Section: PUBP-6727

Mutual Monitoring in the Cloud

Alexander Stein

Problem Statement

Cloud computing infrastructure is essentially ubiquitous, but adoption is not without challenges. Cloud service providers must cater to customers in regulated sectors, complying with cybersecurity frameworks that create high barriers to entry. One barrier is ongoing evaluation of the provider's cybersecurity posture, often resulting in centralized bureaucracies. FedRAMP oversees and documents a prominent example of such a program, the Continuous Monitoring Program.

Are these bureaucracies an optimal solution, or a last resort that fails to keep pace with cloud technology as it proliferates and evolves? If they are a last resort, is there a better way?

Solution Statement

I will use this research to design and evaluate an alternative to centralized continuous monitoring, mutual monitoring. The foundation of mutual monitoring will be federated data services, known in other security use cases as transparency services. The services will necessarily change cloud service provider and customer behavior, while also incentivizing auditors to sell value-add analytics services in these data services, and possibly obsolete centralized authorities like FedRAMP.

Completed Tasks (Last 2 Weeks)

1. I presented a proposal and reviewed scope of research with four advisors that are highly familiarity with FedRAMP strategy, policies, and operations. Three advisors have accepted, while one's acceptance is still pending.

2. I began an outline for critical analysis for FedRAMP's centralized continuous monitoring model (e.g. proposal deliverable #1).

3. I initialized a code repository to save the architecture documents and prototype code in version control (e.g. proposal deliverables #3 and #4, respectively).

4. I incorporate feedback from Professor Kuerbis to add and adjust research topics and evaluation methods in my outline for the project and specific deliverables.

    - How is mutual monitoring different from continuous assessment?
    - Are machine-readable compliance artifact's like NIST OSCAL related, competing, or complimentary?
    - Do cloud providers currently assess and monitor one another? How?
    - What are the incentives to expose posture data in a peer-to-peer model?
    - What mechanisms and disincentives prevent abuse or manipulation?

Tasks for the Next Project Report

In the next two weeks, I will focus on the following goals. I have sorted them in order of priority.

1. Complete first draft of federated data service architecture, request feedback from advisors.

2. Implement primary component of data service, submission API for cloud service providers and external third-party auditors.

3. Complete outline of FedRAMP critical analysis.

4. Start draft of FedRAMP critical analysis, request feedback from advisors.

Questions or issues I'm having

Alignment with Practicum Requirements

1. My project focuses on a policy challenge in cloud security, but does not have a conventional policy recommendation like other policy track proposals. Is a policy document an explicit requirement?

Project Scope

1. One of my deliverables (a critical analysis of FedRAMP's current approach) is ancillary, but will establish important qualitative background. Should I include this deliverable in the final project appendix or use it as an input for a summary analysis in the final report only?

2. One of my deliverables will be a prototype of federated data service, which will have server and client components that does statistical analysis of data without a user-friendly web interface to keep scope focused and the timeline reasonable?

3. If I cannot complete all the code for the prototype and I must scope down the prototype and describe the future to keep to my proposed schedule, will this negatively impact my final grade for this project or is this normal?

Evaluation and Measurement

1. I am proposing a novel solution that is considerably different from the current state, and the latter is not easily measurable. (It is also why I think the problem is important.) However, direct comparison is difficult. Is there any significant risk to my project if I design quantitative and qualitative metrics?

Methodology Paragraph Summary

Timeline

Week #	Description of Task	Status
W1	Initialize code repository for prototype service	Complete
W1	Present proposal to advisors and integrate feedback; obtain commitment from advisors	In Progress
W1	Read FedRAMP documentation for ConMon processes	In Progress
W1	Begin outline of FedRAMP ConMon critical analysis	In Progress

Evaluation

Report Outline

References

Aldribi, A., Traore, I., & Letourneau, G. (2015, August). Cloud slicing a new architecture for cloud security monitoring. In *2015 ieee pacific rim conference on communications, computers and signal processing (pacrim)* (p. 18-22). IEEE. Retrieved 2025-05-24, from http://dx.doi.org/10.1109/PACRIM.2015.7334802 doi: 10.1109/pacrim.2015.7334802

Cambric, S., & Ratemo, M. (2023). *Cloud auditing best practices*. Birmingham, England: Packt Publishing. Retrieved 2025-05-23, from https://learning.oreilly.com/library/view/cloud-auditing-best/9781803243771/

Campitelli, V., Catteddu, D., & Maria, J. D. (2020). *Csa's perspective on cloud risk management.* cloudsecurityalliance.org. Retrieved 2025-05-24, from https://cloudsecurityalliance.org/artifacts/csa-s-perspective-on-cloud-risk-management

Carvallo, P., Cavalli, A. R., Mallouli, W., & Rios, E. (2017). Multi-cloud applications security monitoring. In *Green, pervasive, and cloud computing* (p. 748-758). Springer International Publishing. Retrieved from http://dx.doi.org/10.1007/978-3-319-57186-7_54 doi: 10.1007/978-3-319-57186-7_54

