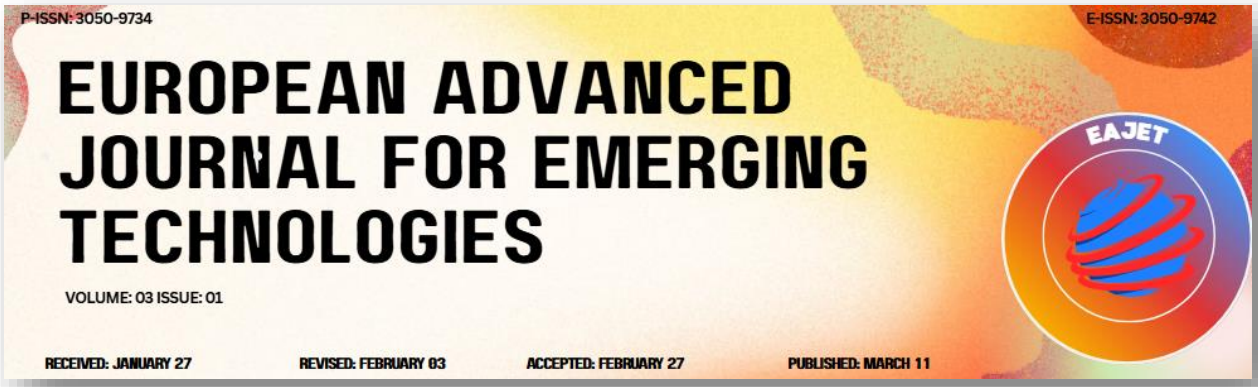


Observability Frameworks for Cloud-Native Healthcare Analytics

Dileep Valiki
Independent Researcher
valiki.dileep.researcher@gmail.com

Abstract

Cloud computing platforms for big data analytics, such as Amazon Web Services, Google Cloud Platform, or Microsoft Azure, have entered a mainstream growth phase, yet despite the enormous market demand, their effective operation remains a challenging task. Monitoring and observability of big data workloads needing support for dynamic and complex infrastructure represent an important area of research. Healthcare analytics platforms are particularly demanding in this respect, as workloads are commonly performing computations over patient data, which introduces additional requirements. During the last few years, several frameworks have been proposed to address various observability needs for cloud-based platforms, yet information on those approaches remains scattered. This survey work provides a structured overview of definitions, architectural patterns, frameworks, and tools, along with special focus on healthcare observability requirements. Furthermore, the discussion identifies potential areas for future investigation.

The cloud observability area is still evolving, making it necessary to review the state-of-the-art, identify gaps, and propose a research agenda. Foundation work covers an analysis of core concepts and architectural patterns for big data observability in the cloud, followed by the examination of requirements driven by healthcare workloads. These aspects have laid the groundwork for a survey of existing observability frameworks and tools tailored to cloud platforms, with special emphasis placed on monitoring telemetry collection, distributed tracing, and performance management. Finally, additional data management considerations are discussed before the identification of architectural patterns that address the specific observability demands from healthcare data processing workloads.

Keywords : Data observability; Healthcare analytics; Cloud architecture; Data provenance; Distributed tracing; Multi-cloud; Hybrid cloud; Streaming data.

1. Introduction

Cloud-based Healthcare Analytics Platforms: Observability and Governance As the global healthcare ecosystem embraces digital transformation, cloud-based platforms promise new levels of efficiency, accessibility, and scalability. However, maintaining confidence in these evolving infrastructures depends on observability—the ability to understand a continuously changing system. This requires rich telemetry covering performance, security, compliance, and operational clarity. In healthcare, special attention must also be paid to lineage, provenance, and the ability to respond to requests from patients, regulators, and researchers. As visualizations are critical for engaging non-technical stakeholders and are heavily exploited within the healthcare domain, special attention should be paid to observability dashboarding.

In recent years, a great deal of research has emerged around observability pipelines and how they might be constructed or used in a vendor-neutral manner. Major public cloud providers also offer extensive sets of proprietary services

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

that address observability needs natively. However, healthcare analytics workloads present their own unique observability requirements, raising questions around how patented solutions can be adapted in a vendor-neutral manner to support these workloads.

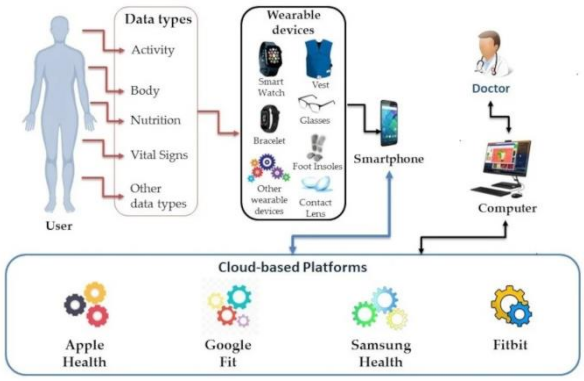


Fig 1: Cloud-Based Platforms for Health Monitoring

1.1. Background and Significance

Cloud-based observability frameworks that address telemetry for data provenance, tracing, and compliance requirements are underexplored in existing literature. Observability in healthcare analytics platforms is of particular interest because of the increasing amount of sensitive data handled by healthcare organizations and the stringent regulations enforcing data privacy. The study fills these gaps by addressing four questions: What are the data-relevant observability requirements for healthcare analytics workloads? Which data provenance, telemetry, and tracing capabilities should observability frameworks provide? Which cloud-native frameworks and techniques are mature enough to address healthcare-oriented observations? Which techniques are emerging and what cloud-agnostic alternatives are available? The contributions include a definition of observability, an identification of the-volume-sensitive metrics, telemetry, traces, and events relevant to healthcare workloads, a discussion of patient data privacy and compliant sharing, an evaluation of telemetry collection, distributed tracing, and performance monitoring techniques in the context of healthcare workloads, and an outline of considerations for multi-cloud deployment.

