication Engineering, Centre of Excellence (CoE), Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia
[3]Geopolymer and Green Technology, Centre of Excellence (CEGeoGTech), Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia
[4]College of Engineering, Universiti Malaysia Pahang (UMP), Pahang, Malaysia

Article Info

Article history:

Received Nov 16, 2021
Revised Jun 26, 2022
Accepted Jul 27, 2022

Keywords:

Dataplicity
IoT gateway
Raspberry Pi 3 model B
Secure tunnel
VPN connections

ABSTRACT

A virtual private network (VPN) connects a private network to the internet, primarily the public network, through a secure tunnel. Using a local area network (LAN) segment, users can send and receive data from their colleagues in different locations on the network. The development of VPN allows users to gain access to company applications and databases. Therefore, data can be transmitted through a secure tunnel without the need to configure port forwarding for the internet of things (IoT) gateway, allowing users to access it from any location in the world. A method such as dataplicity and pitunnel was examined to compare with the conventional setting. This research paper examines the current deployment of VPN connections in IoT gateways, discussing their characteristics, benefits, and drawbacks, as well as comparing them. The advantage of this method is that the IoT gateway is always accessible and has internet connectivity, which is a significant benefit. Dataplicity is a more trustworthy option because they offer excellent assistance for both the backend and frontend environments.

Corresponding Author:

Mohd Natashah Norizan
Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP)
Exit Lebuhraya Changlun-Kuala Perlis, 02600 Arau, Perlis, Malaysia
Email: mohdnatashah@unimap.edu.my

1. INTRODUCTION

People nowadays are keen to get them up-to-date, with the accessibility of making maximum use of the internet. They want the information right on the palm. This goes the same for their house, as they can remotely monitor and control home appliances using a web-based graphical user interface (GUI) [1] or smartphones [2]. Whether in the office or at the sandy beaches, they can easily access their home regardless of time and place. Users can check the temperature [3], humidity [4], rainy seasons [5], gas leakage [6], and even watering their plants [7]. All they need is a smart gateway connected to the internet and communication within the sensors and actuators [8]–[12]. Users can monitor the sensors and control the actuators from the web-based GUI. For example, the air-conditioner operates within 30-minutes resident reaches home, the microwave heats the food, and the water sprinkler activates when it is time to water the plants or sense the soil is drying up [13], [14]. Eventually, this is the so-called self-healing IoT gateway [15]–[18]. Saito *et al.* [19] defined a home gateway as the ingress point between a personal area network and a public access network. This gateway can allow users to monitor, control, and analyze on a day-to-day basis. The device is connected to the sensors or actuators, connected directly via serial communication or zigbee [20] or long-range radio (LoRa) wirelessly [21]. Data collected from the sensors is then passed to the gateway before being sent to cloud storage [22]–[24]. When the data is gathered, the gateway can analyze the provided data, such as gas leakage or surrounding temperature is too high, and take appropriate action, such as alarming users about the gas leakage via short message service (SMS) or email and activating the air ventilation [25]. This self-healing ability can save human life and help users safeguard the house.

A secured connection is compulsory to avoid breaches from the impropriate gestures to the home network [26]. As many people live around us, predators try to sniff important data in the network [27]. Thus, having a virtual private network (VPN) connection is compulsory for IoT gateway to operate [28]. VPN enables the secure extension of a private network over an untrusted public network [29]. The internet engineering task force (IETF) has defined several protocols for establishing a VPN [30]. Secure sockets layer (SSL) and transport layer security (TLS) are two of them [31]. TLS is a protocol that combines the SSL certificates of its predecessor into a single standard. SSL/TLS has been extensively developed to address security and trust concerns while remaining transparent to the user. As a result, users create wireless VPNs using this protocol. The SSL/TLS protocols define the mechanisms to ensure secure data transmission over the internet [32]. The IETF controls the standards. The protocols are cryptographic protocols that ensure the security of computer network communications. Numerous protocols in various flavours are widely used in web browsing, email, instant messaging, and voice over internet protocol (VoIP) applications. For example, TLS, usually coupled with hypertext transfer protocol (HTTP), secures the web and uses the hypertext transfer protocol secure (HTTPS) uniform resource identifier (URI) scheme [33], [34]. TLS is the internet's cryptographic protocol. It comprises protocols for negotiating cryptographic parameters, encrypting and decrypting data, and reporting errors encountered during the process. As a result, a security analysis of any cryptographic protocol is required to identify any vulnerabilities and to assess the protocol's security properties [35].

Although the pandemic hit us in early 2020, the technology did not stop us from venturing into more and more newly developed methods and approaches. Everyone stayed back at home, but at the same time, we needed to gather valuable information from our site. Our site might be on an urban or rural site, and it might be that our site got no copper or fiber connection but eventually had a mobile data connection (4G or 5G) on our site. The latest 5G network for IoT devices [36] provides a large broadcast capacity that supports up to 65,000 connections at a time. based on the telecom regulatory authority of india (TRAI), 93% of broadband penetration is in the urban area, while 29.3% is broadband penetration in India's rural areas [37]. Ahmed *et al.* discuss implementing IoT devices in rural areas with a Wi-Fi based Long Distance and 6LoWPAN enabled WSN network [38]. Kautsarina and Kusumawati [39] discuss the supportive technologies for IoT devices in rural areas. Carrillo and Seki [40] compare the long-term evolution (LTE) and the LoRAWAN application in rural areas involving UAVs to quantify the gain ratio coverage compared to the terrestrial scenario. Mohammed Sadeeq et al. [41] discuss security, storage and computational performance, and other challenges regarding cloud-IoT. Pourqasem [42] proposed the Cloud-based IoT integration, and the infrastructure was based on storing, processing and communication features. Providing the cloud-based IoT influences data format and connecting devices, thus providing the web service-based communication between IoT devices and the cloud [43].