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2020, May). A novel security-by-design methodology: Modeling and assessing security by slas with a quantitative approach. *Journal of Systems and Software*, *163*, 110537. Retrieved from http://dx.doi.org/10.1016/j.jss.2020.110537 doi: 10.1016/j.jss.2020.110537

FedRAMP. (2025). *Fedramp csp authorization playbook.* Retrieved 2025-05-18, from https://web.archive.org/web/20250413105351/https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook.pdf

Gartner. (2024). *Gartner forecasts worldwide public cloud end-user spending to total $723 billion in 2025.* Retrieved 2025-05-18, from https://web.archive.org/web/20250415023404/https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts

-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

Ismail, U. M., Islam, S., & Islam, S. (2016, August). Towards cloud security monitoring: A case study. In *2016 cybersecurity and cyberforensics conference (ccc)* (p. 8-14). IEEE. Retrieved from http://dx.doi.org/10.1109/CCC.2016.8 doi: 10.1109/ccc.2016.8

Kuerbis, B., & Mueller, M. (2023, September). Exploring the role of data enclosure in the digital political economy. *Telecommunications Policy*, *47*(8), 102599. Retrieved from http://dx.doi.org/10.1016/j.telpol.2023.102599 doi: 10.1016/j.telpol.2023.102599

Kunz, I., Schneider, A., & Banse, C. (2022). *A continuous risk assessment methodology for cloud infrastructures.* arXiv. Retrieved from https://arxiv.org/abs/2206.07323 doi: 10.48550/ARXIV.2206.07323

Laurie, B. (2014, August). Certificate transparency: Public, verifiable, append-only logs. *Queue*, *12*(8), 10-19. Retrieved 2025-05-24, from https://dl.acm.org/doi/pdf/10.1145/2668152.2668154 doi: 10.1145/2668152.2668154

Lewis Commission. (2025). *Faster into the cloud: Accelerating federal use of cloud services for security and efficiency.* Center for Strategic and International Studies. Retrieved 2025-05-18, from https://web.archive.org/web/20250116234900/https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250115_Lewis_Cloud_Commission.pdf

Majumdar, S., Madi, T., Wang, Y., Tabiban, A., Oqaily, M., Alimohammadifar, A., … Debbabi, M. (2019). *Cloud security auditing*. Cham, Switzerland: Springer Nature. Retrieved 2025-05-23, from https://link.springer.com/book/10.1007/978-3-030-23128-6

Mireles, J. D., Ficke, E., Cho, J.-H., Hurley, P., & Xu, S. (2019, December). Metrics towards measuring cyber agility. *IEEE Transactions on Information Forensics and Security*, *14*(12), 3217-3232. Retrieved 2025-05-25, from http://dx.doi.org/10.1109/TIFS.2019.2912551 doi: 10.1109/tifs.2019.2912551

Rescorla, E. (2023a). *A hard look at certificate transparency: Ct in reality.* Retrieved 2023-05-23, from https://educatedguesswork.org/posts/transparency-part-2/

Rescorla, E. (2023b). *A hard look at certificate transparency, part i: Transparency*

systems. Retrieved 2023-05-23, from https://educatedguesswork.org/posts/transparency-part-1/

Rescorla, E. (2024). *Why it's hard to trust software, but you mostly have to anyway.* Retrieved 2025-05-24, from https://educatedguesswork.org/posts/ensuring-software-provenance/

Soveizi, N., & Turkmen, F. (2023). *Secflow: Adaptive security-aware workflow management system in multi-cloud environments.* arXiv. Retrieved from https://arxiv.org/abs/2307.05137 doi: 10.48550/ARXIV.2307.05137

stackArmor. (2024). *How much does fedramp compliance cost?* Retrieved 2025-05-18, from https://web.archive.org/web/20240808151743/https://stackarmor.com/how-much-does-fedramp-compliance-cost/

Torkura, K., Sukmana, M. I., Cheng, F., & Meinel, C. (2021, March). Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security*, *102*, 102124. Retrieved from http://dx.doi.org/10.1016/j.cose.2020.102124 doi: 10.1016/j.cose.2020.102124

Weir, G. R. S., & Aßmuth, A. (2024). *Strategies for intrusion monitoring in cloud services.* arXiv. Retrieved from https://arxiv.org/abs/2405.02070 doi: 10.48550/ARXIV.2405.02070

Appendix

Updated Proposal

Practicum Proposal: Mutual Monitoring in the Cloud

Alexander Stein
astein38@gatech.edu

1 Problem Statement

Cloud computing infrastructure is essentially ubiquitous, but adoption is not without challenges. Cloud service providers must cater to customers in regulated sectors, complying with cybersecurity frameworks that create high barriers to entry. One barrier is ongoing evaluation of the provider's cybersecurity posture, often resulting in centralized bureaucracies. FedRAMP oversees and documents a prominent example of such a program, the Continuous Monitoring Program (2025, p. 14).

