Blueprint for a Secure Container to Protect Data in Edge Cloud Computing Environment

Seong-Jin Kim*
sys.ryan0902@gmail.com
Department of Computer and Information Security,
Sejong University
Seoul, Republic of Korea

Ki-Woong Park
woongbak@sejong.ac.kr
Department of Computer and Information Security,
Sejong University
Seoul, Republic of Korea

ABSTRACT

Edge computing is a computing technology that collects, analyses and processes data near the devices that generate the data. This enables services providers to curtail unnecessary data transmissions and deliver low latency services. Cloud computing technology has evolved from centralized environment to edge computing environment due to the need of handling drastically increasing amount of data in cloud computing environments. As the cloud computing environment went through changes, there has been emerging security issues caused by the high mobility of containers. The increased mobility of containers in edge computing environment increased the possibility of data leakage because containers migrate between the edge nodes and we cannot be assured that the data was completely deleted from the edge node the container previously resided. To enhance security of the data in the edge cloud computing environment, we suggest a blueprint of the secure container to protect data from potential threats.

CCS CONCEPTS

• **Computer systems organization** → **Cloud computing**; • **Security and privacy** → *Virtualization and security*.

KEYWORDS

edge computing, cloud computing security, container, data protection, container mobility

ACM Reference Format:
Seong-Jin Kim and Ki-Woong Park. 2020. Blueprint for a Secure Container to Protect Data in Edge Cloud Computing Environment. In *2020 ACM International Conference on Intelligent Computing and its Emerging Applications (ACM ICEA '20), December 12–15, 2020, GangWon, Republic of Korea.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3440943.3444355

1 INTRODUCTION

Traditionally, a lot of services have relied on the cloud computing architecture in large centralized data centers to increase flexibility and efficiency of using hardware resources [1]. But, there are a few hindrances in this architecture when it comes to efficiently employing it. According to the Cisco Global Cloud Index (2016-2021), researchers forecast that the global cloud data center traffic will reach 19.5 zettabytes per year by 2021 [2]. Also, the skyrocketing need of transferring, analyzing and processing large data related to IoT, autonomous vehicles and smart factories makes it difficult for the conventional centralized cloud computing environment to meet such need [7]. A huge amount of data should be transferred to central server located far away from the source of data, which can be too slow for the applications that require real-time service. To satisfy the demands for low latency and extremely high bandwidth for nowadays' unprecedentedly increasing data, the traditional cloud computing is going through a paradigm shift. The final destination of this paradigm shift is the technology called edge computing [1]. Edge computing is a computing technology that minimizes unnecessary data transmissions and provides low latency services by collecting, analyzing and processing data at the vicinity of the devices that generate the data. Many existing businesses have already started to prepare for ushering in cloud edge computing including Amazon [8] and IBM [4]. Surely, edge computing will increase the efficiency of cloud computing environment. However, this change – the movement to shift to the edge computing – creates new security challenges to overcome at the same time. Edge computing increases the mobility of data and containers in cloud computing environment and this makes users or administrators to hesitate to employ cloud computing technology out of fear of sensitive data leakage such as classified or private data. Ensuring the confidentiality of data in cloud environment will enable variety of service areas that handle medical, financial, public and personalized sensitive information to actively utilize cloud computing environment. To guarantee confidentiality of data throughout the creation, transfer, and deletion in cloud edge computing platform, we suggest a blueprint for secure containers that protect and manage data.

2 RELATED WORK

There has been extensive research regarding transferring containers from one node to another, and this technology is usually called container migration. Nadgowda [6] presented live container migration service by using CRIU-based memory migration. The application downtime of this migration service is only limited to the CRUI's in-memory state transfer

ACM ICEA '20, December 12–15, 2020, GangWon, Republic of Korea

ACM ISBN 978-1-4503-8304-2/20/12.
https://doi.org/10.1145/3440943.3444355

time. Lele Ma [5] proposed container migration method by employing Docker container layer management and image stacking to minimize file system synchronization overhead. Additionally, Govindaraj [3] discusses the requirements and challenges of Edge Computing environment and proposes a live migration method termed redundancy migration that decreases the downtime. The majority of previous researches on container live migration were focused on minimizing the downtime. This is a very important aspect of container live migration technology and there were many innovative designs for this. However, there is limited consideration of the data security in containers. As the data in the container moves from one node to another, it is imperative that the container migration service provides the security of data. Container users and administrators expect the data in the container to be safely managed. Our purpose in this paper is proposing a method of securely managing data in the container.

