Technical and Security challenges of Cloud-based Storage Management for IoT Devices

Alen Badrajan
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
a.badrajan@student.utwente.nl

***Abstract*—With each year IoT devices become more popular for public clients in form of Smart Devices and their storage management is a question of research and implementation for many academians and industry professionals. Providing the computational task to the modern Cloud Service Providers(CSP) or local Cloud-based infrastructure often involves network and security challenges which conditions for creating such vulnerabilities must exist, how to mitigate them and optimizations in the storing system. Due to the mass commercialization of IoT devices and their alarmingly increasing number, modern infrastructure for hosting and operations maintenance is necessary to further provide quality services to customers. Optimization methods for storage management and security improvements are developed and proposed regularly, but their implementation in the cloud diverges by the used methodologies, meanwhile, the locally managed infrastructure requires deep knowledge and funds from commercial organizations managing IoT infrastructure. This research aims to contribute to the IoT field by summarizing the related security issues, and storage management challenges and studying small-scale budget solutions with limited processing power and memory for network monitoring.**

***Index Terms*—IoT, Storage Management, Security of Cloud-infrastructure, Fog computing**

I. Introduction

The number of IoT devices involved in the daily routine increase with each year for regular consumers, business clients and academia. Most of the time IoT devices represent diverse sensors connected to the networking layer, so only a few of them have local storage and the computational processes are forwarded to a server, which involves many networking and security challenges along the way [1] [2] [3].

As the number of IoT devices increases and becomes available for a broader audience mentioned by Y. Ghaleb et al. [4], the storage question arises and often regular consumers go for a Cloud-based solution, but some medium-sized businesses may choose to have all the processes on their own infrastructure for various reasons, where implementing such solution would involve multiple engineers. For regular customers, these devices might be Smart Cameras for their home security or RFID cards for public transport, where businesses use them for office authentication. Researchers have been intrigued by the challenges imposed by IoT devices and their infrastructure management as well as methods of improvement and optimizing their network and storage aspects. Traditionally IoT devices don't have local storage or it is mostly limited and based on a physical layer connection(e.g. an SD card), lack maintenance and operational capabilities, where the integration with Cloud services mitigate this problem, but evokes new optimization [1] [5] [6] [7] and security issues [2] [3] [8] [9] with their own proposed solutions. They are further described in the related work section.

This paper intends to provide researchers with an overview of the methods for managing IoT devices from security and storage perspectives, study solutions for existing challenges in IoT infrastructure and ideas for optimization of the processes. We also experiment with a small-scale IoT device(Raspberry Pi 4) and its capabilities of mitigating and detecting a man-in-the-middle attack in the network, by measuring the used memory and CPU overload. We propose the following research questions(RQs) for this paper to answer the topics mentioned earlier.

1) How IoT devices manage their storage locally and Cloud-based?
2) What security issues and challenges affect the IoT-integrated cloud/fog infrastructure?
3) What are the minimum requirements for IoT devices to be protected against ARP spoofing using an IDS?

First question studies how storage management is organized for IoT devices in the cloud and locally(further described as Fog), providing basic definitions of IoT cloud-fog infrastructure, data organization and storage methodologies. The second question researches the common security challenges, mentioning the security attacks affecting IoT and methods of their mitigation. In the end, an experiment by measuring the used resources of a Raspberry Pi 4 hosting an IDS for mitigation purposes, while being attacked using ARP poisoning is provided.

II. Related Work

The used articles were mainly gathered through Google Scholar, FindUT and IEEE using such terms as "IoT", "IoT (storage OR infrastructure) management", "IoT Cloud", "IoT security", "Fog computing", "Fog storage management" to study the general aspects of secure storage management of IoT devices, generic documentation about IoT devices with Cloud-based solutions, and possible improvements. Generic searches which helped to set up the experiment

Article	Description
[1], [5], [6]	storage methods in IoT cloud
[14], [2], [15]	IoT security threads
[13], [7], [11], [9], [16]	cloud data storage/management optimization proposal
[3], [17]	IoT cloud challenges
[4]	Raspberry Pi information
[12], [18]	fog data management description/optimization proposals
[19], [20], [21]	fog description
[22], [23]	comparison of fog and cloud computing
[24]	cloud-fog security issues
[25], [26], [27], [28], [29], [30]	fog security issues/challenges
[8]	energy consumption optimization
[31], [32], [33], [34], [35], [10], [36], [37]	ARP poisoning and IDS