In this paper best method connecting IoT devices with the cloud is proposed without having a copper/fiber connection and solely depending on the 4G/5G connection. To the best of our knowledge, this is the first work that focuses on integrating a secure protocol at the embedded interface, which is unique. Raspberry Pi is used as an example of an IoT gateway in our pilot deployment of the model for IoT gateway to demonstrate how this could be accomplished. As a result of a large number of low-cost and resource-constrained lightweight Internet of Things devices that are being connected over the internet, security measures have historically not been compatible with the processing power of these embedded controllers. because raspberry Pi can be integrated with Wi-Fi, serial peripheral interface (SPI), narrow-band imaging (NBI), Zigbee, LoRA, and a variety of other protocol connectivity, it is an excellent choice for our IoT gateway model. Raspbian, which is a Debian-based operating system, is also available for the Raspberry Pi. It can be configured to run a LAMP (Linux Apache, MySQL, and PHP), allowing the Raspberry Pi to function as a web server. A method such as Dataplicity and PiTunnel was analyzed to compare with the conventional setting. By using this method, users can connect to their device via internet connections from a remote location, where it makes the device's private address accessible from the internet via "IP tunnelling" technology, making the device reachable from anywhere in the world.

2. METHOD

The Raspberry Pi 3 model B is the hardware used in this study. The Raspberry Pi 3 model B is the most recent model available. The Raspberry Pi runs Linux and Windows operating systems (OS), allowing this credit-card-sized computer to act as an IoT gateway [44]. It also supports wired communication protocols like SPI and inter-integrated circuit (I2C), as well as wireless protocols like Zigbee and LoRa. In addition, this minicomputer, powered by a 1.4 GHz Broadcom chip, can function as a standard computer with a camera port, 40 pin GPIO, and Wi-Fi connections.

IoT gateway should provide and support internal and external data exchange in a smart home scenario [45]. Moreover, it is reliable to communicate with wired and wireless sensor nodes. Therefore, the IoT gateway need these requirements to work [46]:

- Data forwarding: the IoT gateway's primary function is to send data from sensor nodes or the internet to receiving applications or software bound to its addresses.
- Protocol conversion: the IoT gateway should convert communication protocols between the 802.15.4/Zigbee/LoRa wireless protocol and TCP/IP protocols. The IoT gateway should collect packets from sensor nodes using short-distance wireless communication protocols (such as Zigbee) and long-distance wireless communication protocols (such as LoRa), then send them to telecommunication networks or the internet using 3G, Wi-Fi, and other network interfaces. As a result, the IoT gateway should analyze and repackage it before capsulating and sending it using telecommunication protocols after receiving sensor data.
- Management and control: the IoT gateway should manage and control the sensor nodes in addition to receiving and uploading data. When the gateway receives commands from a remote server, it should process them and then send them to the sensor nodes via IoT gateway to manage and control the sensor network.

Dataplicity [47] and PiTunnel [48] are two VPN providers for IoT gateway that were investigated. Remote access to the IoT gateway is available from both providers. The IoT gateway will be installed with installers from both providers. Dataplicity is nothing more than a VPN for your Raspberry Pi, as shown in Figure 1. This feature not only allows users to access their Raspberry Pi from anywhere, but it also enables them to "wormhole" a web server through the system, allowing them to run their own little website from the convenience of their all-in-one computer.

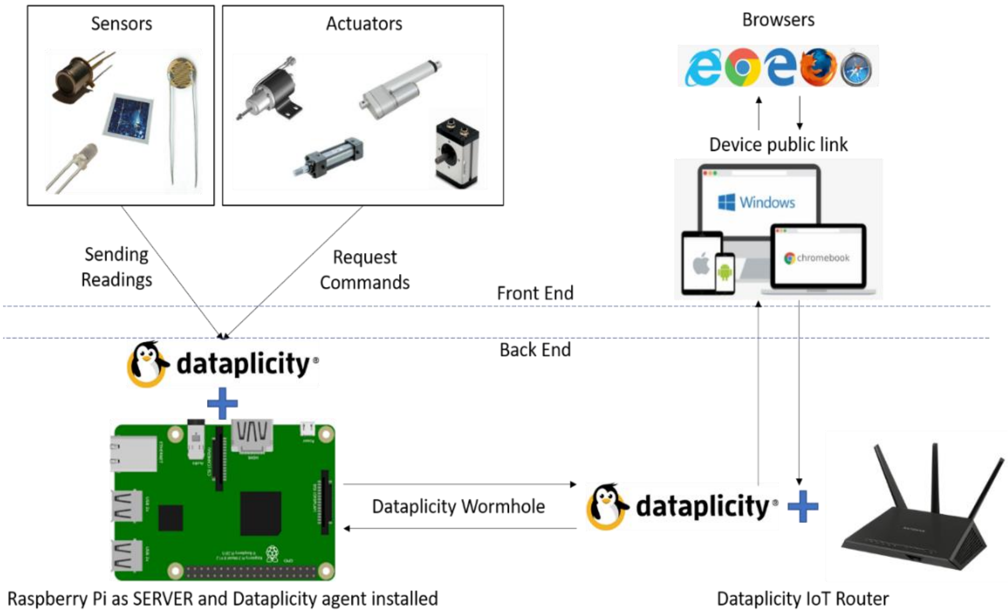


Figure 1. Dataplicity system flowchart [47]

However, PiTunnel differs from dataplicity in that it makes some of its own modifications. Users can connect to their little computer via a terminal or the web by simply running a few commands on the local Pi. A one-of-a-kind feature is the ability to launch a command prompt from within the browser. Other services are heavily reliant on remote terminals for their operations. Although PiTunnel includes that feature, it is primarily concerned with tunnelling, which means that users can access any network service that is running on their raspberry Pi from anywhere in the world, whether it is using the HTTP protocol or some other custom protocol, without having to worry about setting up complicated network routing or static IP addresses as shown in Figure 2.