Equation 1: Observability as "infer internal state from telemetry"

Step 1 (define state and outputs)

- Hidden/internal system state: $x(t)$(queues, saturation, failure modes)
- Observable telemetry: $y(t)$(metrics/logs/traces)

Step 2 (write system + measurement equations)

$$x(t+1) = Ax(t) + Bu(t)$$
$$y(t) = Cx(t) + v(t)$$

Step 3 (define observability matrix)

$$\mathcal{O} = \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix}$$

Step 4 (observability condition)

$\text{rank}(\mathcal{O}) = n \Rightarrow x(t)$ can be reconstructed from $y(t)$

1.2. Research design

The design comprises three distinct elements: scope, analysis, and data. Scope identifies cloud platforms as the focus, while analysis extracts observability requirements from the lineage, telemetry, and event models of healthcare workloads. Healthcare workloads, derived from clinical and analytics use cases, provide the basis for observability requirements. Achieving a resilient health observability structure in cloud platforms facilitates security governance and regulatory readiness. Supporting infrastructure is provided by event-driven data pipelines that connect sources

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

of events, traces, and metrics. Telemetry requirements are informed by the data flow models of workloads and pipelines.

Healthcare platforms are composed of numerous services, often developed at different times and by different teams. The telemetry requirements of these systems are monitored and expanded, producing different formats and schemas. Telemetry pipelines read and transform these data streams, ensuring that they adhere to a common schema suitable for analysis and long-term storage. Potential schema evolution is also considered, identifying strategies to accommodate changes in telemetry sources while ensuring normalization processes remain functional. Healthcare data management is continuously evolving as the need for efficient observability increases. Telecommunications monitoring within cloud platforms should focus on the minimization of sensitive patient information while providing the necessary insights into potential breaches and failings.

2. Foundations of Cloud-Based Big Data Observability

Definitions of key concepts—observability, telemetry, metrics, traces, logs, events, dashboards—provide the foundation for an analysis of architectural patterns enabling observability in the cloud. Specifically, the suitability of monolithic, microservices-based, and data-centric architectural styles for cloud-based observability is assessed.

2.1. Definitions and core concepts

Data lineage and data provenance are distinct but closely related concepts. Lineage encompasses the flow and transformation of data, while provenance seeks to describe the origins of data and the process by which it has been generated. Both concepts have received renewed attention due to the increasing value placed on the integrity of data used in decision-making processes. Data lineage is an important factor for reproducibility, enabling external researchers to verify results using the same datasets and computational processes. The process of making the data available and completely describing the provenance of the results can take considerable time and effort and often relies on a dedicated team. In addition to satisfying the need for reproducibility, lineage models are now also required for auditability and regulatory compliance. Auditing and governing the data subjugate the operation of the public cloud platform and force additional requirements on the infrastructure and data observability pipelines.

The reference datasets provided, for example, through the quality-controlled public repositories of NIST for key image classification tasks represent only a small portion of the methods used in real-world data science workloads. The aggregation of hundreds or even thousands of datasets together with the respective transformation and processing pipelines is simply unfeasible from an operational point of view, even in cases where a team is dedicated to implement them. In practice, data discovery and data access for reproducibility are much sought-after at the expense of full reproducibility. The reducing of the effort required through observability is pivotal in satisfying these requirements; however, it must be balanced against real operational risk. When sensitive data are handled, side step risks still remain. Therefore, a continuum approach to lineage may be adopted, whereby for certain classes of experiments more effort is invested to achieve higher levels of data discovery, access oversight, and even full reproducibility as workload bounding provides the level of risk needed.

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27
REVISED: FEBRUARY 03
ACCEPTED: FEBRUARY 27
PUBLISHED: MARCH 11

Fig 2: Data Quality with Data Observability

2.1. Definitions and core concepts

A data lineage model describes the life cycle of data, answering important information and supporting data governance—key aspects of auditability and compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Lineage models therefore define the relevant points of capture, the type of metadata to collect and store for each point, and the information to supply users in order to guarantee the reproducibility of results, one of the core principles of the research process.

Because medical research often involves processing large amounts of personal health information and patient data, preserving the ability to audit the flow of PHI through the observability architecture, as well as regulatory compliance with industry standards, must be a priority for any observability implementation. An important aspect of supporting auditing, regulatory compliance, and reproducibility is the ability to track the source of the data, its transformations, aggregation points, and consumption. In the health care sector, lineage models from the data observability architecture must be able to prove the correct use of the data and support due diligence regarding regulatory requirements.