Table I. Classified citations by theme

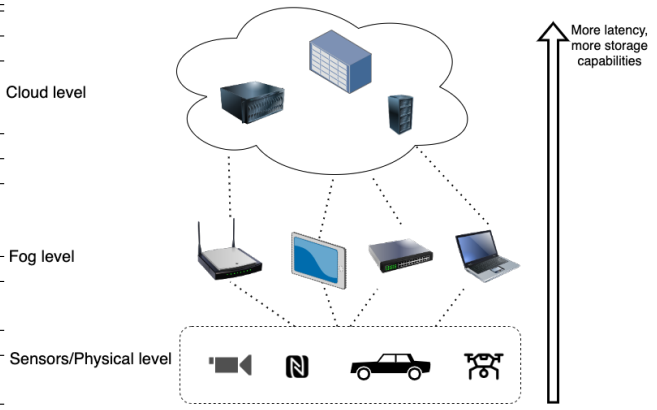

Fig. 1. Fog computing architecture

were "Raspberry Pi setup","arp spoofing", "Snort" as later in the study was mentioned in [10] as possible solutions against the above-mentioned attack.

They involve proposals for storage optimisation on cloud computing L. Qian et all [11], networking optimization X. Zhao et al. [7] and data storage optimization in Cloud Computing Platforms L. Jiang et al. [6], a proposal for storage management for non-relational databases based on NoSQL T. Li et al. [5], a method of lowering the power usage of IoT devices in a storage-less environment N. Chang et al. [8], decreasing network load on Cloud Computing by integrating it with Fog Computing Y. Liu et al. [12]. Also, the overall security challenges for the integration of IoT and Cloud A. A. Mohiuddin et al. [2], general technical and security challenges in IoT and Cloud Computing [3] [13] [9], and the overviewed storage methods in the cloud for IoT and their overall challenges B. Xu et al. [1]. Table.I summarizes the citations used in the article categorized by their topic.

III. How IoT devices manage their storage locally and Cloud-based?

A. Fog storage management

Cases for a locally-based infrastructure, where the IoT devices directly access their storage system and have computational capabilities, are typically represented in Fog computing infrastructures. M. Iorga et al. [19] provide an expanded explanation of the concepts, but Fog computing represents an extension of the cloud infrastructure, focused on the management of its fog nodes which could be any IoT devices with local computation, storage or network capabilities being it physical or virtual.

A simplified example of the Fog architecture is represented in Fig. 1 indicating how the more computation capabilities component has in the Fog infrastructure, the more latency in the network it has to cope with.

The nodes communicate with each other on a separate network layer, whereas summarised by S. Yi et al. [21], their general goals are low latency, location awareness, geographical distribution, scalability, support for mobility, real-time interactions, heterogeneity, interoperability and support for online analytics and interplay with the cloud. Typical applications benefiting from Fog computing and open research questions discussed by V. Kumar et al. [22] and R. Rani et al. [18] are cyber-physical systems(e.g. autonomous driving, traffic monitoring), fusion and aggregation(e.g. geo-distributed systems), rendering and decoding processes like video streaming, where optimisation methods are constantly developed by the leading industry companies, and academia. Jeong, Y. S et al. [13] proposes a secure and scalable IoT storage system capable of integrating with all other components in the Cloud-based infrastructure. For decreasing the network load and optimizing the storage capabilities such as data fusion, data organization and transmission Zhang, Z. J. et al. [12], propose an integration scheme of Fog components with Cloud computing practices.

Due to its edge location in the network, Fog computing is subjected to various security threats, as Qin, Y. et al. [20] categorise them into twelve types of security issues, later to find six possibly negative factors: virtualisation issues, web security issues, internal/external communication issues, data security related issues, and wireless malware protection. Havinga, P. et al. [23] provides an extensive overview of fog/cloud challenges and discusses the used algorithms for solving the Load Balancing and Energy consumption issues.