3 DESIGN

In this section, we suggest the requirements that the secure container should meet, the challenges to overcome to satisfy the requirements and finally the possible solutions for the challenges.

3.1 Requirements of the secure container

The secure container we propose in this paper should meet the following requirements:

- `Isolation of data`: The data in the secure containers should reside only in the isolated virtual area which is confined to CPU and Memory so that it can be protected from being unintentionally stored in random storage. Maintaining the data only in the isolated virtual area makes it possible to completely delete the data without relying on the system's data-deletion mechanism.
- `Completeness of deletion`: The deletion operation of the container must ensure complete removal of data. Complete removal means that the data must be unrecoverable after it is deleted.
- `Spotlessness of migration`: When a container moves from one edge to another, the data of the secure container should be safely move without leaving any trace on the previous edge

3.2 Challenges and solutions

Unfortunately, there are a few challenges to overcome to satisfy the requirements mentioned above. We discuss the challenges and suggest the possible solutions in this section. Firstly, we talk about the isolation of data. The secure container makes the data to stay only in the isolated virtual area which only includes CPU and memory. Figure 1 shows a conceptual image of the Isolated virtual area. Forcing the data to reside only in isolated virtual area ensures that the data is not written to the random storages. This is important since data keeps moving between edges in edge computing environment. The user or administrator will not want security-sensitive

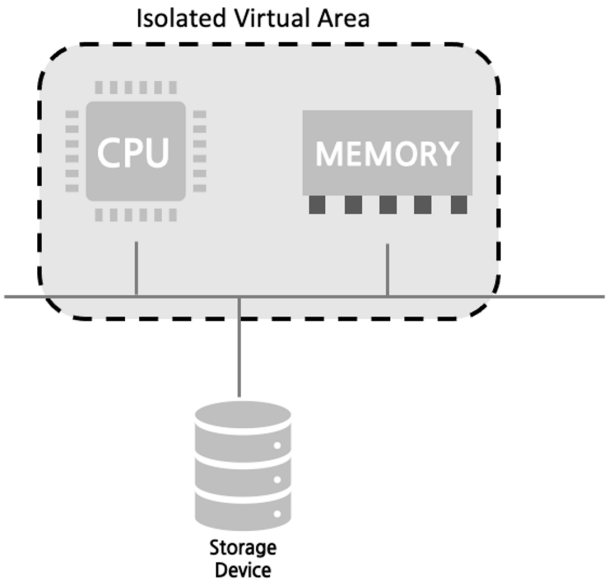

Figure 1: Isolated virtual area

data to be stored in the random storage of many edges since they cannot be assured that the data stored in the random storage will be safely managed. To create isolated virtual area which is confined to CPU and Memory, we use in-memory file system such as tmpfs. In addition, to prevent data from being swapped by the operating system and unintentionally stored in storage device, we need to disable swapping by delicately configuring operating system environment.

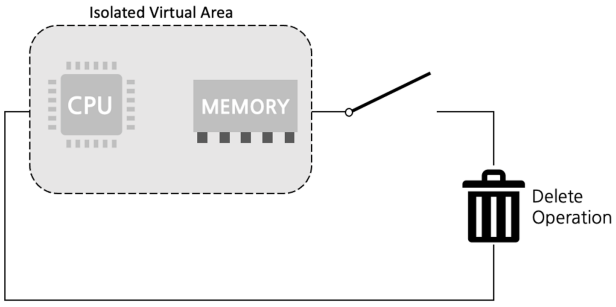

Figure 2: Absolute data deletion operation

Additionally, the secure container has to guarantee that the deletion of the data in the container is absolute. The deleted data should never be able to be accessed after the owner of the data delete it. To achieve this goal, as shown in figure 2, we provide our own data deletion operation that completely removes data from isolated virtual area. Since the secure container keeps data only in the isolated virtual area as mentioned above, we can provide this feature by overwriting memory area occupied by the data.