Are these bureaucracies an optimal solution, or a last resort that fails to keep pace with cloud technology as it proliferates and evolves? If they are a last resort, is there a better way?

2 Choice of Problem

The cybersecurity of cloud services poses many challenges, but the inefficiency of continuous monitoring has systemic impact on the economics and timely, accurate risk modeling for heavily interconnected, interdependent systems built on cloud services. FedRAMP is a highly visible and representative example that other regulatory frameworks emulate, so any improvement or optimization will yield significant improvement to cloud service adoption across regulated industries.

2.1 Economic Impacts

Although FedRAMP is a highly visible cloud security program, there is limited public data with details about costs and economic impact for providers, auditors, and customer agencies. However, industry estimates significant costs for all these stakeholders, even when considering global expenditure on cloud services.

Gartner estimates that global spending on cloud infrastructure in 2024 was $595.7 billion dollars (2024). The think tank CSIS estimates that the United States government spent $17 billion of its total $130 billion dollar IT budget in 2024 on cloud

services alone (2025, p. 1). Although federal agencies are not fully compliant with FedRAMP's requirements mandated in the FedRAMP Authorization Act, the long-term goal is maximal oversight over the cloud building blocks of this seventeen billion dollar investment. And continuous monitoring is a sizable component of this investment.

FedRAMP processes require specialized tools operated by dedicated staff, from providers, auditors, and often the customer agencies. Analysts at stackArmor estimate that an initial authorization costs a provider $250,000 to $750,000 dollars, of which $100,000 to $400,000 alone is for continuous monitoring activities (2024). Given a conservative estimate, any improvement or optimization can benefit all stakeholders in reducing $42,600,000 in spend by 426 services currently authorized, but potentially a much larger sum.

2.2 Cybersecurity Impacts

Even with all this investment, the staff from cloud service providers, auditors, and agency customers experience strategic and operational bottlenecks for heavily interconnected cloud services, increasing ambiguity in a holistic view of cybersecurity posture in real-world composite systems for all parties involved, not only auditors.

Firstly, a centralized review process finalized by a small number of FedRAMP staff constitutes a single point of failure. As FedRAMP documents, cloud providers, auditors, and agency customers must use a single, centralized wiki site, USDA's connect.gov, and coordinate out of band with FedRAMP staff for final review (2025, pp. 3,14). Paradoxically, providers and auditors get no guarantees for the cybersecurity posture of this system where they store data for FedRAMP's reviewers. There is no mutual monitoring or assurance. Access to this data on connect.gov is manually coordinated on an ad hoc basis, hindering sharing between different agency staff who need FedRAMP data, and even those outside these agencies focused on other regulatory frameworks. They rely on reciprocity guarantees to justify the use of FedRAMP authorization and continuous monitoring, which is not particularly feasible in practical terms given restricted access to this data.

The impacts of manually curated data from FedRAMP's continuous monitoring extend beyond its stakeholders. Interrelated regulatory frameworks depend upon it. Given FedRAMP's rigorous review process, especially continuous monitoring, many

providers and their auditors use artifacts from FedRAMP for equivalency, or reciprocity,as evidence for controls in other regulatory frameworks preferred by the defense, commercial, and finance sectors of the United States. Therefore, any optimization in FedRAMP's processes has second order effects on the quality, quantity, and speed of cloud security review methodologies across industry.

3 Expected Deliverables

I will use this research to design and evaluate an alternative to centralized continuous monitoring, mutual monitoring. The foundation of mutual monitoring will be federated data services, known in other security use cases as transparency services. The services will necessarily change cloud service provider and customer behavior, while also incentivizing auditors to sell value-add analytics services in these data services, and possibly obsolete centralized authorities like FedRAMP. To do so, I propose the list of deliverables below, in addition to the final report summarizing their outcome.

1. a critical analysis of FedRAMP's continuous monitoring model
2. an architecture specification for mutual continuous monitoring
3. prototype code for transparency services for mutual continuous monitoring
4. a quantitative cloud security measurement framework to use in the prototype

References

FedRAMP. (2025). *Fedramp csp authorization playbook.* Retrieved 2025-05-18, from https://web.archive.org/web/20250413105351/https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook.pdf

Gartner. (2024). *Gartner forecasts worldwide public cloud end-user spending to total $723 billion in 2025.* Retrieved 2025-05-18, from https://web.archive.org/web/20250415023404/https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

Lewis Commission. (2025). *Faster into the cloud: Accelerating federal use of cloud services for security and efficiency.* Center for Strategic and International Studies. Retrieved 2025-05-18, from https://web.archive.org/web/20250116234900/https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-01/250115_Lewis_Cloud_Commission.pdf

stackArmor. (2024). *How much does fedramp compliance cost?* Retrieved 2025-05-18, from https://web.archive.org/web/20240808151743/https://stackarmor.com/how-much-does-fedramp-compliance-cost/