B. Cloud-based storage management

As opposed to the fog system where local devices handle the data storage and processing, as Havinga, P. et al. [23] mentioned, in cloud-based infrastructure, IoT devices are typically in the perception A. V. Vasilakos et al. [1] or physical sensing layer Jemai, A. et al. [14] being represented by various sensors(e.g thermostats, GPS-integrated devices, real-time cameras). They transmit the collected IoT data via the network layer, which is forwarded to the Cloud-based Application Layer. A. V. Vasilakos et al. [1] describe the cloud-based application layer as consisting of the Data

Acquisition and Integration Module, Data Storage Module, Data Management Module, Data disposing Module, data mining module and more. First, the raw files are transmitted on UDP or TCP protocols and afterwards stored on one of the provided storage systems. Such systems can be for example relational(e.g MS SQL Server, MySQL) or non-relational(NoSQL) databases or also can be distributed in Hadoop (HDFS), where the data is isolated in layers for multiple tenants. Non-relational databases also could improve their storage management system by the method provided by Mao, W. et al. [5] based on NoSQL.

Many people choose to save their data on the cloud due to the flexible storage capabilities and safety insurance from the chosen cloud provider, as Ren, J. et al. [38] mentioned and then further described modern research focuses on cloud storage systems, defining four major topics: the encryption, data integrity, data deletion and memory leakage-resilient systems. Daud, A. et al. [17] extensively describes cloud storage issues, defining data security for which public key inscription, trusted timestamps and directory services are the basic techniques for mitigating the confidentiality, integrity, data access, authentication, authorization, management, and data breaches issues. Later, Daud, A. et al. [17] overviews the data management issues which cope with data dynamics and validity problems, virtualization vulnerabilities, backup, availability and data locality(edge backup servers) issues. For ensuring the correct user management and data security on the IoT cloud network, Liu, X. et al. [16] propose an attribute-based encryption scheme with key revocation and decryption key exposure resistance.

IV. What security issues and challenges affect the IoT-integrated cloud/fog infrastructure?

A. IoT fog infrastructure challenges

Fog devices being deployed at the edge of the network are exposed to diverse security issues such as man-in-the-middle, password protection, mutual authentication, insider issue attack, replay and DoS attack as summarized by Amin, R. et al. [24]. A common example of cyber attacks which affect the Fog nodes is the man-in-the-middle attack as the low computation power and memory usage is hardly detected by the traditional anomaly detection methods and are stealthy, as Luan, H. et al. [26] described in his study.

To protect against intrusion and identify the trusted hardware, Smart Environment Monitoring(SEN) or Intrusion Detection Systems(IDS) are used, but these can't guarantee a totally safe system, since the hardware is also often subjected to vulnerability attacks as Ãsterberg, P. et al. [25] mentioned. Kumar, V. et al. [27] classified the research challenges in fog security and defined five open research questions: trust, privacy preservation, authentication and key agreement, IDS, dynamic join and leave of the fog node, and lastly fog forensics which involves the legal regulations. The trust question implies that in the Fog network, the nodes should be programmed to identify and communicate with each other, a feature which is already provided by the CSP with assuring security certifications, Privacy Preservation should protect against man-in-the-middle attacks as the authentication and key agreement should ensure a non-compromisable authentication, where the Intrusion Detection Systems are used to protect and detect infected nodes in the system, and scalability networking problems arise in the dynamic join and leave of the fog nodes question et Kumar, V. al. [27].

Havinga, P. et al. [23] described in detail the common challenges for fog, cloud and edge computing, briefly enumerating them adhering to fog computing:

1) Serverless computing
2) Energy consumption
3) Data management and locality
4) Orchestration in Fog for IoT
5) Business and service models
6) Load balancing
7) Security and efficiency issues
8) Data integrity and availability

Ranjan, R. et al. [28] identified and classified the common security threads and solutions on all three layers of fog computing, where for the sensing layer the threads are node capturing/device tampering, spoofing attacks, DoS-based attacks, Node outage and more. By Ranjan, R. et al. [28] the application layer encounters sniffer/loggers, phishing attacks, injections, session hijacking, social engineering, DDoS and more. Abdullahi, M. et al. [29] surveyed the security techniques in Fog environments, dividing them by machine learning, cryptographic, computational intelligence techniques and others (e.g. Honeypot, Virtualization, etc.).

Collecting the mentions from the discussed above challenges and issues, the man-in-the-middle attack and DDoS attacks are the most common problems for fog computing systems Al-Fayoumi, M. et al. [30].