Data observability in clinical analytics workloads must provide visibility into all patient data processing and sharing through the cloud. The data observability architecture must track all shares of PHI from patient care workflows across provider data-evaluation pipelines and machine learning pipelines, incorporating lineage and provenance tracing, event tagging, and alerting capabilities.

Equation 2: Telemetry/event volume (why the paper warns about scale)

Step 1 (per-source telemetry rate)
Let source $i$emit $\lambda_i$messages/second.

Step 2 (total ingestion rate)

$$\Lambda = \sum_{i=1}^{N} \lambda_i$$

Step 3 (storage sizing over retention T)
If average message size is Sbytes:

$$\text{Storage} = \Lambda \cdot S \cdot T$$

2.2. Architectural patterns for observability in the cloud

Cloud-based observability can be implemented using different architectural patterns. Event-driven architectures make it easy to automatically detect, track, and connect related operation traces, but care should be taken with the volume of event messages generated. Telemetry data can be obtained using a push or pull model; the push model tends to be preferred since it avoids the need for an explicit pull for every sample collection. Using a sidecar proxy or service mesh pattern can simplify the injection of monitoring probes but introduces overhead in the processing of any service request. Monolithic architectures are easier to manage and less tolerant to failure, while microservices and data-centric patterns scale better and can mask any failure.

Event-driven architectures provide a natural fit for supporting observability in the cloud. In this type of pattern, components of a system can communicate as events occur, including notifications for key actions undertaken by one component of the system. As more components are added to a system, so does the number of event sources that will be generating notifications. Having an event-driven pattern in place allows other components to subscribe to notifications and, in turn, being notified of system actions. All of this enables a more automatic detection and tracing system for cross-component signals.

Another architectural consideration for telemetry is whether checks are undertaken in a pull or push model. In the pull model, the telemetry service explicitly requests a check from each monitored component. In the push model, the telemetry service simply provides a channel for capture and each of the

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

monitored components send data updates to the telemetry service as and when they wish or in accordance with defined frequencies. The latter model is often preferred, as it makes the entire telemetry architecture much simpler.

3. Observability Requirements in Healthcare Analytics

Healthcare analytics services rely on a multitude of data sources and compute platforms, often belonging to different organizations. Consequently, patient-centric analytics workflows span across multiple, sometimes heterogeneous environments, introduce large amounts of telemetry data that may lead to increased observability challenges. Two key areas of observability in healthcare analytics are data lineage and event-driven tracing. Supporting both areas can help reduce downstream analytic application rewrites and ease traditional performance monitoring through telemetry telemetry and insight sharing across platform borders. Such increasingly easy data exchange, however, needs to be coupled with patient data privacy protection and compliance with related regulations.

Data provenance can help track healthcare-related observations, minimize privacy exposure of sensitive patient data, and optimize transpose-replace data management strategies when distribution patterns through analytics pipelines change over time. In a similar spirit, event-driven tracing can complement traditional telemetry-based performance monitoring for healthcare workloads.

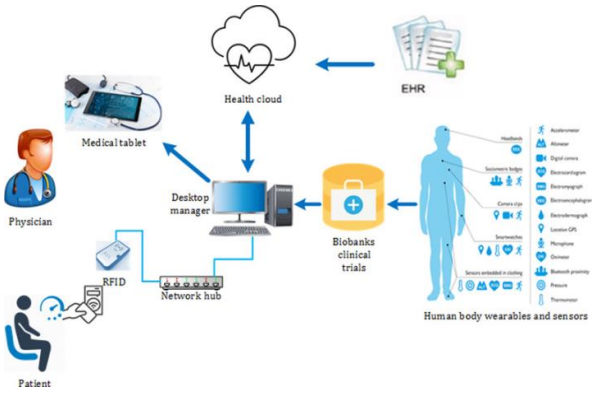
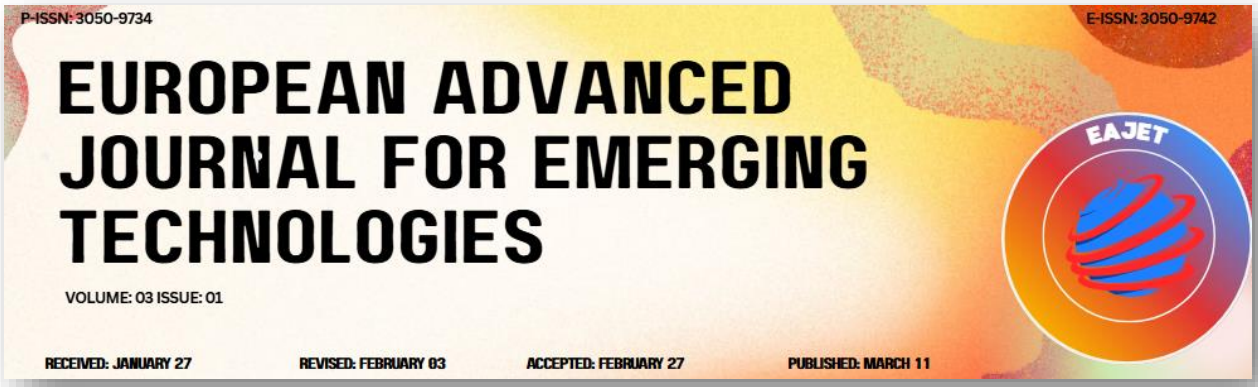


