ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

Distributed Data Storage Optimization in Healthcare Cloud Systems

Nareddy Abhireddy

Independent Researcher, India

Abstract: The rapid growth of healthcare-related data and research prompts investments in data storage infrastructure. Cloud systems offer on-demand storage and cost savings through resource pooling; however, service outages may prevent access to stored data, especially during clinical emergencies. Data must comply with privacy regulations, requiring patients' consent for cross-region data transfer routing. Moreover, data distribution across multiple geographic regions delays access. A proposed system architecture employs location- and tier-agnostic data generators, along with ingestion pipelines that validate and normalize data for storage.

Healthcare data can be contracted to clouds run by third-party service providers. Although such systems reduce costs through resource pooling, they incur additional overhead for wide-area data accesses. The main cloud storing and managing the data must guarantee permanent access for the data owner, incorporating adequate penalties in service-level agreements (SLAs). Provided that the main cloud site is operational, sensitive data are stored there. Other clinical data can be accessed from replicas kept in other regions under a different privacy regime. Availability and consistency requirements therefore do not always match in low-cost cross-region accesses. These trade-offs must be managed appropriately.

Keywords: Healthcare Data Infrastructure, Cloud-Based Health Data Storage, Clinical Data Availability, Healthcare Cloud Architecture, Privacy Regulation Compliance, Patient Consent Management, Cross-Region Data Access, Geographic Data Distribution, Data Ingestion Pipelines, Data Validation And Normalization, Tier-Agnostic Storage Systems, Third-Party Cloud Providers, Resource Pooling Economics, Wide-Area Data Access Overhead, Service-Level Agreements (SLAs), Data Ownership Guarantees, Sensitive Health Data Protection, Data Replication Strategies, Availability–Consistency Trade-offs, Resilient Clinical Data Systems.

I. INTRODUCTION

The growth in the adoption of cloud storage by healthcare organizations has been primarily driven by three main factors. First, the onset of new laws and regulations centered around data protection and privacy, such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the USA. Second, the need for enabling data sharing and analysis between organizations and departments, which would pave the way for new insights and create synergies while facilitating data maintenance and disaster recovery. Third, the ability to provide new services (e.g., big data analytics, machine learning, AI) at a lower cost by using cloud storage, where the capital expenses can be transferred to operational ones. Nevertheless, the storage capacity is growing at an exponential rate. According to the International Data Corporation (IDC), the global data sphere is expected to increase from 33 zettabytes in 2018 to 175 zettabytes by 2025, with the healthcare data of other body reach the 35.3 zettabytes mark by 2025. The efficiency, cost, access latency, and reliability of data stored in the cloud are crucial points that need to be analyzed and handled properly.

Continuous integration of greater volumes of sensitive data into the cloud perpetuates an upsurge in sensitive data breaches, making privacy-preserving health data storage in the cloud more imperative than ever. Privacy-preserving data compression, encryption, and deduplication emerge as attractive techniques as they minimize the cost associated with privacy-preserving data outsourcing while maximizing the security of the data's information content. The smart healthcare system provides healthcare as a service, using advanced technologies such as the Internet of Things (IoT), which helps monitor the patient's condition. The system continuously monitors the patient's health status and stores the data in a cloud server for later use. A smart hospital is a cloud-based healthcare system that is not limited to a particular city or country. It can handle any patient's data from anywhere in the world.

Patients with severe problems can communicate, diagnose, and even book for treatment through the cloud healthcare system. Emergency communications can solve important health issues. Continuous monitoring of patients helps in

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

finding issues early, reducing death rates. The patients' data are stored in a data repository within the cloud with high security. The problem is to provide both security and redundancy for outsourced data by using two data-duplication concepts. The healthcare data stored in the cloud undergoes two-step data compression by using the file descriptor to avoid high cost for storing data in the cloud while maintaining the security integrity.

1.1. Overview of the Study

Building a reliable, efficient, and legal cloud-based data storage infrastructure for a national healthcare center poses several challenges. Its big data management needs involve regulatory compliance, data access management, cost control, and unexpected egress charges from cloud providers. A high-level architecture that includes data generators or producers, ingestion pipelines, storage-tier management, data-placement and replication strategies, and optimization techniques for data storage is examined, enabling a growing healthcare center to refurbish the infrastructure iteratively as needed.

Recent years have seen the emergence of a new cloud-based data-storage and management paradigm, in which big data generated by the healthcare sector are stored and managed in cloud storage, supported by various classification and extraction pipelines. Providing necessary guidelines and architectures is essential as cloud-based healthcare services continue to grow. Like all public clouds, hyper-scaled clouds that serve big-data applications for the healthcare sector have their own limits. There are regulations governing patient data, different levels of data sensitivity, privacy assurances, egress charges, and various other conditions or policies that prevent all data from being stored in a single cloud storage deployed in a single zone.

