Cluster Computing (2020) 23:451–459
https://doi.org/10.1007/s10586-019-02935-z

A hybrid fog-cloud approach for securing the Internet of Things

Rajaputhri Maharaja[1] · Prashant Iyer[1] · Zilong Ye[1]

Received: 4 December 2018 / Revised: 1 March 2019 / Accepted: 17 April 2019 / Published online: 2 May 2019

Abstract
As the Internet of Things (IoT) continues to grow, there arises concerns and challenges with regard to the security and privacy of the IoT. Malicious attacks such as man-in-the-middle and distributed denial of service (DDoS) are typical threats to the IoT systems. In this paper, we propose a FOg CompUting-based Security (FOCUS) system to provide security for IoT systems against those malicious attacks. The proposed FOCUS system applies a threefold protection mechanism: Firstly, it makes use of the virtual private network (VPN) to secure the communication channels for the IoT devices; Secondly, it applies machine learning-based traffic analysis unit to classify the traffic to be trusted, untrusted and suspicious; Thirdly, it adopts a challenge-response authentication to validate the suspicious traffic source so as to protect the VPN server against potential DDoS attacks. Such a threefold protection mechanism is effective in mitigating various malicious attacks and can provide a high standard security for the IoT system. Furthermore, to improve the system performance, FOCUS is implemented in a hybrid fog-cloud model that achieves a low latency and system response time. In the hybrid fog-cloud model, a selected amount of the protection and validation requests are addressed in the fog that is close to the end users, while the excessive requests are addressed in the cloud. Through this, FOCUS can effectively avoid the long queuing delay caused by the limited computational capacity in the fog implementation. The experimental results show that FOCUS can effectively filter out malicious attacks with low response time and small network cost (e.g., network bandwidth consumption).

Keywords Fog computing · Internet of Things · Security

1 Introduction

The rapid expansion of Internet of Things (IoT) [1] enables a set of new applications, services and benefits, while introducing a few challenges and concerns. Recent reports [2, 3] indicates that malware cyber attacks such as man-in-the-middle and distributed denial of service (DDoS) are typical threats to the IoT. Hence, it is essentially important to develop new protection schemes to ensure the security and privacy of IoT systems.

Recently, fog computing has been proposed to improve the connectivity of devices [4] and enhance the IoT system efficiency [5–7], via processing selected data locally and reducing the amount of data that needs to be sent to cloud for processing. Driven by these recent innovations in fog computing, we propose a FOg CompUting-based Security system, called FOCUS, to enhance the security and privacy for the IoT system while achieving a fast response and an efficient network performance. The proposed FOCUS system is novel as it adopts a threefold protection scheme to ensure the security and privacy of IoT systems. Firstly, FOCUS uses a VPN to secure the communication channels for the IoT devices. Secondly, FOCUS implements machine learning-based traffic analysis to classify the traffic to be trusted, untrusted and suspicious. Thirdly, FOCUS applies a challenge-response authentication to validate those suspicious traffic sources and further protect the VPN server against potential DDoS attacks, which enhances the security of IoT systems to a higher level. More specifically, a decision tree classification is used to detect the suspicious traffic sources. If the suspicious clients cannot accurately reply to the challenge questions, they will be considered as untrusted and get blocked. Such a threefold protection scheme is effective in mitigating

✉ Zilong Ye
zye5@calstatela.edu

[1] California State University, Los Angeles 5151 State University Drive, Los Angeles, CA 90032, USA

various malicious attacks and can provide a high standard security protection for the IoT systems. In order to improve the system performance, FOCUS is designed to be implemented in a hybrid fog-cloud model that can well balance the response time and the network cost (e.g., network bandwidth consumption). The hybrid fog-cloud model can achieve a very low response time since most of the protection and validation workload is addressed in the fog end that is close to the end users, while the excessive workload is addressed in the cloud end that effectively avoid the possible long queuing delay caused by the limited computing power in the fog end. In addition, the hybrid fog-cloud model can achieve a small network cost since only a small portion of excessive workload are forwarded to the cloud for processing. We demonstrate a proof-of-concept prototype of FOCUS and conduct experiments to evaluate its performance. The results validate the effectiveness of FOCUS and show that FOCUS can effectively filter out malicious attacks with a low response time and a small network bandwidth consumption.

In summary, the main contributions of this work are listed as follows:

- We propose a novel threefold protection mechanism for IoT systems: (1) VPN techniques are used to protect the communication channel; (2) machine learning-based traffic analysis unit is implemented to classify the traffic; (3) a challenge-response authentication mechanism is adopted to validate the suspicious traffic sources.
- We implement the proposed FOCUS system in a hybrid fog-cloud model, which achieves a fast response. The fog side is responsive as it is close to the end users, while the cloud side can complement to the limited computational resource in the fog side and address the excessive workload.
- We demonstrate a proof-of-concept prototype of FOCUS and conduct experiments to evaluate the performance of such a threefold protection mechanism.

