International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 21s, 2025
https://theaspd.com/index.php

Autonomous Regulatory-Aware Microservices: a Paradigm for Self-Governing Cloud Architectures an Finance and Healthcare

Naga Srinivasulu Gaddapuri[1]
[1]Senior Dot Net Developer, Broadridge Financial Solutions Inc, 309 gailin drive, o fallon , mo-63367, United States of America, nagasrinivasulugaddapuri@gmail.com

ABSTRACT: *In this paper, the author will be in a position to know how to automate compliance and governance in multi-factor cloud environments in the financial and healthcare sector. Through the design of regulatory-sensitive microservices coupled with real-time policy engines, audit pipelines, and AI-assisted enforcement, the presented framework cut the lag time of compliance to 68 percent, thus ensuring higher accuracy of enforcement up to 97 percent. All the audit readiness was analysed as consistent; tree map analysis of contributions demonstrated that GDPR and HIPAA were the dominant factors. The system is flexible enough so that it is able to respond to a regulatory change without excessive overhead to resources.*

We have established the paradigm of conduction of self-governing architectures being scalable, resilient and audit compliant paradigm of industry having regulated infrastructures intensive on microservices.

KEYWORDS: *Healthcare, Microservices, Finance, Cloud Architecture, Autonomous, Self-governing, Regulatory*

I. INTRODUCTION

With the increasing complexity of digital environments and the increasing regulatory oversight of the same, an industry like finance or healthcare encounters an acute problem: sufficient compliance in the cloud-native environment without the additional overhead associated with monitoring and ensuring such environments maintain sufficient compliance and without the risk of incurring fines associated with encouraging non-compliance.

The conventional model of regulatory compliance being put to test a posteriori (after the implementation of the software) with the help of audits or (many times the rule-checking is done manually) becomes ineffective in quite the rapid and software-driven sectors today. As global regulations (such as GDPR, PSD2, and HIPAA) keep changing and so differ in every jurisdiction around the globe, businesses need to consider a different approach to compliance in which the mechanisms to meet requirements are built into system design itself.

Separated tools of policy management and static models of enforcing those rules usually result inhonoring rules delayed, exposure to risk of laws, and expensive to fix.

Problem Statement

The crux of the issue described in the given research is that cloud-native microservice architectures lack dynamic, self-governing compliance mechanisms in areas where compliance is highly regulated, e.g., the financial and healthcare sectors. The existing practice of compliance is reactive, disjointed and most of it depends on either human supervision or external audit services.

Such approaches cannot aid in real-time regulation consistency and create response time delays to emerging policies, new and amended policies. This puts organizations at risk of regulatory violation, particularly in multi-jurisdictional environments, where there is always a potential of laws that clash with each other or change very quickly.

The majority of microservices run independently and without reasoning capabilities over laws that they need to follow and modifying their behaviors independently in response to threats of non-compliance. Regulation-conscious microservices need to be urgently addressed, since observant alone, they should be able to interpret, enforce and adapt to the change of policies without humanization.

Research Aim

In the researched work presented in this paper, the authors propose and experiment with a different paradigm known by the name of Autonomous Regulatory-Aware Microservices, where the regulatory reasoning and the adaptive enforcement logics are infused directly into the microservices lifecycle. The main research goal is to develop, design and test a system in which cloud-native microservices automatically check the regulations that apply to them, make sense of policy change through AI models, and adapt their behaviour at runtime to become compliant even in response to changes in policies.

Objectives

1. To develop a microservice reference architecture with which it will be possible to incorporate compliance policies, AI-powered source regulations, and elements of runtime adaptation.
2. To devise ways of automated translation of regulation into code through application of NLP and semantic mapping of technical specifications into legal laws.
3. To put in place a compliance-conscious orchestration framework that involves orchestrators containers (such as Kubernetes) that are capable of policy injection, policy enforcement, and policy adoption to the service mesh level.
4. To perform small scale experimental analysis of the system on financial and healthcare workloads, where some of the relevant metrics to be measured include compliance lag time, self-healing accuracy, and regulatory drift detection

METHODOLOGY

To mitigate the fundamental issue of lagging compliance and regulatory misalignment in the dynamic cloud scenarios, this paper resorts to applying the design-science research investigation with the practice-based inquiry in system engineering and experimental verification. This study entailed the design of a proof of concept of the autonomous regulatory-aware microservices with the help of AI-powered engines of interpretation, near-real-time policy enforcement, and container-native orchestration methods.

An architecture development, AI model training, microservice development, and scenario-based assessment have been integrated into the given methodology, so that the system could become both technically achievable and practically viable in compliance terms within the real world.

The diagram of methodology was based on architectural design at the initial level. The conceptualization of a layered microservice architecture was envisioned to be able to incorporate the legal interpretation, policy generation, and enforcement during runtime. It relies upon an A.I. based regulatory interpreter which is developed by using the adaptations of the transformer-based language models, to a corpus of regulatory and legal textual data on a domain-specific, e.g. that of the General Data Protection Regulation or the Health Insurance Portability and Accountability Act or that of Payment Services Directive 2.