B. IoT cloud infrastructure challenges and optimization

The cloud layer of the IoT infrastructure is subjected to diverse cyber attacks on all OSI networking layers, as Jemai, A. et al. [14] provided an overview of all the security attacks and threats, most common of which are eavesdropping on the physics layer, man-in-the-middle and DDoS attacks on the network layer, flooding attacks on the transport layer, malicious injection on the application layer and impersonation on the data and cloud layers. Jemai, A. et al. [14] suggest the standardization of lightweight encryption algorithms and the use of machine learning for IoT applications to secure the infrastructure and network. Havinga, P. et al. [23] classified the common challenges and proposed algorithms of the cloud environments which interact closely with fog networks, naming load balancing and energy consumption. In combination with the mentioned threads above by Jemai, A. et al. [14], a summarized table of IoT cloud challenges is represented in Table.II.

Multiple researchers such as A. V. Vasilakos et al. [1] propose methods for optimizing the storage capabilities in the IoT cloud and improving the cache management and data

Layer	Problems	Proposed solutions
Application	Injectionet al. [14]	AES and RSAet al. [14]
Transport	Floodinget al. [14]	TCP/UDP flooding Protection schemaset al. [14]
Network	Man-in-the-Middle and DDoset al. [14]; Load-balancinget al. [23]	IDS and VPNet al. [14]; DRAM, ERAet al. [23]
Physical	Eavesdroppinget al. [14]; Energy Consumtionet al. [23]	Faraday cageet al. [14]; RR et al. [23], Power-lowering algorithmet al. [8]

Table II. IoT Cloud problems and solutions on OSI layers

latency for IoT networks like Lin, Q. et al. [11], which proved to be more effective than the traditional FastCFS. Powerful combinations of IoT infrastructures could be achieved as methods for network bandwidth optimizations Wang, H. et al. [7] and power usage lowering of storage-less IoT devices Chang, N. et al. [8] are proposed. Such combinations might include geographically restrained systems where a constant power source is not present, but has periodic access to the network. Xu, B.et al. [6] proposed a solution for coping with large amounts of data and complex classifications of data management with multiple data types and database systems. Open questions on the security issues such as "Can we establish standard security measures for all type of smart things? How to enable the smart things to choose between cloud, edge, fog and mist computing?" [2], are still studied and discussed.

V. What are the minimum requirements for IoT devices to be protected against ARP spoofing using an IDS?

While gathering academic articles and searching for popular attacks on IoT networks, the man-in-the-middle attack(MITM) was mentioned considerately in the majority of citations, [14], [20], [24], [25], [26], [27], [31], [32], [33], [34], [10], which itself is available due to the limitations of the ARP protocol and its' vulnerability to ARP Cache Poisoning as [31] mentioned. Further, the authors described the ARP protocol as being used for linking the IPs and MAC addresses of the common network-connected devices, where due to the lack of its' security, it can be misused maliciously to perform Denial of Service(DoS) and Man-in-the-Middle attacks. Subbulakshmi, T. et al. [32] represented in detail the necessary steps to perform an ARP spoofing attack and the prevention method of statically defining the ARP tables, which however by Nachreiner, C. [31] is considered inconsistent for large networks.

Multiple defensive techniques are available and being researched against ARP spoofing like enchanting the classical ARP protocol to an advanced version, capable of memorizing on a long-term basis the ARP table like Kim, J. et al. [33] proposed MR-ARP or using an ARP central server with separate hardware like Tapaswi, S. [34] suggested, but such methods under the six classification scheme provided by Tripathi, N. et al. [35], falls under the Centralized Detection and Validation Server, which itself is vulnerable to the flood of spoofed ARP messages, not resistant to the IP Exhaustion problem and non-resistant to single point of failure problem.

Modern IDS(Intrusion Detection System) like Snort or Suricata could help to monitor and actively mitigate ARP attacks, as Snort itself can be activated in alert and mitigation mode, as Baloda, V. et al. [10] did and experimented with a cost-effective solution on their campus network using Raspberry Pi 4. However, such a device has at least 1GB of RAM and such capabilities are not available for all IoT devices(e.g Smart-bulbs using Zigbee protocol like Philips Hue Bradley, M. et al. [15]), which motivated the study of the resources consumption of an IDS, activated on a small scale IoT node like Raspberry Pi 4.