The rest of the paper is organized as follows. We first discuss the related work in Sect. 2. Then, we give an overview of the system architecture of FOCUS in Sect. 3, and introduce the main components of FOCUS and describe their design details in Sect. 4. After that, we present the prototype setup and the experimental results in Sect. 5. Finally, we conclude the paper and propose our future work in Sect. 6.

2 Related work

Recently, there are some research efforts on mitigating cyber attacks for the IoT system. For example, the studies in [8–10] explored the use of virtual private network (VPN) to secure the communication channels between the IoT devices. However, the encryption and decryption processes are computationally intensive, which requires high-performance computing appliances. To improve the scalability and reduce the processing time, the authors in [11] proposed a cloud-based technique to protect the IoT systems. However, the proposed solution may not be efficient, since the implementation resides purely in the cloud end, which may introduce a long latency that delays the response to the potential malicious attacks. Recently, fog computing [12–16] has been proposed to improve the IoT system efficiency, via processing selected data locally and reducing the amount of data that needs to be sent to cloud for processing. However, the limited computational power in the fog may not be sufficient to serve and ensure the security of a large number of IoT devices. Compared to the above existing fog computing-based IoT security approaches , the proposed FOCUS system is novel as it adopts a hybrid fog-cloud implementation model. The fog side is close to the end users, which can provide a fast response against any malware attacks; while the cloud side is responsible for addressing the excessive workload, which can avoid the potential long queuing delay caused by the limited computational power in the fog side.

In [17], the authors proposed a cybersecurity framework that uses Markov model, Intrusion Detection System and Virtual Honeypot Device to identify malware attacks in fog and cloud of things environment. This approach may effectively filter out malware attacks; however, it may not be suitable for protecting the IoT systems where a fast response to potential malware attacks is required. The authors in [18] proposed an intrusion detection method with a three-phase traffic analysis, reduction and classification for identifying positive and false requests for smart devices. The work in [19] adopts quite a similar idea as FOCUS, which ensures the security of IoT systems by integrating both fog computing and cloud computing. In this approach, the time-sensitive workload will be served by the fog side, while the non-time-sensitive workload will be sent to cloud for processing. The proposed FOCUS system distinguishes from the aboved approaches since there are threefold protection schemes in FOCUS. The machine learning-based traffic analysis unit can effectively help FOCUS to detect suspicious traffic sources. In addition, the challenge-response unit has the characteristic of actively initiating the communications with suspicious

traffic sources, which lower the risk of vulnerability of FOCUS.

3 The system architecture of FOCUS

The system architecture of FOCUS is shown in Fig.1. FOCUS consists of four main components, including a VPN server, a traffic analysis unit, a challenge-response unit and a firewall. The VPN server is used to secure the communication channels between the IoT devices. All the network traffic that access the IoT systems is required to be encrypted and tunneled through the VPN server, which prevents malware attacks such as sniff, spoof and man-in-the-middle, etc. It is feasible to use VPN to secure the communication channel between the IoT devices; however, the VPN itself may be vulnerable to malicious attacks such as the DDoS attacks. Hence, to further enhance the system security, FOCUS adopts a traffic analysis unit, a challenge-response unit and a firewall to further protect the VPN server against DDoS attacks. More specifically, the traffic analysis unit applies the decision tree classification [20] to detect suspicious traffic sources. The challenge-response unit is responsible for initiating challenge questions to authenticate the identification of the suspicious traffic sources. The suspicious sources that cannot appropriately answer the challenge questions will not be allowed to access the VPN server and will be blocked by the firewall. In this way, the bots and their DDoS attacks can be filtered out, thus improving the security of the VPN server and the whole IoT system. FOCUS is implemented in a highly distributed manner in fog computing, which further upgrades the security of the IoT clients in the edge. The design details of these components will be presented in the Sect. 3.

As the decision tree classification-based traffic analysis unit and the challenge-response authentication unit are computationally intensive, they are supposed to be implemented in the cloud as in a traditional way. However, it may introduce a long latency and response time to communicate with the remote server in the cloud. To address this limitation, the proposed FOCUS system is implemented in a hybrid fog-cloud infrastructure. Compared to traditional cloud solution, FOCUS gains a few benefits as follows. First, FOCUS handles most of the requests (i.e., the requests to the VPN and the challenge-response authentication unit) in the fog end, which is close to the IoT users. Thus, FOCUS achieves a much smaller response time than that of the pure cloud implementation. The fog end implementation can help with saving the expensive wide area network bandwidth resources, thus reducing the investment and operational cost. Furthermore, the implementation in the highly distributed fog facilities can improve the scalability, robustness and reliability of FOCUS. On the other hand, the excessive workload is addressed by the cloud implementation, so that the system performance will not be restricted by the limited computational resources in the fog. Such a hybrid fog-cloud implementation of FOCUS can achieve a low response time or latency, which is critically important for the IoT system that requires real-time communications.