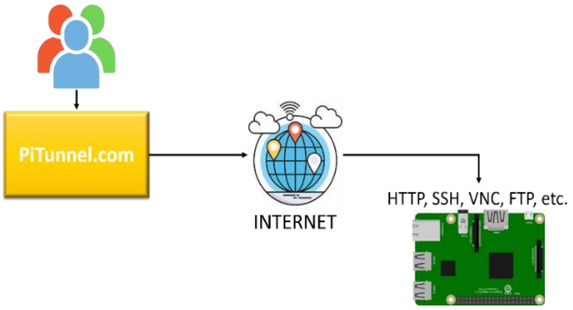


Figure 2. PiTunnel system flowchart [48]

3. RESULTS AND DISCUSSION

To choose the best VPN connections to be implemented into the IoT gateway, a few sets of tests were applied to the VPN to choose the best one. These tests focus on the applications between the VPN provider and IoT gateway. The main goal is to see the VPN provider control, access and modify the IoT gateway either thru web-based or GUI.

For these, three different tests were made to see the following values: i) remote access from VPN website, ii) proper uniform resource locator (URL) designation, and iii) diagnostics tools for the IoT gateway. For the test to be done, both VPN provider installers need to install into IoT gateway. The installer command looks the same between the providers. They use the curl command to fetch and install the software into the IoT gateway. It takes time for the installer to be downloaded and installed into the IoT gateway.

3.1. Remote access

We need to know if dataplicity and PiTunnel allow users to remote access the IoT gateway for the first test. Remote access is the ability to access a computer from a remote location. The ability of remote access is provided either thru LAN, wide area network (WAN) or VPN. In addition, both providers allow users to remote the IoT gateway from the internet through their website. As we can see here in Figure 3, Dataplicity allows users to remotely access the user's device thru the Dataplicity agent that was previously installed. Dataplicity Wormhole allows connections from the internet, going to the IoT gateway terminal. The connections are then passed to the Dataplicity IoT router, and the user can see the terminal. For a website hosted in the IoT gateway, Dataplicity Wormhole open port 80 for access. The URL will change to devide_id.dataplicity.io. The URL is accessible as long as there is an internet connection from the IoT gateway. IoT gateway must have Apache running so that the website hosted inside can be seen from the internet.

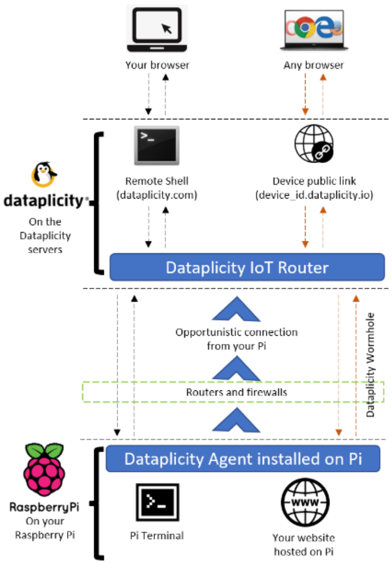
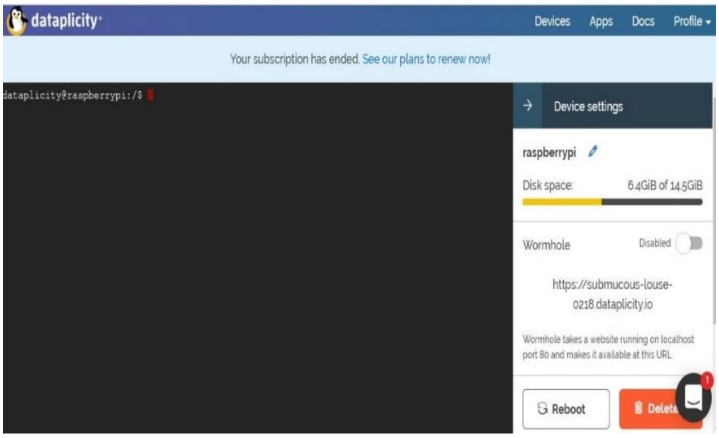

Your browser
Any browser
Remote Shell (dataplicity.com)
Device public link (device_id.dataplicity.io)
dataplicity
On the Dataplicity servers
Dataplicity IoT Router
Opportunistic connection from your Pi
Routers and firewalls
Dataplicity Wormhole
Dataplicity Agent installed on Pi
RaspberryPi
On your Raspberry Pi
Pi Terminal
Your website hosted on Pi

Figure 3. Dataplicity VPN connection model [49]

Both Dataplicity and PiTunnel provide SSL/TLS connections to the IoT Gateway. These encryptions protocols offer security on the data transactions from the internet to the IoT Gateway. The test confirms that the providers can give full access to the user to remote to the IoT, as referred to in Figure 4 and Figure 5.