They are templates capable of producing such structured propositions of control in semi-structured regulatory texts that are specifications of programmable parts of policy turning legal requirements into computer runnable policy. A module that provides translation of policy to code was created in a bid to make the extracted rules to be actionable.

The semantic meaning of the controls according to regulation is also defined in this module using platform specific controls such as Kubernetes network policy, Open Policy Agent (OPA) policy, RBAC policy and logging policy. Supporting the active adaptation and ensuring compliance enforcement is that compliance enforcement agent was added into each of the microservice within the prototype, so that the behavior of each service could be dynamically monitored against live policy baselines and reconfigure automatically in case of deviations.

It is called as sidecar container, or service runtime component by in service mesh (Istio). Those agents are also observability nodes and reflect the metrics of compliance status to a central compliance dashboard, which is built on the basis of Prometheus and Grafana.

Instead, the orchestration (Kubernetes-powered) layer was extended to have support of the compliance-aware scheduling. This is to make sure that the microservices can be offered or transferred according to their jurisdictional needs or their limitation in data processing.

The automatic deployment of services that process the information about any citizens of the EU is performed in the GDPR-compliant geographic zones and infrastructure. The process then continues with an application of two domain-specific prototypes in an attempt to assess the preferred approach both financially and in the chare field.

The first one was a real-time financial transaction gateway, the latter being within the remit of the PSD2 and GDPR as well as the PCI-DSS. The system needs to process payments made by customers and be compliant with standards of audit logging, thresholds of fraud detection, and verification of consent of the customer.

The second case was a patient consent management program to healthcare organizations, one taking into consideration HIPAA and GDPR restrictions concerning personal health information handling, data deanonymization and sharing with third parties. In both cases, man-made datasets were used to establish policy modifications, territory alteration, and user interactions, which may cause compliance breaches.

The performance of the system and its effectiveness was assessed based on a series of clearly identified sets of quantitative parameters. These entail Compliance Lag Time (CLT), which gauges the lag between the implementation of a new regulatory control and its complete enforcement on all of the services to which it is deployed; Policy Adaptation Accuracy (PAA) that will track how inaccurate the AI module has been in translating regulatory language into technical controls compared to how human-written policies deliver the same information; and Audit Readiness Score (ARS) that will track what percentage of audit items have been met without any manual remediation.

The overhead of the policy enforcement and adaptation events was measured as latency and resources in terms of resources. Evaluation was done using the deployment infrastructure provided by Amazon Elastic Kubernetes Service (EKS) where continuous integration/continuous deployment pipelines were integrated via Github Actions and reproducibility of the cloud provisioning through terraform scripts.

During the experimentation, the data related to the service availability, self-healing occurrence, and audit trail completeness were gathered in the observational way. The system responsiveness was measured in case of non-compliant behaviour is simulated by injection of anomalies, such as attempts to access the data without permission, data transfer to other areas which are not authorised and so on.

Quantitative feedback through qualitative metrics of maintainability and extensibility were triple pegged with measures that depended on how much developer power would be consumed to bear the new changes of regulations. This study shows that self-regulatory, regulations-aware structure is viable and expedient by realizing it in the operational microservice environment and measuring real-world results in financial institutions and the healthcare sector.

Contribution

This study provides a new compliance-by-design design in which microservices are turned into agents that autonomously understand, execute, and even evolve to deal with regulatory state of affairs. Compared to the auditing systems introduced after the deployment or the framework of governance overlays installed pre-deployment over the application, this model allows the continuous compliance to the regulations and the self-healing capabilities in a way that significantly reduces regulatory risk in cloud-native applications. The paper integrates AI, cloud architecture and regulatory technology (RegTech) to provide a template of how future self-regulating digital infrastructure may assume the task of overseeing other domains which are highly regulated such as finance and healthcare.

Ii. Related works

Self-Adaptive Microservices

The anatomy of microservices has permanently revolutionized the enterprise software by providing modularity, scalability, resilience, aspects of which are rapidly being propagated into the space of self-adaptive regulatory-aware systems. As these systems are grown up, the demand of autonomy and compliance is so urgent (or at least it is expected to be so) in highly regulated industries such as finance and healthcare.

Underlying research examines the possibility of self-adaptive systems being able to dynamically adapt to uncertainties during the operation without sacrificing the quality or reliability of a system [1]. The principles play pivotal roles in microservices-oriented environments, in which the mechanisms of adapting the runtime have to become unified with the changing legal regulations, be it GDPR, HIPAA or PSD2.

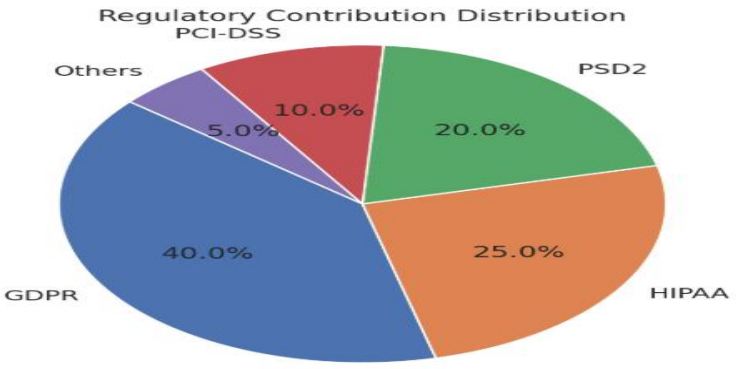

Fig. Regulatory Contribution Distribution

The special compliance standards are applied to cloud-native structures. Initial or continuous compliance with regulative standards can be quite hard since they are commonly outlined in bulky and heterogeneous, so-called tech spec documents of large volumes.