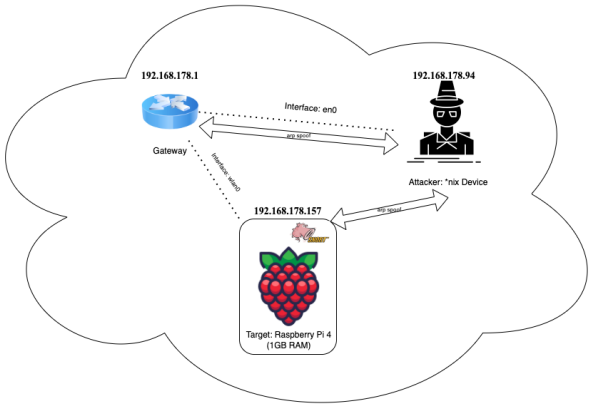

Fig. 2. Network scheme of the used setup

A. Realization of an ARP Poisoning attack

To perform the ARP Poisoning attack, the intruder should already be connected to the network. First, the attacker searches for the connected devices on the network using 'arp -a' command and chooses the target, an example of which is shown in Fig.3 and an overview of the devices connected to the network which will take part in the attack is represented in Table.III showing the IP and MAC addresses of the used devices, followed by the network scheme of the setup Fig.2.

```
~> arp -a
? (169.254.47.216) at 90:78:41:5e:1b:90 on en0 [ethernet]
? (192.168.178.1) at ac:22:5:c7:4a:a1 on en0 ifscope [ethernet]
? (192.168.178.38) at e:1b:7b:56:4:57 on en0 ifscope [ethernet]
? (192.168.178.94) at 18:3e:ef:b8:f2:61 on en0 ifscope permanent [ethernet]
? (192.168.178.157) at dc:a6:32:8:36:b5 on en0 ifscope [ethernet]
? (192.168.178.192) at 7e:c1:86:63:dc:84 on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

Fig. 3. Attacker's 'arp -a' output

Device	IP addresses	MAC addresses
Attacker	192.168.178.94	18:3e:ef:b8:f2:61
Target	192.168.178.157(or .159)	dc:a6:32:8:36:b5
Gateway	192.168.178.1	ac:22:5:c7:4a:a1

Table III. Devices in the network

Before the effectuation of the ARP spoofing, the target receives the correct MAC address of the gateway Fig.4. The attacker spoofs both the gateway and the target at the same time using the ‘arpspoof‘ command Fig.5 and Fig.6, after which the target’s connection is highjacked and all the data packets are sent to the attacker, as the gateway has the attacker’s MAC addresses in Fig.7.

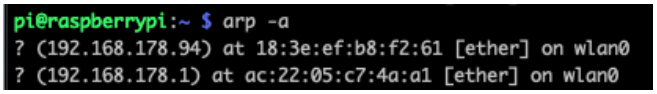

Fig. 4. Target’s ‘arp -a‘ output before the attack

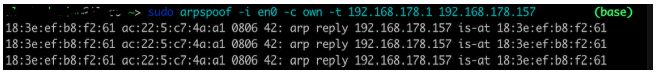

Fig. 5. ARP Poisoning attack execution ‘gateway target‘

Fig. 6. ARP Poisoning attack execution ‘target gateway‘

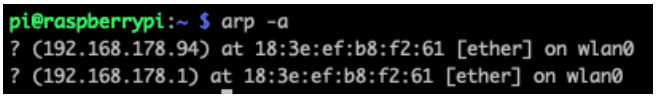

Fig. 7. Target’s ‘arp -a‘ output after the attack

Using a packet tracer like Wireshark, the attacker can investigate the packets sent by the target Fig.8 and await for some non-encrypted requests (e.g. telnet, HTTP). As the ARP spoofing is interrupted, the traffic returns back to normal Fig.9.

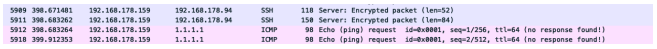

Fig. 8. Wireshark’s output during the attack

Fig. 9. Wireshark’s output during and after the attack

B. ARP Poisoning mitigation on Snort

Following the guidelines for the installation and script setup for acquiring the metrics from [37], Snort 2.9 was installed on the Raspberry Pi and tested in diverse alert modes: console Fig.10 and cmg Fig.11. Using Snort without any alert mode during the attack period Fig.12 detects approximately 7% from all the packets, which was found at the time the attacker spoofed the network.

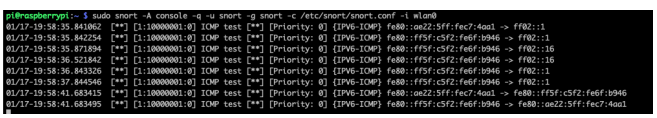

Fig. 10. Snort output in ‘console‘ alert mode

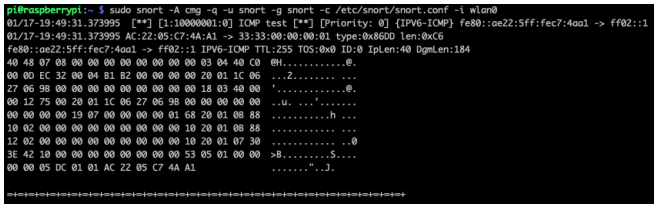

Fig. 11. Snort output in ‘cmd‘ alert mode

Fig. 12. ARP detected packets by Snort during the attack

C. Acquired metrics