Your subscription has ended. See our plans to renew now!

```
dataplicity@raspberrypi:/$
```

raspberrypi

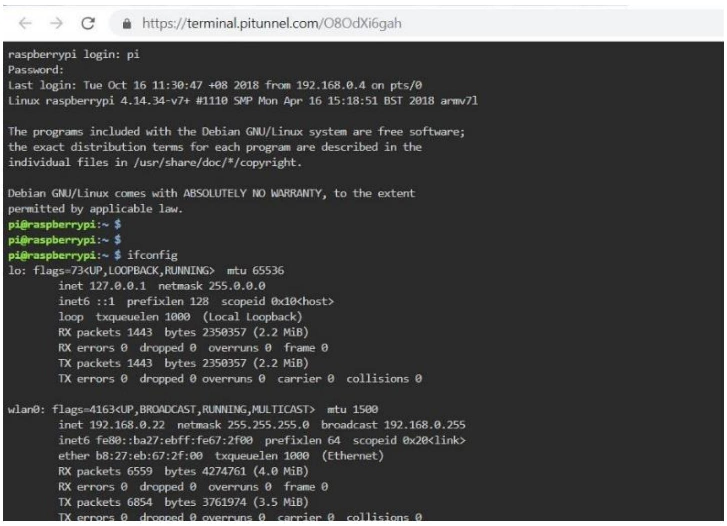
Disk space: 6.4GiB of 14.5GiB

Wormhole Disabled

https://submucous-louse-0218.dataplicity.io

Wormhole takes a website running on localhost port 80 and makes it available at this URL