Fig 3: Observability Requirements in Healthcare Analytics

3.1. Data lineage and provenance

Data provenance, or lineage, concerns the lifecycle of data, answering where data comes from, who has modified it, and in what manner. It conveys the history of a data item from its creation until its most recent query. Two forms of data provenance can be identified: operation-level and tuple-level. Operation-level provenance holds information about the entities involved in an operation, accounting for transformations, although not explicitly capturing the state of the data. Tuple-level provenance identifies the sets of tuples that have influenced the outcome of a specific query tuple, effectively enabling filtering. Provenance can also be understood as a derivative of causality based primarily on the understanding of DBMS operations. It emerges naturally in the context of data integration and warehousing, analytical frameworks for making historically archived data available for complex processing, and monitoring frameworks that exploit the semantics of data exchanges to detect deviations.

Along with being critical for assuring compliance with legislation such as the HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA), data provenance significantly facilitates data management tools for data cleaning, quality checking, display, reuse, control, and auditing. It constitutes an



important aspect of the observability ecosystem for healthcare workloads running on cloud platforms. Confirming that data observability and management are intertwined, data-quality concerns are often associated with missing, stale, or incorrect provenance information. However, although processes connecting different data entities across various systems and protocols represent a major use case for research in data provenance, the structures and concepts proposed may not directly apply to data-intensive processes monitoring health data. The notion of data-channel blocks captures the concept of data transport channel end-to-end in a way that allows assuring distinct degrees of privacy and sensitivity filtering on transparent output vaids down these channels without revealing originally protected data.

Equation 3: Push vs pull telemetry collection (message overhead)

Step 1 (assume sampling rate)
Each of Nservices sampled at $f$samples/second.

Step 2 (pull model message count)
Each sample requires request + response:

$$M_{\text{pull}} = 2Nf$$

Step 3 (push model message count)
Each sample is one pushed update:

$$M_{\text{push}} = Nf$$

Step 4 (compare)

$$\frac{M_{\text{pull}}}{M_{\text{push}}} = 2$$

3.2. Event-driven tracing and telemetry in healthcare workloads

Event-based monitoring conveys optional additional information regarding system activity, reflecting underlying workload characteristics. Telemetry associated with such events may arise in different forms, being collected either during their occurrence or at their completion. Furthermore, user-specified workloads can impose their own telemetry patterns on the operational environment. Specific event tracing and telemetry generation can be facilitated by the inherent architectonic nature of both Google Cloud and Azure cloud environments, which predominantly rely on synchronous event-driven components.

Hardware usage traces and performance telemetry can be automatically collected in some of the core cloud elements. In particular, the underlying cloud virtualization layers offer such features and associated telemetry collection and display. Their openness can permit automated tracing and collection of selected workload execution related data across systems. However, additional workload specific metrics or indicators may need to be incorporated in the monitoring specific cloud components used by clients. Optionally, client agencies may specify their semantics and designate additional user processes or applications (e.g. using Cloud Run, Containers) that need similar tracing and monitoring specific processing.

Alternative cloud usages observing a hybrid strategy can explicitly indicate whether any workload segments should remain unmonitored. Workload-specific custom telemetry conveyance can also be included in such tracing operations that make evident new workload process or application state classifications or semantic ranges. Tracing export features integrated in some cloud-based products (e.g. Cloud SQL) or made possible through wrapper services for others (e.g. App Engine User or Background workload segmentation) enable telemetry capture during both the operational phases.

4. Observability Frameworks and Tooling for Cloud Platforms

Setting up observability for complex workloads in the cloud is a daunting task from processing and tooling perspectives. The first major requirement emerges from the discipline of

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27
REVISED: FEBRUARY 03
ACCEPTED: FEBRUARY 27
PUBLISHED: MARCH 11

telemetry collection and normalization across multiple computing resources. Dedicated tools ease this task on major cloud platforms, but requirements change across industries as well as sometimes call for combinations of cloud resources with on-premises or with other providers' resources. The main sources of telemetry are virtual machines where division of compute and control planes is a key operating principle, even more visible when combining containers, serverless and edge computing. The second major requirement is performance monitoring, and especially the generation of metrics from application code through a mechanism often called distributed tracing. While each cloud provider supports such tracing by adapting frameworks such as OpenTracing to their platform, tools able to couple monitoring of different services remain scarce. Application stacks that implement an event-driven architecture may benefit from tracing all relevant services with a telemetry collection distribution that is naturally layered into three levels.

Telemetry collection and normalization are tedious tasks. Cloud providers ease the challenge by delivering observability services capable of collecting metrics, logs and traces from virtually any resource in the platform, and usually also from on-premises resources through an on-premises agent. These central services are normally complemented by resource-specific services capable of monitoring telemetry for several different resource types. While cloud providers seldom supply external third-party integration using proprietary vendors with no support, these central services are nonetheless capable of incorporating their results to the platform in a seamless way. Such development allows the design of a cross-cloud observability solution that is entirely cloud-agnostic, capable of augmenting telemetry from services in multiple cloud providers.