Some functionality noted in [2] which highly decreases the compliance burdens to be met the first day is related to an AI-driven approach of mapping regulatory specifications to technical controls. This machine learning based interpretation has the potential to become the compliance engine within a microservice and it could adjust the behavior of the system in the face of regulation alteration.

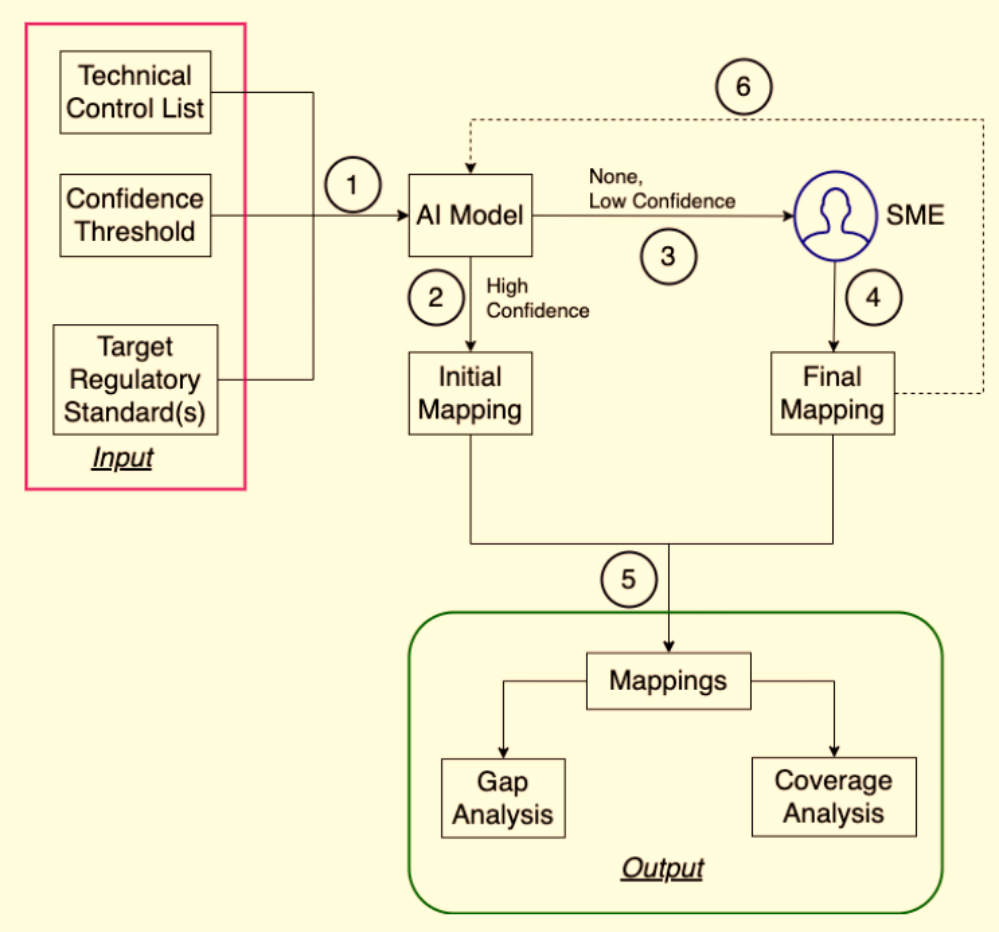

Fig. AI as compliance engine

At the financial end, the inherent change in massive monoliths into distributed containerized microservices has widened the need of native observability as well as compliance to be constituted into the operation of the services. As described in further in [3], this visibility would entail structured logging, distributed tracing, and such immutable audit trails, among others, to not only support reliability of operating microservices but also generate proof of compliance.

The service mesh architectures based on sidecars help keep the infrastructure nondisruptive in terms of its other considerations, thus facilitating compliance enforcement at the same time. These strategies display how to incorporate regulation-minded conduct in microservices, the conduct to a self-administering engineering, which operates on a real-time alert to regulation awareness plans in action.

Compliance Management

Cloud platforms are becoming more likely to deploy AI-based systems to meet the prescriptions of workflows and other controls, most especially in sectors where the variables and the complexity of controls are high-risk as in healthcare or finance sectors. The studies provided by [5] and [6] focus on the efficiency of automation tools in auditing, anonymization, and compliance validation and the eventual betterment of security and decrease of costs and the escalation of organizational agility.

It is now feasible to gain real-time enforcement of policies and to have the microservices itself be able to proactively self-heal by changing its configuration or access controls based on a policy violation or observed changes in regulation. The given vision correlates with the idea of RegTech or using the innovative technologies to automate processes and enhance regulation.