Utilizing the script provided by [37], the metrics including the CPU usage, CPU temperature and RAM usage were collected for different snort alert modes, repeating the procedure 10 times to detect any possible change of resource usage during the attack and without it. The amount of used memory observed during the experiment did not variate. There were no significant differences between any of the used alert modes as shown by the collected metrics Fig.13 and Fig.14. We will focus our attention on the amount of RAM used while the application is running. Snort took roughly 55MB of memory and 12-17% CPU usage. Judging from these aspects, it would be reasonable to assume an IoT device with the same technical specifications of 1GB RAM and similar processing power to Raspberry Pi 4 implementing an IDS, like Snort for the detection and mitigation of ARP poisoning attacks or Suricata if the device has lower technical capabilities. IoT devices which can implement IDS and act as network monitoring and alarm tool can be tablets, laptops and micro-computers such as Raspberry Pi which have the necessary memory and computation power to support the running application. Smaller IoT devices without the possibility to run an IDS like smart bulbs cannot act as a defensive device on the network.

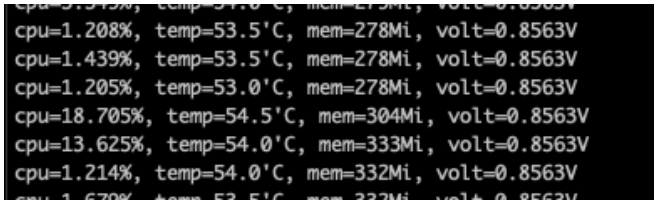

Fig. 13. ‘Cmg‘ mode data before and during the attack

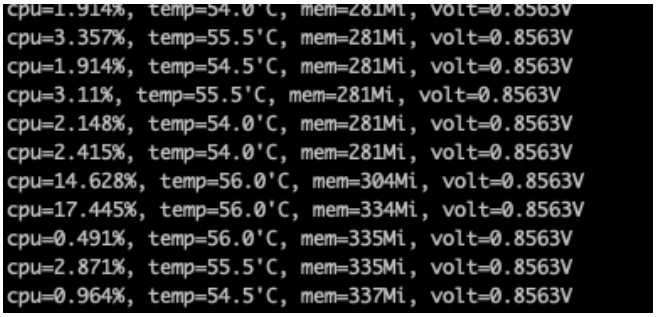

Fig. 14. 'Console' mode data before and during the attack

VI. Discussion

This section describes our findings on the imposed RQs.

IoT devices are connected to either cloud or fog systems which take care of the computation tasks, by storing the data on databases hosted on servers or at edge locations. Both being similar to each other, face typical cloud storage challenges such as data integrity and security, and network load and latency problems

The man-in-the-middle and DDoS attacks are one of the most common security threads affecting fog networks, which can be mitigated and monitored using an IDS. Common challenges include data integrity, load balancing, energy consumption and organization in Fog. Cloud infrastructure also deals with similar problems as fog networks, but their integration of IoT is not as focused as in fog.

The experiment has shown that running an IDS on a small-scale IoT device (Raspberry Pi 4) roughly takes 55 MB and a similar device is needed for securing a local network.

VII. Conclusion and Future Work

The lack of legislation and standards for IoT devices and their implementations creates diverse approaches and as a result, different security loopholes.

As researchers constantly propose new optimization methods and protocol upgrades to cope with security attacks fog and cloud IoT infrastructure, future proposals for ensuring the data storage&operation safeness and network latency/load could improve the overall situation of IoT storage. Further proposals for increasing the security of IoT networks can study the combating and monitoring aspects of such systems under network attacks such as man-in-the-middle and DDoS.

The experiment has shown that implementing an IDS on edge nodes of IoT infrastructure, requires relevant computation and memory capabilities according to the chosen IDS. Less capable devices than Raspberry Pi could use a more lightweight IDS that could help low-resource IoT devices to mitigate the ARP poisoning problem like Suricata which proved to be CPU efficient as compared by Ahn, S. et al. [36] to Snort. Researchers could investigate how Suricata or other light IDS work on low-resource IoT nodes.