4 The design principles of FOCUS

In this section, we first describe the design details of the four main components of FOCUS. After that, we present the signal workflow between these main components. Finally, we describe the hybrid fog-cloud design details.

4.1 The VPN server

There exists a number of candidates that may become the standard protocol for securing IoT device-to-device communications. In particular, the MQ Telemetry Transport (MQTT) protocol is promising because of its effectiveness and light weight. A traditional user-password authentication is implemented in MQTT to secure the IoT communication channel; however, it is still vulnerable to malicious attacks since multiple IoT users share the same set of user-password in MQTT. To enable safe and trusty data communications between IoT devices, FOCUS leverages VPN and tunneling techniques to connect the IoT devices in the network. The data communications between the clients and all of their IoT devices are conducted over the VPN. In FOCUS, a VPN server is established to

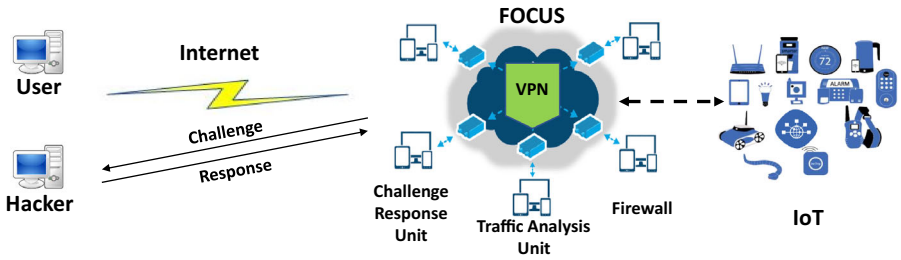


Fig. 1 The system architecture of FOCUS

encrypt the data traffic that enters the tunnel and decrypt it in the other end of the tunnel. In this way, even if the data are "sniffed" by hackers, it is computationally intractable for them to decrypt the message in a reasonable amount of time. In addition, the encrypted VPN can hide the geographical location of the IoT devices, which makes it more difficult for the hackers to identify the target IoT devices. In addition to the use a pair of keys for the encryption/decryption, FOCUS adopts the technique of socket security layer (SSL) for the IoT clients to use when connecting to the VPN server. The main reason that we choose to use SSL rather than IPSec is because the cost to implement SSL is much smaller than IPSec, e.g., SSL are built-in capabilities in most of the web browser while IPSec may require additional hardware/software. Through the above protection mechanism, the integrity of the data packet will be checked and the altered data will be dropped. In addition, the packets that are replayed by bots or hackers can be detected and be rejected to access the IoT system. In this way, the data communication between the clients and the VPN server are secured to be private and integral, which protects the security of the IoT system.

4.2 The traffic analysis unit

FOCUS contains a traffic analysis unit which analyzes the network traffic that attempts to access the IoT systems. The traffic analysis unit adopts the decision tree classification to distinguish legal requests from malicious attacks. The network traffic is categorized into two categories that are *trusted* and *suspicious*, based on a number of attributes such as traffic bursty behavior, flow count, flow parallelity and flow packet count. It is common that the malware traffic has fixed packet length, sequence number and window size. Their source and destination IP addresses, as well as their port numbers, may be spoofed and generated randomly. Hence, we adopt a decision tree classification technique to detect such traffic pattern and report the suspicious malware traffic sources to the challenge-response unit for a further authentication (to be introduced in the next subsection).

We adopt the algorithm in [20] to construct the decision tree. The network traffic is characterized into two classes, which are *normal* and *suspicious*. We derive ten attributes from the network traffic and packet signature, which are adopted as the splitting criterion in the decision tree. In the decision tree, the leaf nodes are the two classes and the non-leaf nodes represent the tests to be carried out on a particular attribute. Here, we define a gain ratio for a given attribute a as $R(a)$ in Eq. (1),

$$R(a) = \frac{E(T) - \sum_{i=1}^{n} \left(\frac{|T_i|}{|T|} \times E(T_i) \right)}{- \sum_{i=1}^{n} \left(\frac{|T_i|}{|T|} \times log_2 \left(\frac{|T_i|}{|T|} \right) \right)} \quad (1)$$

where T is the training dataset, T_j represents the partitioning according to class i and $E(T)$ is the entropy of the training dataset that is defined in Eq. (2).

$$E(T) = - \sum_{i=1}^{k} \left(\frac{|T_i|}{|T|} \times log_2 (\frac{|T_i|}{|T|}) \right) \quad (2)$$

In each iteration, we will first select an attribute with the largest gain ratio as the splitting criterion and create a branch for each possible value of a given attribute, and then divide the training dataset into subsets according to the criterion. This procedure iterates until all the instances in the dataset are labeled, and thus constructing a decision tree. Once the decision tree is constructed, it is straightforward to classify the incoming network traffic. Starting from the root, we apply the test condition to the incoming traffic and follow the appropriate branch based on the outcome of the test. This can lead the incoming traffic to either a leaf node or another internal node in which a new test condition will be performed. Eventually, the incoming traffic that reaches a leaf node will be labeled according to the class that is assigned with the leaf node.