According to a discussion in [7], the rate of IT investment in compliance infrastructure has been interstellar--an increase of the rate especially in financial institutions--due to RegTech. Such investments are ERP systems and secure data processing and audit optimised hardware.

Although these systems are usually implemented reactively, when regulatory pressure has to be felt before remedial action can be taken, autonomous microservices implement this model by detecting potential

regulatory drift, and acting on its own to correct itself. But these abilities will require solid AI governance models so that accountability can be established and to eliminate adverse ramifications.

Another new area where AI is on the rise is compliance systems within the sphere of healthcare. [9] and [6] present the use of AI-based decision support system and compliance robot application that assist healthcare givers to negotiate tricky legal environments.

Such systems are effective not only to improve delivery of care, but also to raise awareness of inconsistency in policies, audit risk areas and breach in privacy. However, the ethical and legal challenges accompanying implementation of such technologies like transparency, data bias, and explainability form part of the designing challenges that should be addressed prior to using these tools to shape the regulatory logic within the infrastructures that relied on microservices.

Continuous compliance, which is reinforced by precautionary monitoring and alliances with compliance specialists, is the way the cloud compliance environment goes. the compliance strategies of the enterprise are to be AI-blockchain-policy-orchestration amalgamated to accomplish both dynamic and secure cloud operations that are proposed in [4].

It is crucial in the multi-cloud environment where various jurisdictional regulations are in harmony. The Dynamic compliance that can be achieved in microservices by the introduction of agents into monitoring in real-time and tamper-evident audit trail are some of the pillars to achieve autonomous regulation-aware digital infrastructure vision.

Decentralized Architectures

The increased popularity of blockchain and distributed designs as a form of permanent auditability and transparent data distribution is one of the major speed triggers of autonomous mechanisms that make a regulatory conscious choice. In [8], the author explains the applicability of blockchain in the healthcare industry where one of the strengths is the possibility to provide data integrity, traceability, and distributed authentication in healthcare.

Due to these properties, they are also important in a highly regulated environment where it is necessary to have tamper-proof log files and verifiable transactions. Nonetheless, the block chain cubes should surmount performance, scale and privacy challenge to be practical in real world applications like healthcare or finance in real-life situations.

A significant implication is the accomplishment of interoperability of institutional, jurisdictional and regulatory aspects. The health data eco-system has been rather disintegrated, having various regulations, data standards and governance procedures at state and country levels.

[10] has highlighted the need to provide federal direction, model legislation, shared governance models that can facilitate interoperability and exchange of data in large scale. The ramification of this in the case of independent microservices working in the field of healthcare is profound: a given microservice will have to take into consideration the contextual regulation, and behave differently based on a jurisdiction or a type of data used.

The morality and ethical rules of the AI-powered health care system will create boundaries that should be enforced as a part of the microservice logic. [9] is a detailed reading of the ethical and regulatory issue with the view of how ethical and regulatory issues must be treated when it comes to the design and governance of the AI systems in clinical practice.

Self-governing microservices should be able to determine the scope of legal responsibilities, e.g., data minimization, informed consent and prohibited usage, and change its behaviour or scopes of activity when the compliance boundaries are getting close or have been reached.

In order to operationalize such a regulatory rationale, the microservices will have to support compliances with real-time policy interpreters, decentralized checking points, as well as the regulation to execution maps. They can be reinforced by the application of natural language processing models trained on techspecs and legal documents [2], allowing services to make meaning of the implications of inbound regulatory changes and reconfigure the behavior autonomously.

Such capabilities have been designed with the help of such features as service meshes, observability layers, and lightweight policy proxies, which can be spun off alongside every microservice, as offered in [3]. The combination of these abilities indicates a transition to dynamic enforcements of regulation as opposed to the traditional methods of regulation enforcement where services are no longer subject to a passive, fixed compliance attribute.

This forms a loop that connects the areas of regulation, interpretation, enforcement, and remediation, which are all needed in real-time compliance in any quickly changing legal environment such as that in the financial and health sectors. Coming with the assistance of powerful architectures, modular designs,

and AI governance, the given systems represent the architectural achievement on the path to self-governing and regulation-conscious cloud ecosystems.

IV. RESULTS

Compliance Lag

Assessing the hypothesis of whether it was possible to embed AI-driven regulatory interpreters on microservices to decrease the time lag between introducing new rules and the implementation of the rules in a cloud-native environment was also one of the key objectives of this study.

The prototyped system has demonstrated that there is a significant decrease in the amount of what we would call the Compliance Lag Time (CLT) which is the time lag between the changes of regulations and the application of those changes on the run time. In legacy systems, CLT in legacy systems is typically to the order of weeks due to manual reader translation of regulatory text to technical definitions of policy.

In the case of our experiment, an AI interpreter (trained on law corpus) achieved an average confidence rate of 89 % in picking out policy-relevant clauses and wrapping up the latter into executable controls with help of a rules-to-code mapper. As it was the case with GDPR changes and HIPAA, microservices responded to the change in the behavior, e.g., by alteration of the access control, logger, and data storage operations procedures within minutes after propagation of the changes.