Acknowledgment

Many thanks, to my supervisor S. Simonetto and coordinator dr.ir. A. Chiumento for the provided guidance during the whole duration of the thesis.

References

[1] L. J. H. Cai, B. Xu and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," *IEEE Internet of Things Journal*, vol. 4, pp. 75–87, 2017.

[2] . A. A. Mohiuddin, I., "Security challenges and strategies for the IoT in cloud computing," *In 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE*, pp. (pp. 367–372)., 2020.

[3] A. N. M. Z. S. R. A. D. M. S. A. S. . Z. R. R. Sadeeq, M. M., "IoT and Cloud computing issues, challenges and opportunities: A review." *Qubahan Academic Journal*, vol. 1(2), pp. 1–7, 2021.

[4] d. C. D. A. . Z. Y. Ghaleb, T. A., "On the popularity of internet of things projects in online communities." *Information Systems Frontiers*, vol. 24(5), pp. 1601–1634., 2022.

[5] L. Y. T. Y. S. S. . M. W. Li, T., "A storage solution for massive IoT data based on NoSQL," *In 2012 IEEE International conference on green computing and communications. IEEE*, vol. (pp. 50-57)., 2012.

[6] D. X. L. C. H. J. Z. B. F. . X. B. Jiang, L., "An IoT-oriented data storage framework in cloud computing platform," *IEEE Transactions on Industrial Informatics*, vol. 10(2), pp. 1443–1451, 2014.

[7] L. D. E. S. X. . W. H. Zhao, X., "Reliable IoT storage: Minimizing bandwidth use in storage without newcomer nodes." *IEEE Communications Letters*, vol. 22(7), pp. 1462–1465, 2018.

[8] . C. N. Lee, H. G., "Powering the IoT: Storage-less and converter-less energy harvesting." *In The 20th Asia and South Pacific Design Automation Conference. IEEE*, pp. (pp. 124–129), 2015.

[9] L. Y. B. Y. Z. . A. M. Shahrul, M., "Hierarchical Naming Scheme In Named Data Networking for Internet of Things: A Review and Future Security Challenges," *IEEE Access*, vol. 10, pp. 19 958–19 970, 2022.

[10] S. A. V. P. . B. V. Varma, P., " Snort IDPS using Raspberry Pi 4," *International Journal of Engineering Research Technology (IJERT)*, vol. 9, 2020, July.

[11] Q. Z. C. M. Y. B. W. X. W. J. . . L. Q. Qian, L., "FastCache: A write-optimized edge storage system via concurrent merging cache for IoT applications," *Journal of Systems Architecture*, vol. 131, 102718, 2022.

[12] L. Y. C. H. C. B. B. K. . Z. Z. J. Fu, J. S., "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 14(10), pp. 4519–4528, 2018.

[13] S. F. C. S. L. K. C. . J. Y. S. Jiang, H., "A secure and scalable storage system for aggregate data in IoT," *Future Generation Computer Systems*, vol. 49, pp. 133–141, 2015.

[14] S. A. A. J. A. Mrabet, H.; Belguith, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors*, vol. 20, 3625, 2020.

[15] . B. M. De La Cruz, J., " Philips Hue Bulb IoT App Security ."

[16] Y. G. M. Y. . L. X. Xu, S., " A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. ," *Future Generation Computer Systems*, vol. 97, pp. 284–294, 2019.

[17] B. A. J. S. A. A. A. . D. A. Ghani, A., "Issues and challenges in cloud storage architecture: a survey. ," *arXiv preprint arXiv:2004.06809.*, 2020.

[18] K. N. K. M. K. A. . B. A. Rani, R., "Storage as a service in Fog computing: A systematic review." *Journal of Systems Architecture*, vol. 116, 102033, 2021.