4.3 The challenge-response unit and firewall

Once the traffic analysis unit distinguishes the *suspicious* sources from the *trusted* sources, FOCUS will initialize an authentication process to verify the *suspicious* sources through a challenge-response authentication procedure. Basically, the challenge-response unit will generate a challenge question (note that questions are generated randomly and are different in different attempts) and send it to the *suspicious* traffic sources. If the source IP has been spoofed or if the source is a bot, it is not able to reply with the correct response. Such suspicious clients will be labeled as *untrusted* and be blocked by the firewall. If the source can reply with the correct response, then it is verified and will be changed to the *trusted* class. Such a challenge-response authentication is a robust protection since the challenge question is randomly generated at FOCUS and the question is not a fixed question but a time-varying one, e.g., the challenge question can be a series of random number or a simple math question. It is not easy for hackers to break into FOCUS since they have zero knowledge about how the challenge-response unit generate the challenge question. Furthermore, the challenge-response procedure is initialized by FOCUS rather than the traffic sources, which is a proactive way to provide the security protection.

After being processed by the traffic analysis unit and the challenge-response unit, the incoming network traffic can be labeled as either *trusted* or *untrusted*. The firewall will allow the *trusted* traffic requests to access the VPN server if there is no objection from the access control list in the firewall, while rejecting the *untrusted* ones to contact the VPN server. Thus, the VPN server can be protected against potential DDoS attacks. As a result, the security of the communication channel to the IoT system is furtherly enhanced, thanks to the double protection from both the VPN and the challenge-response authentication.

4.4 The signal workflow of FOCUS

The signal workflow of FOCUS is shown in Fig. 2. All the traffic that attempts to access the VPN server are examined by the traffic analysis unit. The traffic can be labeled as either *trusted* or *suspicious* using a machine-learning based decision tree classification. The *trusted* traffic are directly forwarded to the firewall and then be granted access to the VPN server if there is no objection from the access control in the firewall (e.g., traffic flow 1 and 2). In contrast, the *suspicious* traffic will be examined by the challenge-response unit. Here, the challenge-response unit will generate a random yet time-varying challenge question to authenticate the sources of the *suspicious* traffic. If the *suspicious* traffic source can provide an appropriate answers to the challenge question, then it can be changed back to *trusted* traffic and be able to access the VPN server (e.g., traffic flow 3). Otherwise, if the *suspicious* traffic source fails to accurately respond to the challenge question, it will be labeled as *untrusted*, which will be blocked by the firewall (e.g., traffic flow 4). We can see that FOCUS can effectively protect the VPN server against potential DDoS attacks, thanks to the challenge-response authentication. Consequently, the VPN can ensure a secure communication channel between the IoT devices. As a result, the two levels of protections or so-called double protection in FOCUS can provide a robust and reliable security protection to the IoT system.

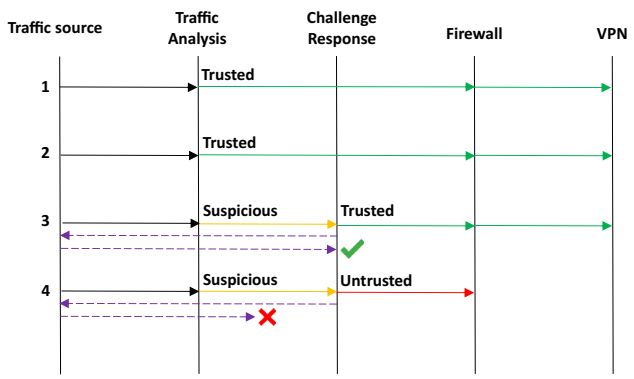


Fig. 2 The signal workflow of FOCUS

4.5 The implementation of FOCUS in a hybrid fog-cloud model

FOCUS is effective in protecting the IoT against malicious attacks given its two-level protection mechanism. In order to further improve the efficiency of the protection system, we implement FOCUS in a hybrid fog-cloud model, denoted by FOCUS-H. In this hybrid fog-cloud model, there are FOCUS implementation nodes in both fog side and the cloud side. In addition, a processing queue is implemented in the fog side of the FOCUS system, which has a limited size and contains the traffic packets that are waiting to be processed by the FOCUS protection system in the fog side. When the number of to-be-validated traffic is small, the fog side of FOCUS has enough computing power to process them. In this case, the queue has enough space to buffer the to-be-validated traffic packets and the FOCUS's cloud implementation nodes are in the stand-by mode. When there is a large volume of traffic waiting to be validated by the FOCUS system, the queue's capacity may be exceeded, given that the fog node has limited computational power. In this case, FOCUS-H would forward the additional incoming traffic packets to FOCUS's cloud implementation nodes for processing, so that the validation of traffic will not experience a long queuing delay. In addition, the workload of validating traffic can be shared by both the fog and cloud implementation of FOCUS.