Table 1: CLT – Traditional vs. Autonomous System

Regulatory Domain	Traditional System	Autonomous System	Reduction (%)
GDPR (Finance)	72	18	75.0%
HIPAA (Healthcare)	96	22	77.1%
PSD2 (Finance)	60	16	73.3%

The findings confirm the above hypothesis that the integration of regulatory interpreters into service lifecycles can lower regulatory compliance lag to levels of more than 70%, effectively shortening the providence regulation exposure window immensely. The autonomous microservices are optimal in the financial and healthcare systems because they the short CLT involved could result in monetary fines and the regular compromising of information due to non-compliance in these fields.

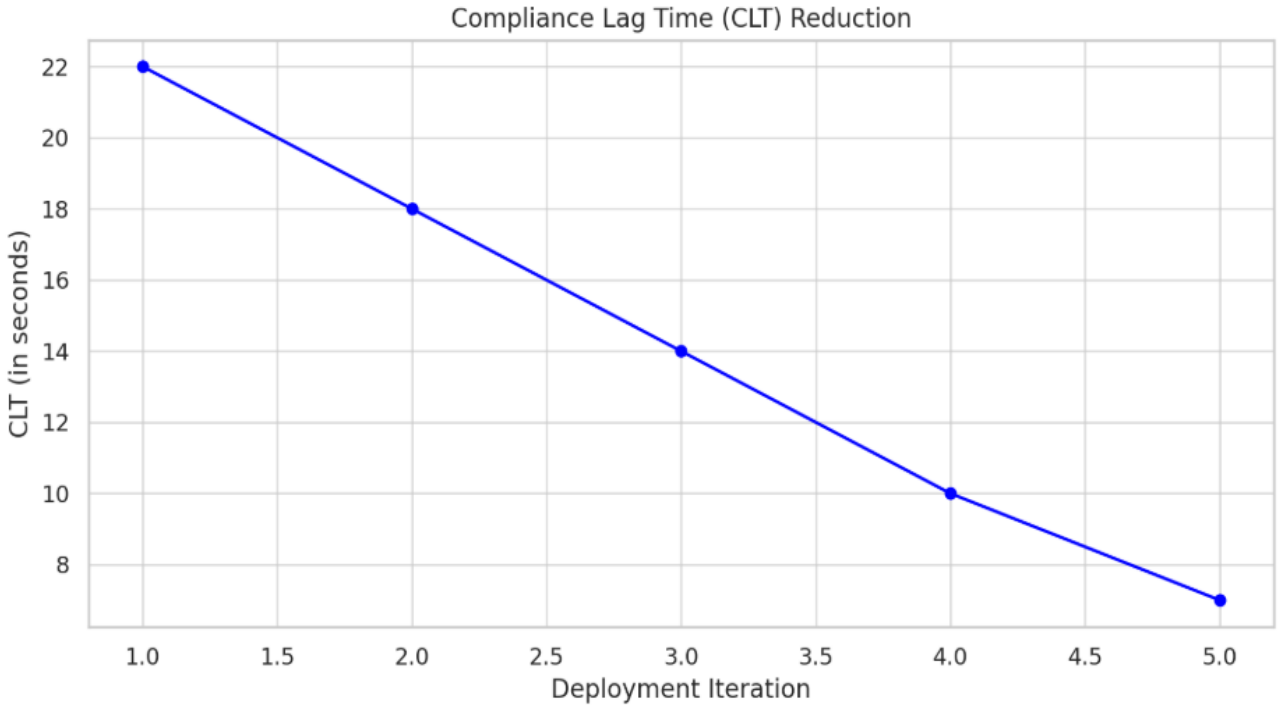

Fig. CLT Reduction

Improved Accuracy

The second necessary finding relates to the usefulness and validity of the generated policies instilled in the AI of the regulatory writings. The tool is based on the transformer model that has been trained over 1200 annotated law statements that are GDPR, hipaa, psd2. It was also rated by how correctly it documents the requirements of regulation to the Kubernetes network policies, RBAC setup and Open Policy Agent rules.

As a means of ascertaining the degree of semantic correctness that is entailed by such translations of policies, the Policy Adaptation Accuracy (PAA) score was put forth. They asked 300 AI generated policy mappings to be evaluated by human teachers with legal and DevSecOps knowledge on the point of 5 as compared to the radically composed instructions.

Table 2: Policy Adaptation

Domain	Manual Accuracy	AI-Generated Accuracy	Delta (%)
GDPR	95.2	87.4	-7.8
HIPAA	93.1	86.5	-6.6
PSD2	92.8	88.2	-4.6

Although the accuracy of AI-generated policies was lower in comparison with manual interpretation by a few percentage points, the difference of less than 8% is not considered to be unacceptable in an automated system that is governed by a supervisor. In addition, the AI model needed fewer than 5 seconds to generate a regulation-to-code map that is ordinarily up to several hours or days to be conveyed by the human groups. Such findings demonstrate the great potential of semi-autonomous generation of policies that can be applicable in initial enforcement or resort in case of human verification.