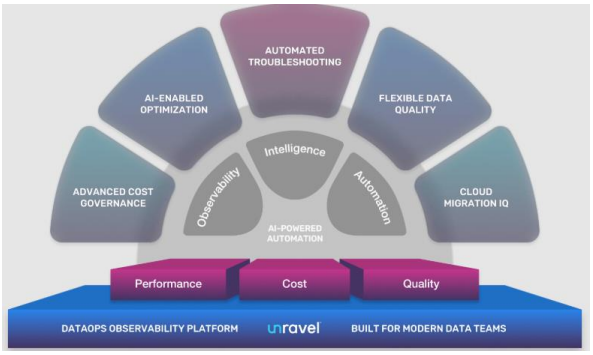


Fig 4: Tooling for Cloud Platforms of Cloud-Based Big Data

4.1. Telemetry collection and normalization

Modern cloud platforms provide a plethora of monitoring and observability tools. However, gaps remain in the overall observability picture, particularly in the connection and interrelation of the different domains, and in the metadata behind the observability data itself. Hyperscalers, infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) offerings deliver a large set of telemetry data collection and analysis features for the supporting infrastructure and platform services, allowing the customers to concentrate on their workloads; the ultimate success or failure for a specific cloud service is tied to the quality and performance of the workloads running on it. Nevertheless, not all monitoring and observability services are provided by the cloud vendor itself; most specialized and custom tooling detects and collects telemetry data on its own.

A significant part of observability relies upon application-level visibility, both for detecting issues in live environments and for providing an adequate response to service-level agreements (SLAs) and service-level objectives (SLOs) provisioning. Components for application performance management (APM) and others specialized in distributed transaction-tracing are typically supplied by different vendors. Such tooling is traditionally considered external to the main cloud service and provides a look into the

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

workloads at an application level. Although the collected telemetry data is typically not retained in the service offering for any other purpose than supporting those particular products or their interoperability, besides in some cases having a telemetry export to the cloud vendor main observability platform, standardization and normalization of the data nevertheless make it valuable for another type of inquiry and validation of the overall platform.

Equation 4: Distributed tracing and performance monitoring (latency decomposition)

Step 1 (trace is a chain of spans)
A request trace has spans $k = 1..K$.

Step 2 (span latency split)

$$L_k = S_k + N_k$$

- S_k: service/compute time
- N_k: network + queue/wait time

Step 3 (end-to-end latency)

$$L_{\text{total}} = \sum_{k=1}^{K} L_k$$

4.2. Distributed tracing and performance monitoring
Observability tooling for distributed tracing and performance monitoring has matured, largely driven by the proliferation of microservices architectures running in production at scale. Both AWS and Azure now provide tailored observability services for these workloads that can be used out of the box with minimal configuration. Open-source alternatives such as Jaeger and Zipkin run in Kubernetes clusters and can aggregate data from applications running across different clouds. Locally hosted services such as eBPF and OpenTelemetry also support instrumentation for tracing, monitoring, profiling, and security, particularly for containerized workloads.

Despite their prominence in public cloud environments, distributed tracing and performance monitoring services are less widely adopted in cloud workloads outside of Internet-facing sites. Much of this gap can be attributed to regulatory concerns in the finance and healthcare sectors. Such workloads often center around batch-oriented job processing of sensitive data, resulting in enterprise information systems that echo corporate silos rather than the independently deployable and scalable microservices of social media. Nonetheless, there is increasing interest in distributed tracing for machine learning workloads as training jobs shift from single clusters to spans across different infrastructures.

5. Data Management Considerations in Healthcare Observability

An often-overlooked aspect of observability is data management. From a practical standpoint, most patient-related data is subject to country-specific privacy laws that require patients' consent before their data can be shared with third parties. Moreover, the transformation of unstructured clinical notes into usable datasets requires considerable processing of sensitive data that is, moreover, rarely used during the execution of complex analytic workloads. Data-minimization and access-control measures can therefore add significant value and improve the overall efficiency of healthcare analytics without violating legal requirements.

Privacy-preserving access controls artifacting observability signals from complex workloads also reduce the volume of sensitive information shared. For example, dermatology-focused studies often require vast amounts of high-resolution images of skin lesions. Such images rarely appear in subquery join results, yet standard observability practices still require their collection and transit over the network. Access controls ensures only authorized, compliant, and semantically relevant images are included in observability signals, allowing associated processing costs to be avoided. A connected set of solutions minimizes divided-data, exfiltration, and profilsing exposure risks while also

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

lowering the network footprint and computing requirements associated with data sharing, enabling a compliant monitoring strategy.

Equation 5: Data lineage & provenance (operation-level vs tuple-level)

Step 1 (model lineage as a graph)
Lineage/provenance as DAG $G = (V, E)$:

- V: artifacts (tables/files/models)
- E: transformations (ETL/jobs/queries)

Step 2 (operation-level provenance)

$$Prov_{op}(op) = \{inputs, outputs, actor, time, parameters\}$$

Step 3 (tuple-level provenance)
For an output tuple t_{out}:

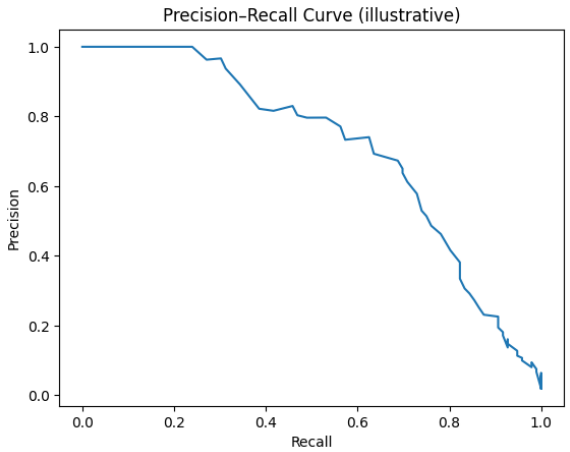
$$Prov_{tuple}(t_{out}) = \{t_{in} \mid t_{in} \text{ influences } t_{out}\}$$

Step 4 (standard formalism: provenance semiring)

- Join → multiplication (AND)
- Union → addition (OR)
  Example expression: $(a_1 a_2) + a_3$

5.1. Patient data privacy and compliant data sharing
A major concern in healthcare analytics is the privacy and protection of patient data. However, some workloads may require the sharing and aggregation of private data across institutions. Therefore, data-sharing concerns should not be viewed as a hindrance to observability in healthcare workloads. Data minimization processes permit the access and sharing of specific attributes of the patient data while removing or obscuring all other aspects of sensitive patient information. Compliant data-sharing services allow public health organizations to request patient data from patients' organizations, through an auditable workflow. Data may be disclosed based on the presence or absence of specific keywords within the request. Such keywords are mapped to data attributes in patient data, to trigger the processing.

Observability methods must consider these aspects and be context-aware when supporting the execution of such workloads. Access-control mechanisms align with patient data privacy by exposing and sharing a minimum amount of sensitive data required for the completion of each specific workload. Data-processing patterns should also reflect compliance aspects; although real-time processing is advantageous, batch processing is typically a better fit for patient data.



5.2. Rationale for data minimization and access controls
Cloud platforms simplify dissemination of substantial datasets, but adopting an ethical approach is crucial for compliance with data privacy regulations (such as HIPAA and GDPR) when handling sensitive information, such as electronic health records (EHRs). A recommended method for sanctioned data access is through data minimization where only the subset of information on individual patients, or groups of patients sharing comparable characteristics (preventing patient re-identification), must be shared with analytics jobs as inputs. This rules out exposing the bulk of

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

sensitive information, even in de-identified snapshots, to a community of data analysts or machine learning engineers. Besides data minimization, it is also important to follow the principle of need-to-know, so sensitive information about a particular patient or those of a defined subgroup is accessible only to data analysts or machine learning engineers required to use that information.

Theory does not always translate to practice, as vulnerability assessments often reveal service accounts or clusters with access to everything in the EHR. Data minimization can be automated by leveraging technical controls available on modern cloud storage services. For built-in data-exposure controls, event-driven tracing can be utilized, as discussed with telemetry.

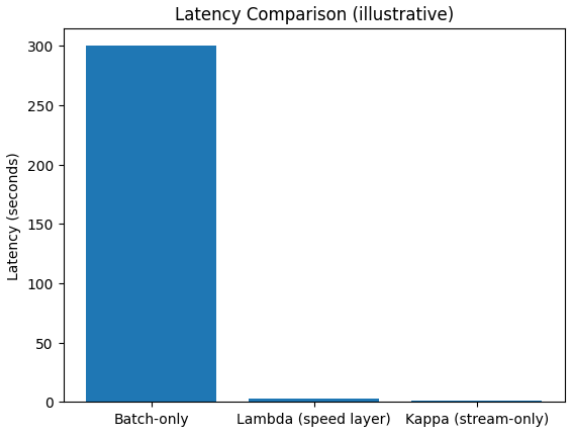
6. Architectural Patterns for Cloud-Based Observability in Healthcare

For fully cloud-based solutions, the observability framework should follow the multi-cloud architecture concept. Multi-cloud strategies enable customers to distribute workloads across several cloud providers, preventing vendor lock-in and making it easier to satisfy geographical data storage concerns. Cloud providers use a variety of billing strategies and service offerings, and thus, workload placement decisions depend on complex cost structures. In particular, raw storage pricing differs significantly from one provider to another, making separate providers attractive for archiving large amounts of rarely accessed data.

Nevertheless, while all customer applications may use different clouds to minimize costs, some workloads, such as those involving patient interaction and centralized control, are better placed on a single provider—typically that company's main cloud. To avoid latency penalties, provisioning between the main provider and others involves using maximum-based autoscaling at the main provider when the other providers have a low latency, and minimum-based autoscaling at the other providers.