Figure 4. Dataplicity remote access



https://terminal.pitunnel.com/O8OdXi6gah

```
raspberrypi login: pi
Password:
Last login: Tue Oct 16 11:30:47 +08 2018 from 192.168.0.4 on pts/0
Linux raspberrypi 4.14.34-v7+ #1110 SMP Mon Apr 16 15:18:51 BST 2018 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
pi@raspberrypi:~ $
pi@raspberrypi:~ $
pi@raspberrypi:~ $ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1443  bytes 2350357 (2.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1443  bytes 2350357 (2.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.22  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::ba27:ebff:fe67:2f00  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:67:2f:00  txqueuelen 1000  (Ethernet)
        RX packets 6559  bytes 4274761 (4.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6854  bytes 3761974 (3.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

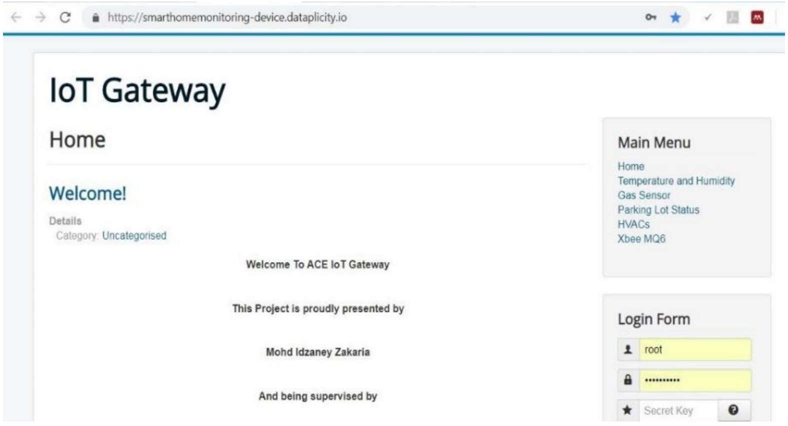
Figure 5. PiTunnel remote access

3.2. Proper URL designation

The user needs to install the webserver into the IoT gateway for the second test. The user can install either Nginx or Apache on the IoT gateway. Dataplicity provides two types of URLs to the user, where Dataplicity called the application a Wormhole. They use HTTPS embed in the domain to deliver security. One is a free domain, where the user uses a free given domain provided by Dataplicity, while the other one is paid domain, where the user needs to pay the domain monthly recurrence, and the user is free to choose its domain. Dataplicity offers a subdomain, which is the URL is: **<subdomain>.dataplicity.io.**

For IoT gateway, we installed Joomla into the webserver. Joomla is a content management system (CMS) that is very popular for designing a website. It has a user-friendly front end and back end design. It uses the what you see is what you get (WYSIWYG) concept. According to Zhu *et al.* [50], the visible part of a web page includes tools like the Web Browser, the displayed contents, and the layout, while the invisible part includes the code written on the web page, such as extensible hypertext markup language (XHTML), cascading style sheets (CSS), and so on. The Joomla website template is crisp and manageable, allowing the user to amend at the back end. The structure and layout are user-controllable and require no website coding savvy; thus, it is constructive. As we can see here in Figure 6, the layout is very structured and in place. However, the title and the menus are incorrect positions. The article also is in its location. This is what the user needs for the IoT gateway.

Referring to Figure 7, PiTunnel, on the other hand, provides a free subdomain, and the user cannot choose its domain. PiTunnel also provides an HTTPS connection to the IoT gateway port. When the user accesses the Joomla template's website, the structure is miserable and improper. The menu is moving far below, and the article is shifted.



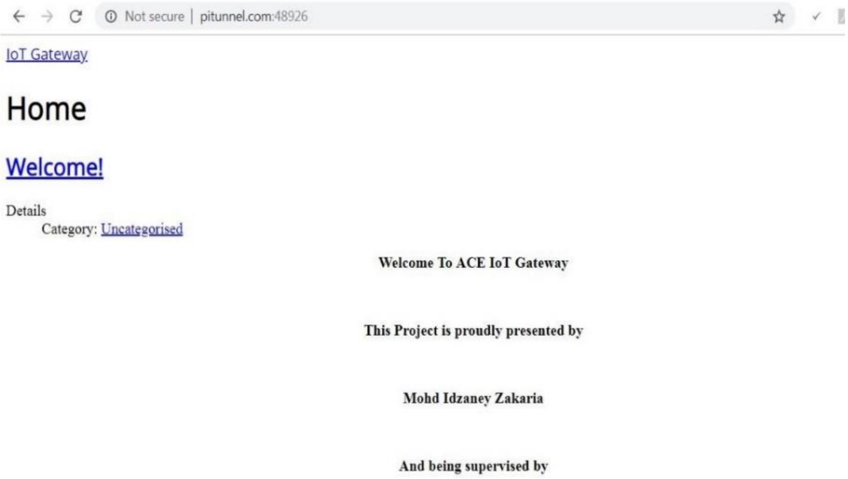
Welcome To ACE IoT Gateway

This Project is proudly presented by

Mohd Idzaney Zakaria

And being supervised by

Figure 6. Dataplicity joomla layout



Welcome To ACE IoT Gateway

This Project is proudly presented by

Mohd Idzaney Zakaria

And being supervised by

Figure 7. PiTunnel joomla layout

3.3. Diagnostic tools

For the third test, diagnostics tools for the IoT gateway. The diagnostics tools are vital as part of the IoT gateway, and the user needs to know the basic and in-depth condition of IoT gateway hardware. Dataplicity provides diagnostics tools, allowing the user to monitor system configuration from the user's mobile phone. Dataplicity segmented the tools into three parts: networking, system and advanced.

The networking button tells the user which interfaces are connected to the internet, as seen in Figure 8. It also stated the network traffic data, giving a real-time chart of the network traffic transmitted to or from the IoT gateway. This gives the user the first impression if there are suspicious attacks from outside. The high incoming traffic pattern from the internet will show the user that a flood ping or distributed denial of service (DDoS) attack is possible. After information theft, DDoS attacks are the second most common cybercrime. Flood attacks using the DDoS transmission control protocol (TCP) can quickly deplete the cloud's resources, consume most of its bandwidth, and damage an entire cloud project [51]. The user can recognize and take appropriate actions, such as appending the IP address or moving the IP address to a blocklist. The system button tells the user the central processing unit (CPU), random-access memory (RAM), and disk usage conditions. The advanced button provides the ifconfig status, domain name system (DNS) resolver, mount point, and cpuinfo. Meanwhile, in Figure 9 PiTunnel only provided IoT gateway OS version, memory usage, CPU usage and temperature, graphics processing unit (GPU) temperature and active tunnel.

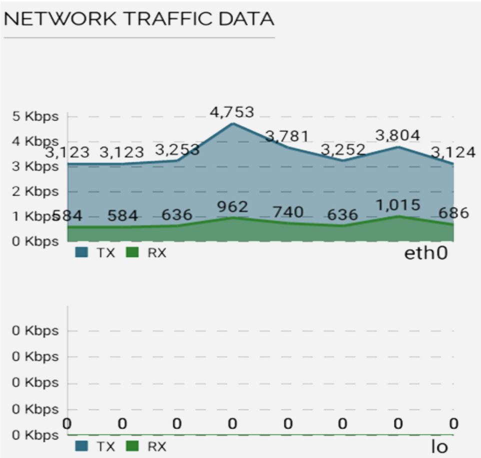
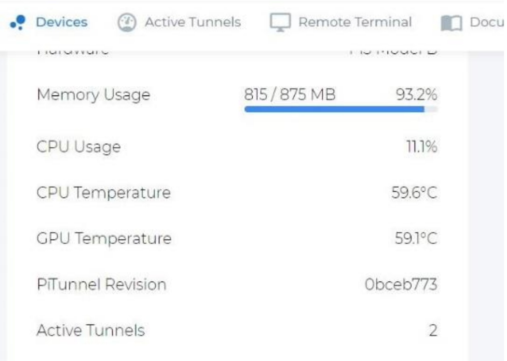


Figure 8. Dataplicity network traffic data



Memory Usage 815 / 875 MB 93.2%

CPU Usage 11.1%

CPU Temperature 59.6°C

GPU Temperature 59.1°C

PiTunnel Revision 0bceb773

Active Tunnels 2

Figure 9. PiTunnel IoT gateway status

Table 1. Comparison between conventional setting, Dataplicity and PiTunnel

Description	Conventional setting	Dataplicity	PiTunnel
Network knowledge	Intermediate/advanced	Beginner	Beginner
Port setting	Both on router and IoT device, vulnerable to DDoS attack	No changes to be done	No changes to be done