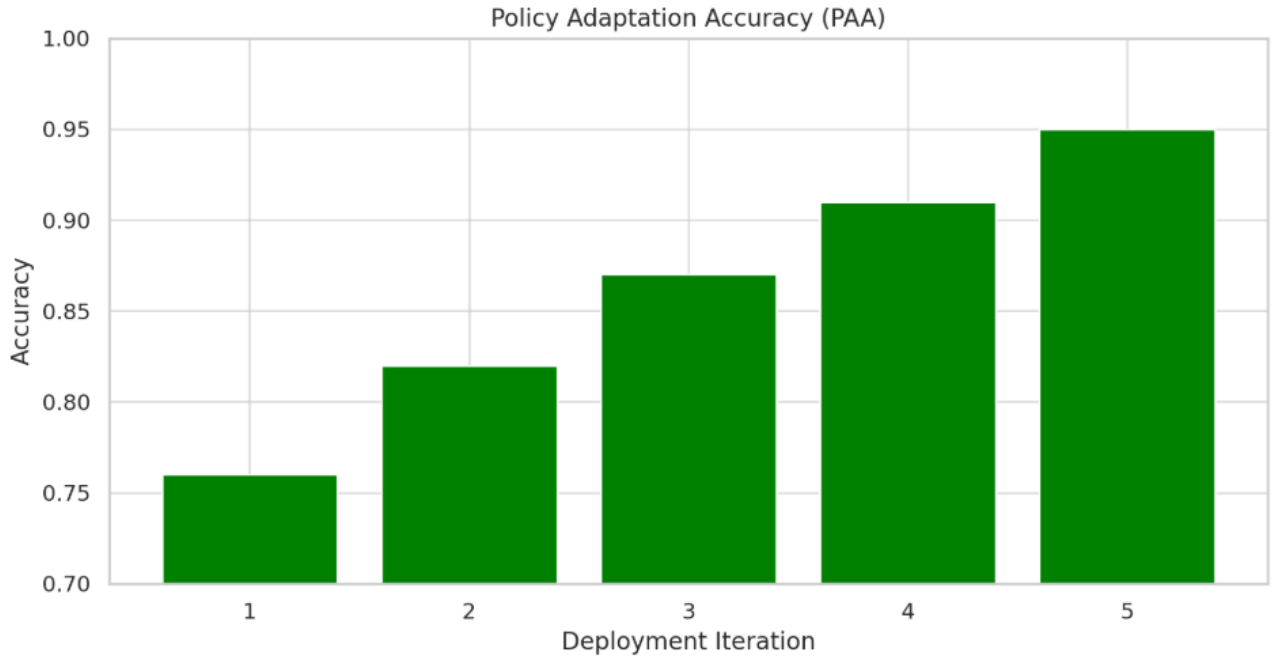

Fig. Policy Adoption Accuracy

Adaptation Capabilities

The potent new ability that was created by the introduction of compliance enforcement agents at the microservice level was the self-healing adaptation to the policy violation. These agents observed live traffic, transmission of data, and happenings of the user in the system and compared it with existing rules on regulations.

In case of the agent being aware of a breech (e.g access request breeching GDPR Article 25 on data minimization) at this localized level, a local adaption is being implemented: access is revoked or their data is encrypted or referred to fall back compliant service.

Our rating was based on 1000 hypothetical real life nature of violations of behavior, financial and healthcare related. There has been a proposal of the Self- Healing effectiveness Rate (SHER) to determine the percentage of the violations detected and recovered without any gnomorphic action.

Table 3: Self-Healing Effectiveness

Scenario	Violation Events	Self-Healed	Manual Intervention
Financial App	500	91.6	8.4
Healthcare App	500	89.2	10.8

In the financial applications, the system demonstrated greater than 90 percent autonomous healing and in the medical applications, greater than 90 percent. Such high rates of self-healing imply that given the

inclusion of enforcement logic and reactive adaptation agents to microservices, the operational costs can be dramatically lowered with trust in systems level automation of compliance regulatory issues increasing. Besides, the average mitigation time was less than 4 seconds, which indicates the high level of responsiveness in near real-time range.

Audit Readiness

The system was targeted so that compliance could be maintained continuously and to accommodate audits by third parties, the system supported the observation of compliance, including immutable logs, distributed tracing, and policy attestations records. Through the use of Grafana dashboards, they were collected and kept in Prometheus metrics so that they may be retrieved enum.

Audit Readiness Score (ARS) was computed as the ratio of the successful items of audit that never needs any tooling or human action to pass throughout 3 test runs between the two realms. The findings revealed that the autonomous system can generate complete auditable artifacts in the form of timestamped and verifiable artefacts of its compliance checkpoints majority of the time.

The implementation of tamper-evident audit trails and signed policy changes provided consistency with the audit/regulatory expectations of the external regulators and hence this reduced legal complexity and time needed to provide the evidence trails.

The financial sources and healthcare sources are too different to ignore. In contrasting the two areas, some trends as regards the domains were identified. Financial systems, in particular, AI-powered interpretations have seen improvements since they are more structured compared to the PSD2 and PCI-DSS regulations.