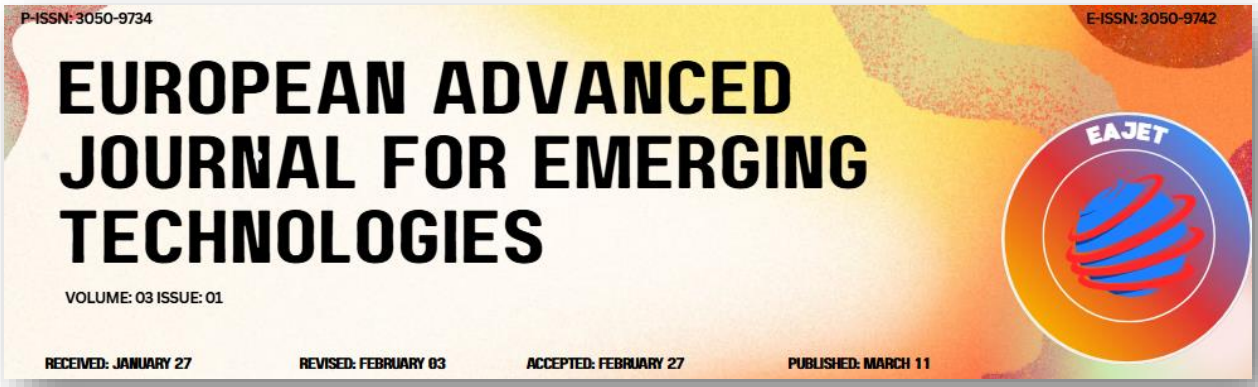
The hospital's devices typically produce relatively small amounts of less critical data that are sent to the same provider as the rest of the patient's main workloads so that telemetry forwarding costs are minimized. In contrast, telemetry produced from the fulfilment of the contracts is published to all clouds, allowing centralized monitoring across all patient workloads, which can be useful for detecting secondary incidents that can have costly impacts. Finally, in this context, observability is mainly achieved through traditional data delivery and processing pipelines, although using lightweight data delivery protocols (such as gRPC) is necessary to avoid unduly impacting latency.

For hybrid-cloud solutions, where the majority of the workloads are managed on-premise, the observability framework should follow the streaming pattern instead of batch processing, allowing near real-time warnings about potential service-level agreement violations. The detection of proximity breaches relies on caching aggregated values of the last events received for the smallest cool-down periods of the telemetry destinations, delivering a value to the centralized monitoring when some other destination has a related cool-down period expiring.



6.1. Multi-cloud and hybrid strategies

Modern cloud computing clusters, supported by a global



fiber-optic data transfer network, facilitate the engineering of highly complex application workloads in the healthcare domain that rely on distributed technologies for nearly all operations. Sadek et al. provide insight into how the development of cloud offerings from multiple service providers has enabled organizations supporting sensitive medical data to deploy workloads across several cloud providers, thus creating a new paradigm referred to as multi-cloud. This multi-cloud approach provides many advantages such as routing internal data flows through nodes located in different jurisdictions according to the applicable privacy requirement for each data flow, and it enables performing workload segments on the infrastructure of the most competent provider.

Despite these advantages, the deployment of workloads in multiple clouds simultaneously creates new problems, particularly in terms of observability. Volume and quality of documentation are generally lower than for multi-tenancy scenarios. Updating processes for observability tooling and associated telemetry sources for newly deployed services or products is often missing. The traffic to be monitored concentrates on a specific provider, leading to lower amounts of source and destination IP addresses to detect outliers. An observability platform designed to support these scenarios helps cloud architects monitor the overall execution flow of an application without being limited by a single cloud provider.

6.2. Streaming analytics versus batch processing
Combining Cloud-Based Big Data Observatory Requirements with Multi-Cloud and Hybrid Cloud Strategies
Combining Cloud-Based Big Data Observatory Requirements with Multi-Cloud and Hybrid Cloud Strategies—part of streaming analytics versus batch-processing requirements

Combining cloud-based Big Data observatory requirements with multi-cloud and hybrid-cloud strategies requires an additional telemetry-monitoring summarization and visualization layer, primarily focused on patient-control observability/lineage of sensitive patient data and patient-related detections, events, and actions as well as on-the-move data. Such a layer allows using a mix of public-cloud geolocation functionalities and private-cloud control of sensitive data in a privacy-compliant way.

Due to the developing concept of sensitive data and the on-going severe data leaks, privacy issues have reached new prohibition- and control-related levels. Therefore, the minimization of sensitive patient data while keeping benefits remains important, even in patient data–sharing and patient-accessing-related solutions. From the data source through data transmission to data usage, these sensitive data are considered. From streaming analytics through batch or streamed for-holding monitoring to detections, telemetry collection, and visualization, the sensitivity of data needs to be minimized or handled in a privacy-compliant way.

7. Conclusion

In seeking to fill the gap in the distributed systems and cloud computing disciplines between observability and cloud-based big data analytics frameworks for healthcare, defined requirements for observability in healthcare analytics workloads were collected, existing cloud-based big data observability frameworks and tooling were considered, and potential solutions for data management questions were explored. These solutions state that healthcare workload observability must satisfy requirements for data lineage and provenance, event-driven telemetry and tracing, and patient data privacy and safety; that voltage-scaled telemetry workload collectors, such as OpenTelemetry and Amazon CloudWatch, are necessary components; that integrated distributed tracing and performance monitoring solutions, such as Google Cloud Trace, Amazon X-Ray, or OpenTelemetry, are essential; that cloud human resource monitoring must be enabled; that cloud provider data sharing must achieve compliance with sensitive patient data; and that effective least-privilege access control requires Mason’s core principle of databasis-conserving data minimization.

P-ISSN: 3050-9734
E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

The results confirm that cloud-based big data observability solutions for healthcare, including tooling or frameworks, fulfil requirements already established in the relevant scientific literature, both from a general perspective and with specific reference to cloud-based data management analysis and monitoring.