The hybrid fog-cloud implementation of FOCUS is shown in Fig. 3. Such an implementation is flexible and efficient. In most of the cases, the protection and validation process are conducted in the fog side of FOCUS, which ensures a fast response time for protecting the IoT systems. When the to-be-validated traffic volume is large, the protection and validation workload can be partially offloaded from fog to the cloud side, so that the queuing delay can be reduced and hence response of the protection system can still be maintained in a reasonably short amount of time. Compared to implementing FOCUS fully in the cloud, FOCUS-H introduces a faster response and a smaller network cost, thanks to the fog side implementation that shares the most part of the protection and validation workload. Compared to the pure fog implementation, FOCUS-H can have a faster response in general, since the pure fog implementation of FOCUS has limited computational power and may experience a very long queuing delay when there is a large volume of traffic that needs to be validated. However, this is at a cost of a higher network cost since a portion of the traffic would be forwarded from network edge to the cloud for processing when the queue in the fog side is exceeded. As a result, FOCUS-H can well

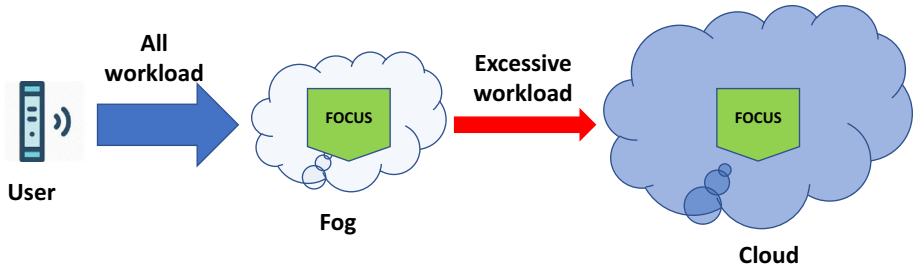


Fig. 3 The hybrid fog-cloud implementation of FOCUS

balance the tradeoff between the protection response and the network cost.

5 Proof-of-concept prototype and performance evaluation

We demonstrate FOCUS in a proof-of-concept prototype that runs in a local server with Intel i7-6650U CPU and 16 GB Memory. The VPN works on port 443 and the challenge-response authentication runs on port 8080. The decision tree classification takes into consideration two classes that are *trusted* and *suspicious*, as well as ten attributes that includes traffic flow packet count, arrival rate and bursty behavior, etc. Note that we duplicate such an implementation of the traffic analysis unit, challenge-response unit and the firewall in a remote server in the Azure cloud, which is denoted by Cloud in the following performance evaluations. In the hybrid fog-cloud implementation, we allow 80% of the requests to be addressed in the fog end, while the rest of them will be transferred to the Azure cloud end for processing. The legal requests to the IoT devices are simulated on two servers, while the DDoS attacks are generated by running a software called PyLoris [21] in another server. We evaluate the performance of FOCUS in terms of the protection effectiveness and the system efficiency. The detailed performance evaluations are presented in the following parts.

5.1 The protection effectiveness of FOCUS

First, we evaluate the protection effectiveness of the system, i.e., how effective the proposed FOCUS system can filter out malicious attacks (e.g., DDoS attacks). In the experiments, we generate a number of legal requests, as well as a set of real-world DDoS attacks using Pyloris in a remote server. The legal requests starts at the beginning of the experiment, while the DDoS attacks start to attack the VPN server 50 seconds after the experiment starts. The protection effectiveness performance of FOCUS is shown in Fig. 4.

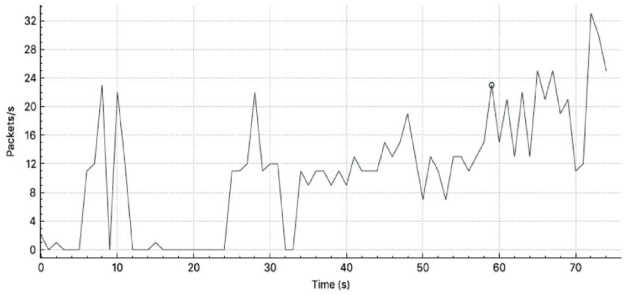
Figure 4a shows the number of requests to the VPN server over time when FOCUS is not in use, while Fig. 4b shows the number of requests when FOCUS is turned on. From Fig. 4a, we can see that, when FOCUS is not used, the VPN server receives a large volume of requests (DDoS attacks occur at time 50 s), which may overwhelm the VPN. As a comparison, we can see from Fig. 4b that FOCUS can effectively detect the DDoS attacks (which starts at 50s) and block the DDoS requests. From these experiments, we can see that FOCUS can well protect the VPN server against DDoS attacks, thus consequently protecting the secure communication channel to the IoT devices, which makes the IoT system secure and reliable.