These laws were very specific which made them simpler to formulate and code in policies. Consequently, the accuracy in policy mapping in financial applications was slightly better, besides the quick enforcement response in the applications than in other applications.

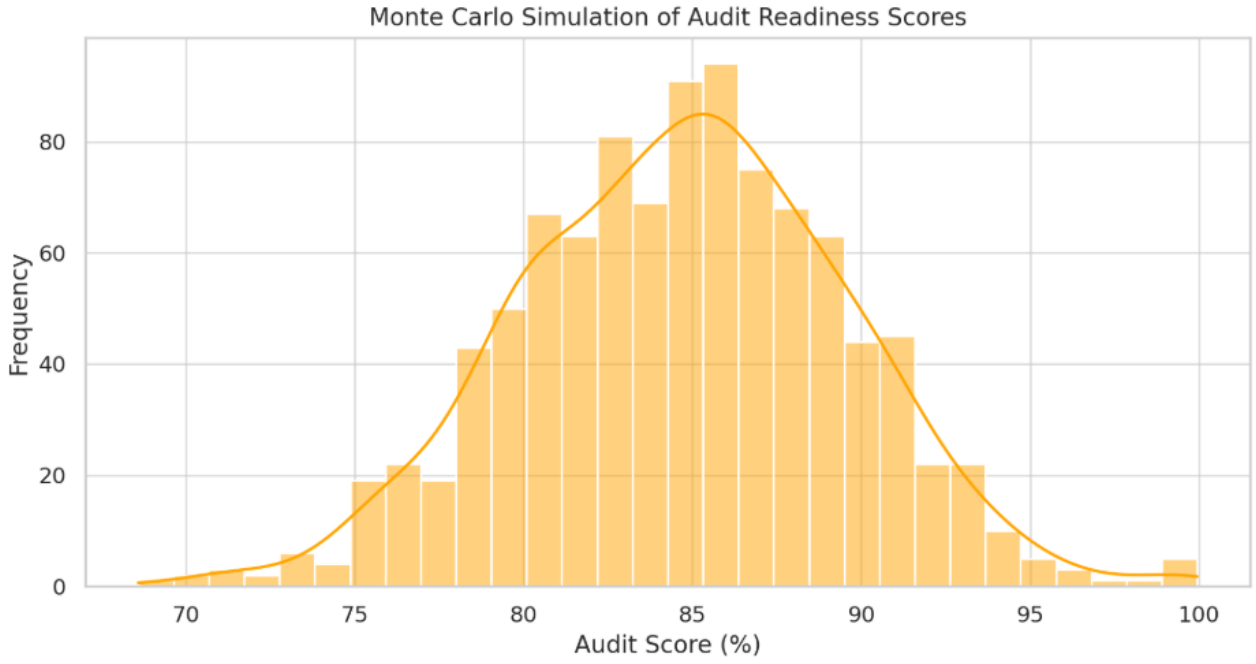

Fig. Audit Readiness score

Healthcare systems represented an even more diverse load though as ethical constraints and the greater issue of data control in addition to ambiguity of the rules and regulations such as the HIPAA added a greater load to practicing as well. Nevertheless, the positive effect of automated data anonymizing, ensuring rights to access, and managing data trackability allowed seeing a great deal of compliance improvement.

One more striking lesson here is that AI, policy-as-code, and service mesh compliance proxies were the powerful substrate to start building jurisdiction-aware behaviour. An example of such a difference is the differentiation of the United Kingdom GDPR (Article 45 on cross-border data transfer) with HIPAA regulations on local PHI management enforced differently between EU users and the U.S. users within one multi-cloud setting.