Architecture	Typical end-to-end latency (s)	Model refresh cadence (hrs)
Batch-only	300.0	24
Lambda (speed layer)	2.5	6
Kappa (stream-only)	1.2	6

Table: Illustrative architecture QoS table

7.1. Future Trends

Big Data observability in the cloud is a rich field of exploration, with many significant developments. Advanced open-source Cloud observability platforms—such as OpenTelemetry for telemetry, OpenTracing for distributed traces, and OpenLineage for data lineage—enable Open Source observability for applications hosted across multiple clusters and clouds, whether public, private, or hybrid. With novel architecture patterns, they eliminate blind spots in the telemetry collection and normalization phase, facilitate the generation of distributed traces and telemetry data for application components deployed across clusters in different clouds, and address Data Privacy regulation challenges in the Healthcare domain through data minimization and regulated data sharing.

Healthcare Analytics Platforms hosted in the cloud must monitor the entire Data Flow of their Analytics Workloads to provide appropriate Telemetry data and Distributed Traces for troubleshooting and performance tuning. Recent knowledge developments support the implementation of the three core observability concepts—Data Lineage and Provenance, Event-Driven-Telemetry Generation, and Patient Data Privacy—by means of Ad-hoc Patters and the adoption of Public Cloud Providers' offerings. Future Work will address additional aspects and the design of comprehensive Generative Learning patterns.

8. References

[1] Ahmad, S., & Al-Qutaish, R. E. (2022). Monitoring and observability in cloud-native microservices: A systematic mapping study. Journal of Cloud Computing, 11(1), 1–25.

[2] Al-Hashimi, M., Al-Sayyed, R., & Al-Shraideh, M. (2022). The impact of artificial intelligence on automating administrative and operational processes in healthcare. International Journal of Healthcare Technology and Management, 19(1/2), 45–60.

[3] Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2022). Cloud computing-induced digital transformation in healthcare: A review and future research directions. International Journal of Information Management, 65, 102502.

[4] Bhardwaj, A., & Gupta, K. (2022). AIOps for cloud-native healthcare platforms: Enhancing reliability through automated observability. IEEE Transactions on Cloud Computing, 10(4), 2150–2163.

[5] Ciecierski-Holmes, T., Singh, R., Axt, M., & Kozlakidis, Z. (2022). Artificial intelligence for strengthening healthcare systems in low- and

P-ISSN: 3050-9734 E-ISSN: 3050-9742
EUROPEAN ADVANCED JOURNAL FOR EMERGING TECHNOLOGIES
VOLUME: 03 ISSUE: 01
RECEIVED: JANUARY 27 REVISED: FEBRUARY 03 ACCEPTED: FEBRUARY 27 PUBLISHED: MARCH 11

middle-income countries: A systematic scoping review. npj Digital Medicine, 5(1), 162.

[6] Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2022). Big data in healthcare: Management, analysis and future prospects. Journal of Big Data, 9(1), 1–25.

[7] Florea, R., & Radu, L. D. (2022). AIOps: The future of IT operations in big data environments. Applied Sciences, 12(9), 4567.

[8] Galety, M. G., Sagayam, K. M., & Abraham, A. (2022). Predictive monitoring in healthcare systems using AIOps and machine learning. Health and Technology, 12(4), 789–801.

[9] Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2022). Medical 4.0 technologies for healthcare: Features, capabilities, and applications. Internet of Things and Cyber-Physical Systems, 2, 12–30.

[10] Javaid, M., Haleem, A., Pratap Singh, R., & Suman, R. (2022). Enabling cloud computing technologies for healthcare: A review. Journal of Industrial Integration and Management, 7(03), 395–417.

[11] Kumar, A., & Singh, P. K. (2022). An observability framework for big data pipelines in cloud-based healthcare analytics. Computing, 104(8), 1821–1845.

[12] Ordibazar, A. H., & Al-Hashimi, M. (2022). Real-time monitoring of epidemic impacts on hospital operations using AIOps observability. Journal of Biomedical Informatics, 128, 104031.

[13] Patel, R., & Samad, A. (2022). Contextualized real-time data for AIOps observability in the healthcare industry. International Journal of Computing and Digital Systems, 11(1), 445–458.

[14] Periasamy, J., & Wang, Y. (2022). Optimizing patient data through AIOps: A framework for precise clinical diagnosis. Frontiers in Public Health, 10, 895123.

[15] Qadri, Y. A., Nauman, A., Zikria, Y. B., & Kim, S. W. (2022). The future of healthcare Internet of Things: A survey of emerging technologies and applications. IEEE Communications Surveys & Tutorials, 22(2), 1121–1167.

[16] Rivera, M., & Florea, R. (2021). Building resilient observability frameworks for big data in cloud ecosystems. Software: Practice and Experience, 51(12), 2410–2432.

[17] Wang, L., & Zhang, Y. (2022). Cloud-native observability for healthcare big data: Challenges and opportunities. Journal of Systems Architecture, 124, 102421.

[18] Zahid, H., & Periasamy, J. (2022). Remote healthcare transformation through digital provider applications and AIOps monitoring. Medical Education Online, 27(1), 204561.

[19] Alhayani, B., Abbas, S. T., & Mohammed, H. J. (2022). Intelligent automation of electronic health records using cloud-based AI frameworks. Journal of Medical Systems, 46(3), 112–125.