Figure 4c and d shows that FOCUS can effectively filter out DDoS attacks. We perform an experiment that includes four tests during 5 min. The threshold of flow packet count is set to 7 SYN sessions. We can see from Fig. 4c that all the traffic passes through the tests when FOCUS is not in use, even if there are many flow packets from 192.168.56.103 (shown in Test 2). When FOCUS is turned on as shown in Fig. 4d, the traffic from 192.168.56.103 is blocked in test 3 and 4, while the traffic from 192.168.56.102 passes through in all the tests. This is because the traffic from 192.168.56.103 exceeds the flow packet count threshold and it also fails to verify the challenge question provided by FOCUS, thus being labeled as an *untrusted* source. From this experiment, the results indicate that the rejection is accurate in terms of the traffic sources (e.g., the servers that simulate malware attacks).

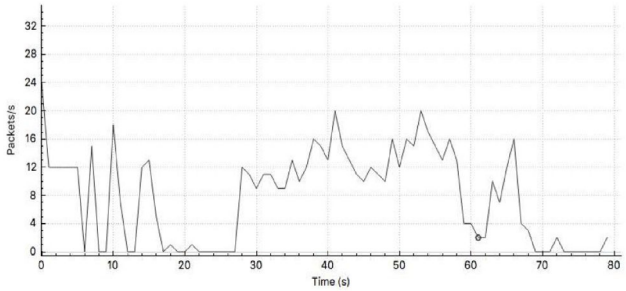
5.2 The system efficiency of hybrid fog-cloud implementation of FOCUS

In this subsection, we will evaluate the system efficiency performance of FOCUS implementations in the cloud (FOCUS-C), in the fog (FOCUS-F) and in the hybrid fog-cloud model (FOCUS-H), in terms of their response time and the network bandwidth consumption.

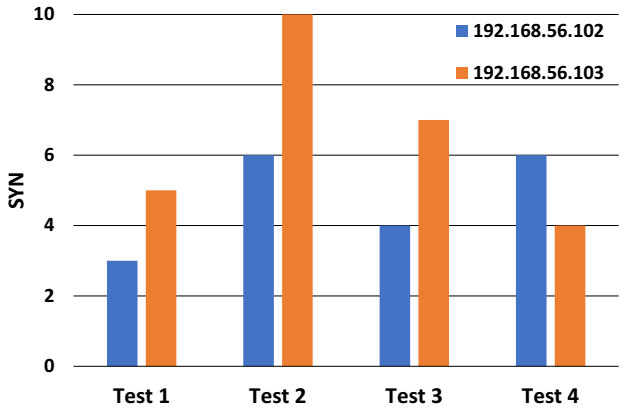
Figure 5a compares FOCUS-C, FOCUS-F and FOCUS-H in terms of the average response time performance. We can see that as the number of requests increases, the average response time for all the approaches increases. FOCUS-F performs the best when the number of requests is small, however, its response time increases exponentially as the number of requests increases (e.g., even worse than