IoT gateway behaviour	Cannot detect	Can be monitor	Can be monitor
Security	WPA2 encryption	Client-initiated HTTPS	HTTPS Security

4. CONCLUSION

IoT gateway provides users with a web-based GUI for monitoring and controlling purposes, and users can do remote access to the IoT gateway in case of system support. The need for a virtual private network in the IoT gateway networking delivers security and private management. The non-authentic user will be prohibited from accessing the IoT gateway and reducing the possibility of hacking into the IoT gateway. In this paper, the authors analyzed VPN providers into IoT gateway for smart homes to choose the best for a set of scenarios using remote access, proper website URL and diagnostics tool. Concluding the VPN connectivity, Dataplicity provides such a reasonable provision for the user. Moreover, Dataplicity is a more reliable choice as they provide tremendous support for the backend and frontend environments. This connection can be expanded into smart agriculture, smart farming, smart factory, smart water sensor and eHealth. Future research will also include a look at large-scale IoT infrastructure, penetration testing, and a live demonstration of a malicious attack.

ACKNOWLEDGEMENTS

The author would like to acknowledge the Fundamental Research Grant Scheme (FRGS) support under the grant number FRGS/1/2017/STG02/UNIMAP/02/2 from the Ministry of Higher Education Malaysia and Universiti Malaysia Perlis.

REFERENCES

[1] J. A. Ghani, M. Rizal, M. Z. Nuawi, M. J. Ghazali, and C. H. C. Haron, "Monitoring online cutting tool wear using low-cost technique and user-friendly GUI," *Wear*, vol. 271, no. 9–10, pp. 2619–2624, Jul. 2011, doi: 10.1016/j.wear.2011.01.038.

[2] R. P. Hudhajanto, N. Fahmi, E. Prayitno, and Rosmida, "Real-time monitoring for environmental through wireless sensor network technology," in *2018 International Conference on Applied Engineering (ICAE)*, Oct. 2018, pp. 1–5. doi: 10.1109/INCAE.2018.8579377.

[3] R. Ab Rahman, U. R. Hashim, and S. Ahmad, "IoT based temperature and humidity monitoring framework," *Bull. Electr. Eng. Informatics*, vol. 9, no. 1, pp. 229–237, Feb. 2020, doi: 10.11591/eei.v9i1.1557.

[4] P. Serikul, N. Nakpong, and N. Nakjuatong, "Smart farm monitoring via the blynk IoT platform : case study: humidity monitoring and data recording," in *2018 16th International Conference on ICT and Knowledge Engineering (ICT&KE)*, Nov. 2018, pp. 1–6. doi: 10.1109/ICTKE.2018.8612441.

[5] M. Cristani, F. Domenichini, C. Tomazzoli, and M. Zorzi, "'It could be worse, It could be raining': reliable automatic meteorological forecasting for holiday planning," 2019, pp. 3–11. doi: 10.1007/978-3-030-22999-3_1.

[6] V. Suma, R. R. Shekar, and K. A. Akshay, "Gas leakage detection based on IOT," in *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, Jun. 2019, pp. 1312–1315. doi: 10.1109/ICECA.2019.8822055.

[7] P. Jariyayothin, K. Jeravong-aram, N. Ratanachaijaroen, T. Tantidham, and P. Intakot, "IoT backyard: smart watering control system," in *2018 Seventh ICT International Student Project Conference (ICT-ISPC)*, Jul. 2018, pp. 1–6. doi: 10.1109/ICT-ISPC.2018.8523856.

[8] O. O. Kazeem, L. O. Kehinde, O. O. Akintade, and L. O. Kehinde, "Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things," *Int. J. Internet Things*, vol. 2017, no. 1, pp. 9–13, 2017, doi: 10.5923/j.ijit.20170601.02.

[9] S. B. Zahir *et al.*, "Smart IoT flood monitoring system," *J. Phys. Conf. Ser.*, vol. 1339, no. 1, p. 012043, Dec. 2019, doi: 10.1088/1742-6596/1339/1/012043.

[10] M. Chandran *et al.*, "An IoT based smart parking system," *J. Phys. Conf. Ser.*, vol. 1339, no. 1, p. 012044, Dec. 2019, doi: 10.1088/1742-6596/1339/1/012044.

[11] J. S. C. Turner *et al.*, "Modeling on impact of metal object obstruction in urban environment for internet of things application in vehicular communication," 2020, p. 020053. doi: 10.1063/1.5142145.

[12] F. Gaetani, R. D. Fazio, G. A. Zappatore, and P. Visconti, "A prosthetic limb managed by sensors-based electronic system: experimental results on amputees," *Bull. Electr. Eng. Informatics*, vol. 9, no. 2, Apr. 2020, doi: 10.11591/eei.v9i2.2101.

[13] R. Lakshmanan, M. Djama, S. Perumal, and R. Abdulla, "Automated smart hydroponics system using internet of things," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, p. 6389, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6389-6398.

[14] S. Vijayalakshmi, C. Anuradha, R. C. Ilambirai, and V. Ganesh, "Real-time monitoring and control of flow rate in transportation pipelines using Matlab-based interactive GUI and PID controller," *Int. J. Power Electron. Drive Syst.*, vol. 11, no. 4, p. 1767, Dec. 2020, doi: 10.11591/ijpeds.v11.i4.pp1767-1774.

[15] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the internet of things (IoT)," in *2017 Eleventh International Conference on Sensing Technology (ICST)*, Dec. 2017, pp. 1–5. doi: 10.1109/ICSensT.2017.8304465.

[16] J. P. Dias, T. B. Sousa, A. Restivo, and H. S. Ferreira, "A pattern-language for self-healing internet-of-things systems," in *Proceedings of the European Conference on Pattern Languages of Programs 2020*, Jul. 2020, pp. 1–17. doi: 10.1145/3424771.3424804.

[17] M. S. Aktas and M. Astekin, "Provenance aware run-time verification of things for self-healing internet of things applications," *Concurr. Comput. Pract. Exp.*, vol. 31, no. 3, p. e4263, Feb. 2019, doi: 10.1002/cpe.4263.