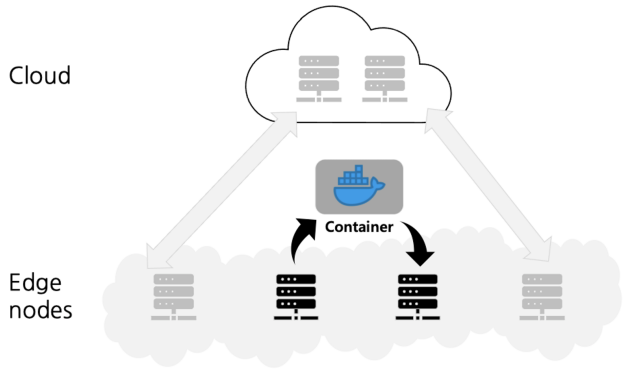

Figure 3: Spotless migration of the secure container

Finally, the secure container should support spotless migration in the edge computing environment. To this end, a protocol for secure container migration in the edge computing environments is needed. The protocol must ensure that the migrated container does not allow possible adversaries from accessing data through the previous edge that the container resided before migration.

4 CONCLUSION

As the paradigm of cloud computing shifts from the centralized environment to the edge computing because of increasing demands for low latency and high bandwidth, new security vulnerabilities have emerged. And there is high need for ensuring the security of data in edge cloud computing environment. In this paper, we suggest a blueprint for secure containers that protect and manage data to satisfy the rising security need. We proposed three major requirements for the secure container as follows. 1) Isolation of data, 2) Absoluteness of Deletion, 3) Spotlessness of migration. Also, to overcome challenges in providing the requirements of secure container, we devised possible solutions accordingly. By ensuring the confidentiality of data in edge cloud computing environment, we expect that we can encourage a number of service areas that handle sensitive or classified information to make use of cloud computing environment.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) (NRF2020R1A2C4002737) and the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2018-0-00420).

REFERENCES

[1] Beth Cohen, Gergely Csatári, Bruce Jones, David Paterson, Ildikó Váncsa. [n.d.]. Edge Computing: Next Steps in Architecture, Design and Testing. https://www.openstack.org/use-cases/edge-computing/edge-computing-next-steps-in-architecture-design-and-testing/.

[2] CISCO. 2018. Edge Computing: Next Steps in Architecture, Design and Testing. https://newsroom.cisco.com/press-release-content?articleId=1908858.

[3] K. Govindaraj and A. Artemenko. 2018. Container Live Migration for Latency Critical Industrial Applications on Edge Computing. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vol. 1. 83–90. https://doi.org/10.1109/ETFA.2018.8502659

[4] IBM. 2020. What is new in IBM Watson IoT Platform. IBM Knowledge Center. https://www.ibm.com/support/knowledgecenter/en/iot/overview/whats_new.htm

[5] Lele Ma, Shanhe Yi, and Qun Li. 2017. Efficient Service Handoff across Edge Servers via Docker Container Migration. In *Proceedings of the Second ACM/IEEE Symposium on Edge Computing* (San Jose, California) *(SEC '17)*. Association for Computing Machinery, New York, NY, USA, Article 11, 13 pages. https://doi.org/10.1145/3132211.3134460

[6] S. Nadgowda, S. Suneja, N. Bila, and C. Isci. 2017. Voyager: Complete Container State Migration. (2017), 2137–2142. https://doi.org/10.1109/ICDCS.2017.91

[7] Peter Middleton and Joseph Unsworth. 2016. Forecast: IoT Data Storage Capacity, 2013-2020. Gartner Research. https://www.gartner.com/en/documents/3375517/forecast-iot-data-storage-capacity-2013-2020.

[8] SUZY VISVANATHAN. 2018. VMware Cloud on AWS Outposts: Cloud Managed SDDC for your Data Center. https://cloud.vmware.com/community/2018/11/28/vmware-cloud-aws-outposts-cloud-managed-sddc-data-center/.