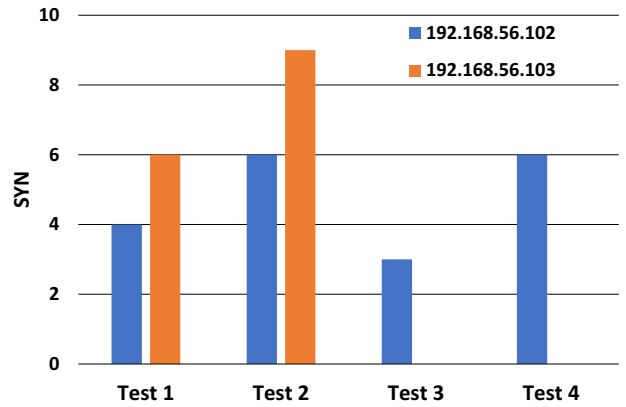
(a) No. of Packets Without FOCUS



(b) No. of Packets With FOCUS



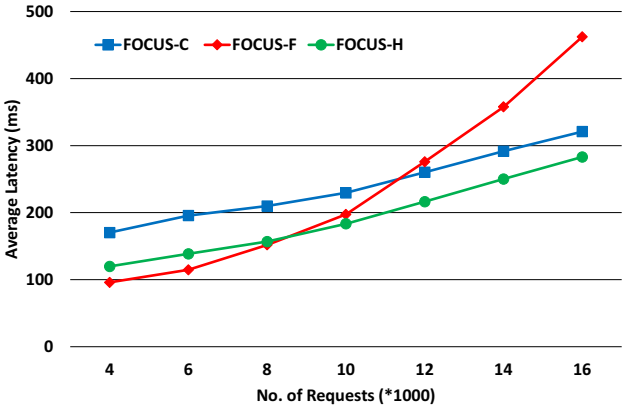
(c) No. of SYN Sessions Without FOCUS



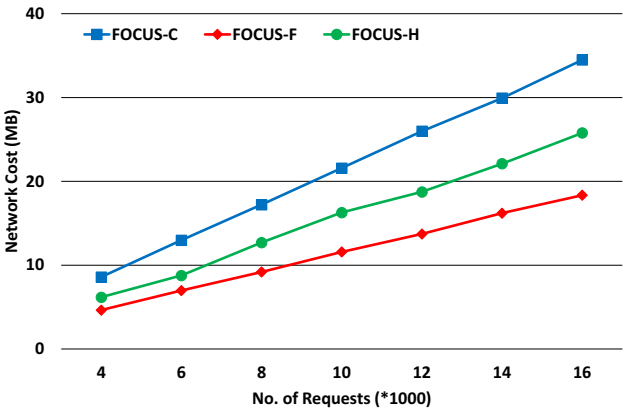
(d) No. of SYN Sessions With FOCUS

Fig. 4 The protection effectiveness of FOCUS

the pure cloud implementation FOCUS-C in the end) . This is because the response of FOCUS-F may experience a very long queuing delay since it is purely implemented in



(a) Average response time of FOCUS



(b) Average network cost of FOCUS

Fig. 5 The system efficiency of FOCUS

the fog and the computational power of the fog side is limited. We can also see that the hybrid fog-cloud implementation, FOCUS-H, achieve a relatively better performance than FOCUS-C and FOCUS-F, especially when the number of requests is large. The reason behind is because FOCUS-H allows the protection workload to be shared by both the fog and cloud implementation. FOCUS-H can maintain a low response time by maintaining most of the traffic validation in the fog side that is close to the end user, while processing the additional traffic validation in the cloud which can potentially avoid the possible high queuing delay in the fog.

Figure 5b shows the network cost (e.g., network bandwidth consumption) as the number of requests increases. Here, the network cost is defined as the multiplication of the bandwidth requirement and the number of communication hops of a given request. We can observe that FOCUS-F can achieve the lowest bandwidth consumption compared to that of FOCUS-C and FOCUS-H. This is primarily because FOCUS is implemented in fog computing that is close to the end users, which yields a much smaller number of communication hops than that of FOCUS-C and FOCUS-H, which may forward traffic or a

portion of the traffic to the remote servers in the Azure cloud that requires a large number of communication hops to reach. However, this is at a cost of a higher response delay when the number of requests increases, as we can see in Fig. 5a. In contrast, FOCUS-H achieves the second best network cost performance among the three approaches. FOCUS-H achieves a much smaller network cost than FOCUS-C because most of the processing and traffic validation are still conducted in the fog side in this hybrid fog-cloud implementation.

From these two simulation results, we can conclude that the hybrid fog-cloud implementation, FOCUS-H, can well balance the tradeoff between system response time and the network cost. FOCUS-H maintains most of the protection and validation workload in the fog side that is close to the end users, so that it can maintain the short response time. Furthermore, thanks to the shared workload in the cloud, FOCUS-H can avoid the unnecessary long queuing delay caused by the limited computational power in the fog, compared to FOCUS-F. In terms of the network cost, FOCUS-H achieves a reasonable performance as it only forwards a portion of the traffic to the cloud for processing, which generates a much lower network cost compared to the pure cloud implementation FOCUS-C.

6 Conclusion

In this paper, we have proposed a FOg CompUting-based Security System (FOCUS) to enhance the security and privacy of IoT systems against malicious attacks. The proposed FOCUS system has a double protection scheme. It first adopts a VPN to secure the communications to the IoT devices, and then applies a challenge-response authentication to further protect the VPN server against DDoS attacks. We have implemented FOCUS in a hybrid fog-cloud infrastructure and conducted a set of physical experiments to evaluate its performance. The results have shown that FOCUS can effectively filter out various malicious attacks, thanks to the decision tree classification and the challenge-response authentication. We have also shown that the hybrid fog-cloud implementation of FOCUS can achieve a very low response latency given that most of the protection and validation workload are addressed in the fog that is close to the end users, while the additional workload is addressed in the cloud. In addition, we have shown that the hybrid fog-cloud implementation of FOCUS can obtain a very small amount of network cost because of the flexible workload share between the fog and cloud, in which only a portion of the traffic needs to be transferred to the cloud for processing.