[18] R. Kaur and G. Kaur, "Proactive scheduling in cloud computing," *Bull. Electr. Eng. Informatics*, vol. 6, no. 2, pp. 174–180, Aug. 2017, doi: 10.11591/eei.v6i2.649.

[19] T. Saito, I. Tomoda, Y. Takabatake, J. Arni, and K. Teramoto, "Home gateway architecture and its implementation," *IEEE Trans. Consum. Electron.*, vol. 46, no. 4, pp. 1161–1166, 2000, doi: 10.1109/30.920474.

[20] I. Froiz-Míguez, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes," *Sensors*, vol. 18, no. 8, p. 2660, Aug. 2018, doi: 10.3390/s18082660.

[21] M. Rizzi, P. Ferrari, A. Flammini, E. Sisinni, and M. Gidlund, "Using LoRa for industrial wireless networks," in *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, May 2017, pp. 1–4. doi: 10.1109/WFCS.2017.7991972.

[22] A. Iqbal *et al.*, "Interoperable internet-of-things platform for smart home system using web-of-objects and cloud," *Sustain. Cities Soc.*, vol. 38, pp. 636–646, Apr. 2018, doi: 10.1016/j.scs.2018.01.044.

[23] S. Vatari, A. Bakshi, and T. Thakur, "Green house by using IOT and cloud computing," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, May 2016, pp. 246–250. doi: 10.1109/RTEICT.2016.7807821.

[24] N. S. M. Aseri *et al.*, "Smart embedded-analytics sensors with cloud-based measurement system for HVAC," 2020, p. 020050. doi: 10.1063/1.5142142.

[25] D. Xibo and W. Ru-yue, "Development of ammonia Gas leak detection and location method," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 15, no. 3, p. 1207, Sep. 2017, doi: 10.12928/telkomnika.v15i3.5079.

[26] J. Ball, “Secure connection?,” *New Sci.*, vol. 241, no. 3218, pp. 26–27, Feb. 2019, doi: 10.1016/S0262-4079(19)30328-8.

[27] P. Anu and S. Vimala, “A survey on sniffing attacks on computer networks,” in *2017 International Conference on Intelligent Computing and Control (I2C2)*, Jun. 2017, pp. 1–5. doi: 10.1109/I2C2.2017.8321914.

[28] J. Fan, Z. Wang, and C. Li, “Design and implementation of IoT gateway security system,” in *2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM)*, Oct. 2019, pp. 156–162. doi: 10.1109/AIAM48774.2019.00039.

[29] J. Kuusijarvi, R. Savola, P. Savolainen, and A. Evesti, “Mitigating IoT security threats with a trusted network element,” in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec. 2016, pp. 260–265. doi: 10.1109/ICITST.2016.7856708.

[30] L. Caldas-Calle, J. Jara, M. Huerta, and P. Gallegos, “QoS evaluation of VPN in a raspberry Pi devices over wireless network,” in *2017 International Caribbean Conference on Devices, Circuits and Systems (ICCDCS)*, Jun. 2017, pp. 125–128. doi: 10.1109/ICCDCS.2017.7959718.

[31] R. Oppliger, *SSL and TLS: theory and practice*. 2009.

[32] P. Sirohi, A. Agarwal, and S. Tyagi, “A comprehensive study on security attacks on SSL/TLS protocol,” in *2016 2nd International Conference on Next Generation Computing Technologies (NGCT)*, Oct. 2016, pp. 893–898. doi: 10.1109/NGCT.2016.7877537.

[33] S. Turner, “Transport Layer Security,” *IEEE Internet Comput.*, vol. 18, no. 6, pp. 60–63, Nov. 2014, doi: 10.1109/MIC.2014.126.

[34] J. A. McMurry *et al.*, “Identifiers for the 21st century: How to design, provision, and reuse persistent identifiers to maximize utility and impact of life science data,” *PLOS Biol.*, vol. 15, no. 6, p. e2001414, Jun. 2017, doi: 10.1371/journal.pbio.2001414.

[35] A. K. Ranjan, V. Kumar, and M. Hussain, “Security analysis of TLS authentication,” in *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, Nov. 2014, pp. 1356–1360. doi: 10.1109/IC3I.2014.7019737.

[36] J. M. Khurpade, D. Rao, and P. D. Sanghavi, “A survey on IOT and 5G network,” in *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, Jan. 2018, pp. 1–3. doi: 10.1109/ICSCET.2018.8537340.

[37] S. K. A. Kumar, G. V. Ihita, S. Chaudhari, and P. Arumugam, “A Survey on rural internet connectivity in India,” in *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Jan. 2022, pp. 911–916. doi: 10.1109/COMSNETS53615.2022.9668358.

[38] N. Ahmed, D. De, and I. Hussain, “Internet of things (IoT) for smart precision agriculture and farming in rural areas,” *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4890–4899, Dec. 2018, doi: 10.1109/JIOT.2018.2879579.

[39] Kautsarina and D. Kusumawati, “The potential adoption of the internet of things in rural areas,” in *2018 International Conference on ICT for Rural Development (IC-ICTRuDev)*, Oct. 2018, pp. 124–130. doi: 10.1109/ICICTR.2018.8706849.

[40] D. Carrillo and J. Seki, “Rural area deployment of internet of things connectivity: LTE and LoRaWAN case study,” in *2017 IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Aug. 2017, pp. 1–4. doi: 10.1109/INTERCON.2017.8079711.

[41] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari, “IoT and cloud computing issues, challenges and opportunities: a review,” *Qubahan Acad. J.*, vol. 1, no. 2, pp. 1–7, Mar. 2021, doi: 10.48161/qaj.v1n2a36.

[42] J. Pourqasem, “Cloud-based IoT: integration cloud computing with internet of things,” *J. Res. Ind. Eng*, vol. 7, no. 4, pp. 482–494, 2018, [Online]. Available: www.riejournal.com

[43] F. Abdali-Mohammadi, M. N. Meqdad, and S. Kadry, “Development of an IoT-based and cloud-based disease prediction and diagnosis system for healthcare using machine learning algorithms,” *IAES Int. J. Artif. Intell.*, vol. 9, no. 4, p. 766, Dec. 2020, doi: 10.11591/ijai.v9.i4.pp766-771.

[44] H. R. and M. H. S. Hussain, “Surveillance robot using raspberry Pi and IoT,” in *2018 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C)*, Apr. 2018, pp. 46–51. doi: 10.1109/ICDI3C.2018.00018.