[19] F. L. B. R. M. M. J. G. N. S. . M. C. Iorga, M., "Fog computing conceptual model." 2018.

[20] P. S. . Q. Y. Khan, S., "Fog computing security: a review of current applications and security solutions. ," *Journal of Cloud Computing*, vol. 6(1), pp. 1–22, 2017.

[21] H. Z. Q. Z. . L. Q. Yi, S., "Fog computing: Platform and applications." *In 2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)*, pp. 73–78, 2015.

[22] L. A. A. K. S. S. M. . B. A. A. Kumar, V., "Comparison of fog computing cloud computing." *Int. J. Math. Sci. Comput*, vol. 1, pp. 31–41, 2019.

[23] C. A. B. R. A. A. . H. P. Mijuskovic, A., " Resource management techniques for cloud/fog and edge computing: An evaluation framework and classification." *Sensors*, vol. 21(5), p. 1832, 2021.

[24] S. A. . A. R. Kunal, S., "An overview of cloudâfog computing: Architectures, applications with security challenges." *Security and Privacy*, vol. 2(4), e72, 2019.

[25] S. A. . Ã. P. Butun, I., "Hardware security of fog end-devices for the internet of things," *Sensors*, vol. 20(20), 5729, 2020.
[26] W. S. H. X. . L. H. Stojmenovic, I., "An overview of fog computing and its security issues." *Concurrency and Computation: Practice and Experience*, vol. 28(10), pp. 2991–3005, 2016.
[27] M. R. S. L. M. L. F. M. A. C. N. . K. V. Mukherjee, M., "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19 293–19 304, 2017.
[28] M. S. P. B. S. A. M. G. . R. R. Puthal, D., " Fog computing security challenges and future directions ," *IEEE Consumer Electronics Magazine*, vol. 8(3), pp. 92–96, 2019.
[29] A. S. I. M. C. H. A. C. H. . A. M. Yakubu, J., " Security challenges in fog-computing environment: a systematic appraisal of current developments. ," *Journal of Reliable Intelligent Environments*, vol. 5(4), pp. 209–233, 2019.
[30] A.-F. M. . A.-F. M. Ashi, Z., " Fog computing: security challenges and countermeasures," *Int. J. Comput. Appl*, vol. 175(15), pp. 30–36, 2020.
[31] C. Nachreiner, "Anatomy of an ARP poisoning attack," *Retrieved*, vol. 4, 2005.
[32] R.-S. . S. T. Majumdar, A., "ARP poisoning detection and prevention using Scapy. ," *In Journal of Physics: Conference Series*, vol. 1911, No. 1,, p. 012022, 2021.
[33] K. D. . K.-J. Nam, S. Y., "Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks. ," *IEEE communications letters*, vol. 14(2), pp. 187–189, 2010.
[34] . T. S. Kumar, S., "A centralized detection and prevention technique against ARP poisoning ," *In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. (pp. 259–264, 2012, June.
[35] . M. B. M. Tripathi, N., " Analysis of various ARP poisoning mitigation techniques: A comparison." *In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE*, pp. 125–132, 2014, July.
[36] . A. S. Park, W., " Performance comparison and detection analysis in snort and suricata environment. ," *Wireless Personal Communications*, vol. 94(2), pp. 241–252, 2017.
[37] A. Morales, "Running Snort on a Raspberry Pi as a gateway ," *SCU's Internet of Things Research Lab*, 2019. [Online]. Available: https://www.siotlab.us/running-snort-on-a-raspberry-pi-as-a-gateway/
[38] X. N. . R. J. Yang, P., "Data security and privacy protection for cloud storage: A survey ," *IEEE Access*, vol. 8, pp. 131 723–131 740, 2020.