As for our future work, we plan to explore other machine learning-based network traffic classification methods, such as the Support Vector Machine classifier and Naive Bayes Network classifier, to have a more accurate network traffic classification to detect the malicious attacks. Furthermore, we plan to extend FOCUS to a more distributed implementation in both fog and cloud infrastructure, as well as implementing a load balancer to well distribute the workload between fog and cloud, in order to increase the system scalability as well as meeting the requirements by the heterogeneous IoT devices in different networks. Finally, in our future experiments, we plan to demonstrate the effectiveness and efficiency of FOCUS using real-world IoT applications and scenarios, e.g., smart home systems, interconnected vehicular systems, etc.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
2. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **99**, 1–17 (2017)
3. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. **99**, 1–10 (2017)
4. Ridhawi, I., Moayad, A., Kotb, Y., Ridhawi, Y., Jararweh, Y.: A collaborative mobile edge computing and user solution for service composition in 5G systems. Trans. Emerg. Telecommun. Technol. **29**(11), e3446 (2018)
5. Chiang, M., Zhang, T.: Fog and IoT: an overview of research opportunities. IEEE Internet Things J. **3**(6), 854–864 (2016)
6. Yi, S., Li, C., Li, Q.: A survey of fog computing: concepts, applications and issues. In: Proceedings of the Mobidata'15, pp. 37–42 (2015)
7. Ahmed, A., Ahmed, E.: A survey on mobile edge computing. In: Proceedings of IEEE ISCO'16, pp. 1–8 (2016)
8. Liu, A., Chen, F.: Privacy preserving collaborative enforcement of firewall policies in virtual private networks. IEEE Trans. Parallel Distrib. Syst. **22**(5), 887–895 (2011)
9. Bonetto, R., Bu, N., Lakkundi, V., Olivereau, A., Serbanati, A., Rossi, M.: Secure communication for smart IoT objects: protocol stacks, use cases and practical examples. In: Proceedings of WoWMoM'12, pp. 1–7 (2012)
10. Niruntasukrat, A., Issariyapat, C., Pongpaibool, P., Meesublak, K., Aiumsupucgul, P.: Anun Panya Authorization mechanism for MQTT-based Internet of Things. In: Proceedings of ICC'16 workshops, pp. 1–7 (2016)
11. Kakanakov, N., Shopov, M.: Adaptive models for security and data protection in IoT with Cloud technologies. In: Proceedings of IEEE MIPRO'17, pp. 1001–1004 (2017)
12. Alrawais, A., Alhothaily, A., Hu, C., Cheng, X.: Fog computing for the Internet of Things: security and privacy issues. IEEE Internet Comput. **21**(2), 34–42 (2017)
13. Rios, R., Roman, R., Onieva, J. A., Lopez, J.: From SMOG to Fog: a security perspective. In: Proceedings of IEEE FMEC'17, pp. 56–61 (2017)

14. Batool, S., Saqib, N. A., Khan, M. A.: Internet of Things data analytics for user authentication and activity recognition. In: Proceedings of IEEE FMEC'17, pp. 183–187 (2017)
15. Mukherjee, B., Neupane, R., Calyam, P.: End-to-end IoT security middleware for cloud-fog communication. In: Proceedings of IEEE FMEC'17, pp. 151–156 (2017)
16. Huang, Q., Yang, Y., Wang, L.: Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. IEEE Access **5**, 12941–12950 (2017)
17. Sohal, A., Sandhu, R., Sood, S., Chang, V.: A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. **74**, 340–354 (2018)
18. Aloqaily, M., Otoum, S., Ridhawi, I., Jararweh, Y.: An Intrusion Detection System for Connected Vehicles in Smart Cities. Elsevier Ad Hoc Networks, Amstredam (2019)
19. Fu, J., Liu, Y., Chao, H., Bhargava, B., Zhang, Z.: Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing. IEEE Trans. Ind. Inform. **14**(10), 4519–4528 (2018)
20. Wu, Y., Tseng, H., Yang, W., Jan, R.: DDoS Detection and Traceback with Decision Tree and Grey Relational Analysis. In: Proceedings of IEEE MUE'09, pp. 1–9 (2009)
21. PyLoris.: https://sourceforge.net/projects/pyloris/

Rajaputhri Maharaja is a graduate student in Department of Computer Science, California State University Los Angeles. Her research interests are security and privacy in Internet of Things.

Prashant Iyer is a graduate student in Department of Computer Science, California State University Los Angeles. His research interests are system and algorithm design in Internet of Things.

Zilong Ye is an Assistant Professor at California State University Los Angeles. He received his Ph.D. degree from the State University of New York at Buffalo. He received his B.S. from Shandong University in 2007 and his M.S. from Shanghai Jiao Tong University in 2010. His research interests lie in computer networking, Internet of Things, software-defined networking, network function virtualization, and optical networking. He served as TPC co-chair of the 1st International Workshop on SDN and NFV, 2017 and the 1st International Symposium on 5G Emerging Technologies, 2017.