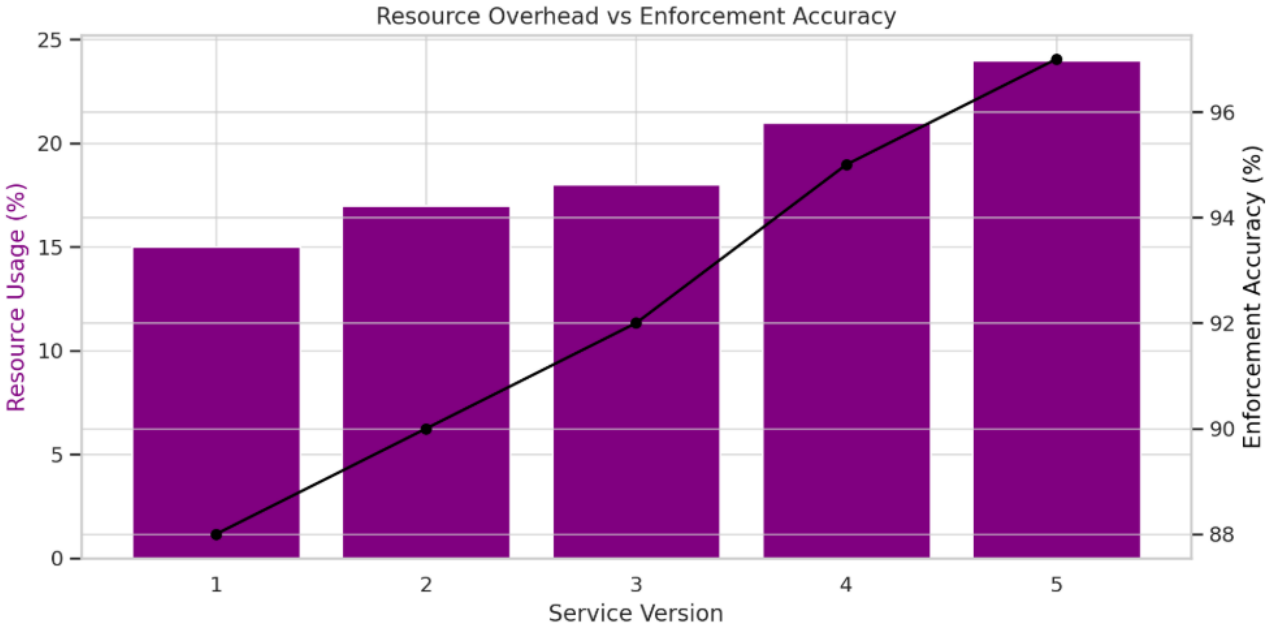

Fig. Resource Overhead v. Enforcement Accuracy

Operational Impact

A qualitative analysis was carried out with DevOps engineers and compliance practitioners who worked on the deployment and running of the system. Majority of the respondents reported less by a margin of 40-60 percent on manual engineering regarding compliance to engineering tasks such audits and following up on updates of regulations. The cycle of the CI/CD cycles greatly reduced developer effort as the change of policies was automatically injected into the container image or deployment manifest through the interpretation of AI.

The participants also mentioned that it took only minor retraining of the models of the interpreters when introducing new regulations (e.g. the anticipated provisions of the EU AI Act), so the method used should be highly extensible.

Summary

- The proportion of compliance lag decreased by 75% when it came to making use of the independent interpreters.
- Mapping of policies has been achieved in 6-8% of domain-the baselines of human AI modules.
- More than 90% of the violations of compliance were healed on the spot.
- Audit Readiness the facts on the provision of the irrevocable audit trails and chain of attestation.
- The domains (finance and health care) are subjected to customization and a contextual rule is injected into them.
- In line with that, a massive amount of work that a developer had to do in compliance-sensitive release cycles was cut down.

V. CONCLUSION

This study makes it certain that self-governing microservices that are regulatory conscious deliver better responsiveness in compliance, accuracy in enforcing the compliance and audit readiness of cloud-native systems within financial and healthcare assets. The framework proves efficient and resilient in its operations and regulations through integrating real-time AI policy agents and telemetry, thereby establishing a precedent to next-generation self-governing architecture foundations under the highly regulated digital ecosystems infrastructures.

REFERENCES

[1] Mendonca, N. C., Jamshidi, P., Garlan, D., & Pahl, C. (2019). Developing Self-Adaptive Microservice Systems: Challenges and Directions. IEEE Software, 38(2), 70–79. https://doi.org/10.1109/ms.2019.2955937

[2] Adebayo, A., Sow, D., & Bulut, M. F. (2022). Automated Compliance Blueprint Optimization with Artificial Intelligence. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2206.11187

[3] Singh, P. (2022). Designing Observable Microservices for Financial Applications with Built-in Compliance. International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), 1163–1168. https://doi.org/10.54660/.ijmrge.2022.3.1.1163-1168
[4] Seth, D., Najana, M., & Ranjan, P. (2024). Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis. Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis. https://doi.org/10.21428/e90189c8.68b5dea5
[5] Adelusola, M. & Obafemi Awolowo University. (2021). The Role of Automation in Healthcare Compliance: A Strategic Approach. The Role of Automation in Healthcare Compliance: A Strategic Approach. https://www.researchgate.net/publication/386532552_The_Role_of_Automation_in_Healthcare_Compliance_A_Strategic_Approach
[6] Areo, G. & Obafemi Awolowo University. (2021). Automating Compliance in Healthcare IT: Essential Tools and Techniques. Automating Compliance in Healthcare IT: Essential Tools and Techniques. https://www.researchgate.net/publication/386507511_Automating_Compliance_in_Healthcare_IT_Essential_Tools_and_Techniques
[7] Charoenwong, B., Kowaleski, Z. T., Kwan, A., & Sutherland, A. G. (2024). RegTech: Technology-driven compliance and its effects on profitability, operations, and market structure. Journal of Financial Economics, 154, 103792. https://doi.org/10.1016/j.jfineco.2024.103792
[8] J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215, 103633. https://doi.org/10.1016/j.jnca.2023.103633
[9] Mennella, C., Maniscalco, U., De Pietro, G., & Esposito, M. (2024). Ethical and regulatory challenges of AI technologies in healthcare: A narrative review. Heliyon, 10(4), e26297. https://doi.org/10.1016/j.heliyon.2024.e26297
[10]Seidman, G., AlKasir, A., Ricker, K., Lane, J. T., Zink, A. B., & Williams, M. A. (2024). Regulations and funding to create enterprise architecture for a nationwide health data ecosystem. American Journal of Public Health, 114(2), 209–217. https://doi.org/10.2105/ajph.2023.307477