[45] T. Adiono, S. F. Anindya, S. Fuada, and M. Y. Fathany, “Curtain control systems development on mesh wireless network of the smart home,” *Bull. Electr. Eng. Informatics*, vol. 7, no. 4, pp. 615–625, Dec. 2018, doi: 10.11591/eei.v7i4.1199.

[46] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, “IOT gateway: bridging wireless sensor networks into internet of things,” in *2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Dec. 2010, pp. 347–352. doi: 10.1109/EUC.2010.58.

[47] “Dataplicity.” https://www.dataplicity.com (accessed Oct. 02, 2022).

[48] “PiTunnel.” https://www.pitunnel.com (accessed Oct. 22, 2022).

[49] S. Saha, R. H. Rajib, and S. Kabir, “IoT based automated Fish farm aquaculture monitoring system,” in *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, Oct. 2018, pp. 201–206. doi: 10.1109/ICISET.2018.8745543.

[50] J. Zhu, X. Liu, Y. Urano, and Q. Jin, “A novel WYSIWYG approach for generating cross-browser web data,” in *2010 International Conference on Computational Science and Its Applications*, 2010, pp. 155–164. doi: 10.1109/ICCSA.2010.47.

[51] A. Sahi, D. Lai, Y. Li, and M. Diykh, “An efficient DDoS TCP flood attack detection and prevention system in a cloud environment,” *IEEE Access*, pp. 1–1, 2017, doi: 10.1109/ACCESS.2017.2688460.

BIOGRAPHIES OF AUTHORS

Mohd Idzaney Zakaria received the M.Eng. in Electric-Electronic from the University Technology of Malaysia (UTM). Upon completing his degree, he joins Telekom Malaysia as Network Engineer (NOC) for four years and a System Administrator (SA) for three years. Having an interest in the latest technology of computing, he enrolled MSc degree at Universiti Malaysia Perlis (UniMAP). His research interest includes IoT, Big Data, M2M and Machine Learning. He can be contacted at email: idzaneyzakaria@gmail.com.

Dr. Mohd Natashah Norizan is a Senior Lecturer at the Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), Malaysia. He received his Bachelor's degree in Electronic Engineering from UniMAP, Malaysia, in 2008, a Master of Science degree in Microelectronics from Universiti Kebangsaan Malaysia (UKM), Malaysia, in 2011 and a Doctor of Engineering in Sustainable Energy and Environmental Engineering from Osaka University, Japan. Before joining UniMAP, he worked as a Technical Support Engineer at Telekom Malaysia Applied Business. He is active in volunteering work with IEEE Malaysia Section, acting as the Senior Member of IEEE and a vice president of the IEEE Malaysia Section Sensors and Nanotechnology Joint Councils Chapter. He is a chartered engineer and a member of the Institution of Engineering and Technology (IET), United Kingdom, a graduate engineer of the Board of Engineers Malaysia (BEM), Malaysia and a professional technologist of the Malaysia Board of Technologist (MBOT), Malaysia. He can be contacted at email: mohdnatashah@unimap.edu.my.

Assoc. Prof. Dr. Muammar Mohamad Isa is an Associate Professor at the Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis. He has been a faculty member since 2005 and held various positions of increasing scope and responsibilities, including the Program Chairperson for Diploma of Microelectronic Engineering (2007), Deputy Dean of Student Affairs and Alumni (2007-2009), Deputy Dean Academic and Research (2013-2015), and Deputy Director at the Centre of Graduate Studies (2017 – 2020). He is a member of numerous professional societies and is a registered Professional Technologist with the Malaysia Board of Technologists. His research focuses on III-V devices' simulation, fabrication, and characterization for future high-speed, high-frequency, and low-noise applications. Some of his research includes the design and fabrication of Si-based micro-antenna for early cancer cell detection. He also collaborates actively in research with industries, especially in intelligent IoT systems for large-scale agricultural plantations. He can be contacted at email: muammar@unimap.edu.my.

Prof. Dr. Mohd Faizal Jamlos received an M.Sc. degree from the University of Adelaide, South Australia, Australia, in 2008 and a Ph.D. degree from Universiti Teknologi Malaysia, Johor, Malaysia, in 2010. He is currently a Professor with the Faculty of Mechanical Engineering, Universiti Malaysia Pahang (UMP). Previously he was an Associate Professor with the Advanced Communication Engineering Centre (ACE), School of Computer and Communication Engineering, Universiti Malaysia Perlis. He has co-authored more than 220 scientific publications in peer-reviewed journals and conferences. His research interests include wireless embedded systems, remote sensing, on-platform antennas and microwave circuitry, and IoT applications. He is also a Practice Professional Engineer of Board of Engineers Malaysia (BEM), a National Medical Researcher (NMRR) and a Corporate Member of the Institute of Engineers Malaysia (MIEM). He can be contacted at email: faizaljamlos@ump.edu.my.

Dr. Muslim Mustapa is from the Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP). He received his Bachelor's degree in Electrical and Electronic Engineering from Universiti Teknologi Petronas. Then he furthered his Master's study in Electrical and Computer Systems Engineering at Monash University. He served at UniMAP as a lecturer for two years before continuing his PhD study in Electrical Engineering at the University of Toledo. Now he is working as a Senior Lecturer at the Faculty of Electronic Engineering Technology. His research interests are in hardware security and embedded system design. He can be contacted at email: muslim@unimap.edu.my.