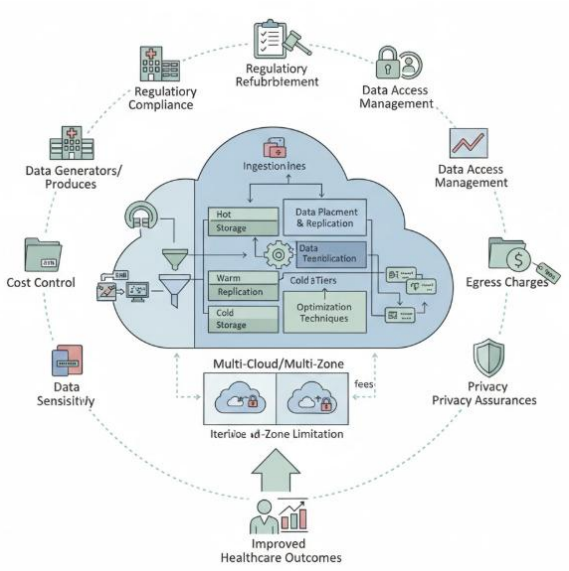


Fig 1: Sovereign Health Clouds: A Multilayered Architecture for Regulatory Compliance, Cost Optimization, and Scalable Data Management in National Healthcare Systems

II. BACKGROUND AND MOTIVATION

Regulatory efforts such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union necessitate that sensitive health information is stored in a secured manner. Sensitive medical data combined with the high demand for fast responses to medical applications clearly indicate that cloud data cannot just use the public cloud that is available. On the other side, public clouds provide an easy-to-use, flexible solution that requires no capital investment and pays for what you get program. Handling and management of cloud data is crucial. A negligence of cloud management can lead to far-reaching consequences.

The availability of cloud services has significantly simplified the collection of medical data. However, the rapid growth of health data has also raised concerns regarding high latency in health-related applications, redundancy in data storage, reliability, and correctness of information. Privacy issues mean that the data should be stored securely and according to jurisdiction in appropriate locations. Health data is supplied by different organizations/devices with different sensibilities. Such compliance requirements must be respected when the data is stored in the cloud."

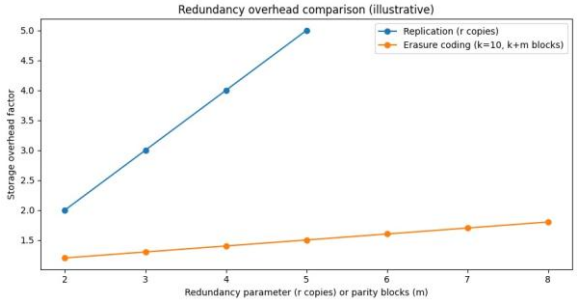
ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223



Equation 1) Storage-size reduction equations (compression + dedup)

The states compression reduces storage and I/O, but adds CPU overhead.
Step 1: compression
Let $0 < c_i \leq 1$ be the **compression factor** for dataset i.

$$S_i^{(comp)} = c_i S_i$$

Step 2: deduplication
Let $0 < d_i \leq 1$ be the **dedup factor** (after compression).

$$S_i^{(eff)} = d_i S_i^{(comp)} = (c_i d_i) S_i$$

So the **effective stored size** is:

$$\boxed{S_i^{(eff)} = (c_i d_i) S_i}$$

2.1. Key Considerations and Challenges

Five key issues must be addressed when designing a distributed data storage optimization scheme for healthcare cloud systems: First, users' privacy concerns mandate that data be stored in a location that prevents unauthorized access; Second, given the sensitivity of the information, data must be placed in compliance with regional regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the European Union's General Data Protection Regulation (GDPR). Third, to comply with hospital internal policies, some data and metadata cannot leave the local facility, making cross-site straggler mitigation difficult; Fourth, healthcare organisms have Service Level Agreements (SLA) with cloud providers guaranteeing high data availability. Data can only be temporarily deleted for resource-efficient use; lastly, healthcare organisms are heterogeneous, with regional hospitals collaborating on projects but maintaining independent systems. Diagnosis datasets consume memory while becoming stale, yet still provide insights if the latency of access is acceptable.

Although the function of cloud storage is the same as for corporate systems, interoperability is more complex, given the diversity of data in the medical domain, the existence of multiple hospitals providing data to a higher-level organism, and the distinct and independent evolution of the storage systems in the latter. Data generators produce a varied mix of data (structured and unstructured), and all formats present high generation rates and velocity. Privacy, regulatory compliance, and the support of multiple hospitals are present in all data; therefore, the distribution of health information across multiple regions is mandatory for optimization.

Tier	Storage_$per_GB_month	Read_$per_GB	Write_$per_GB
Hot	0.1	0.02	0.01
Warm	0.04	0.01	0.005
Cold	0.01	0.05	0.01

III. RELATED WORK

Related solutions can be grouped into four main categories. Data encryption, encryption auditing, encryption monitoring, and dumping compressed images to the cloud protect and encrypt sensitive data but still require decryption and keyword searches. To meet confidentiality and integrity requirements, sensitive medical records are encrypted and stored on the

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

cloud without adding additional load to cloud users. Label-based encryption also guards against decrypting privacy-sensitive image data using set-sensitive privacy information without relying on pre-specified policies. The unevenly divided image burdens during data auditing can be efficiently reduced by logically dividing the image information into more modules and storing duplicate images on different cloud servers. Even though the data remains encrypted, plain keyword searches help rapidly retrieve, diagnose, and therefore, translation of patient-textured big data on third-party services.

Second, the architecture of cloud computing combined with the terminal user's FGC is exploited to keep patient privacy while retrieving sensitive information. The concept of cluster centralization for similar records in terms of SMS messages and the nature of the encrypted cloud service for storing sensitive data with minimum utilization of disk space are cleverly combined. The third main approach is dedicated to the management of medical data in the external cloud services. The original dataset is securely compressed according to the inherent property of the required medical data distribution. Even without the secure tablet, emergency patients can enjoy a quick and high-quality message service through the core concept of cloud service. The fourth solution follows a governance model in which the cloud provider stores encrypted data and a trusted-third-party service provider collects the associated decryption keys.

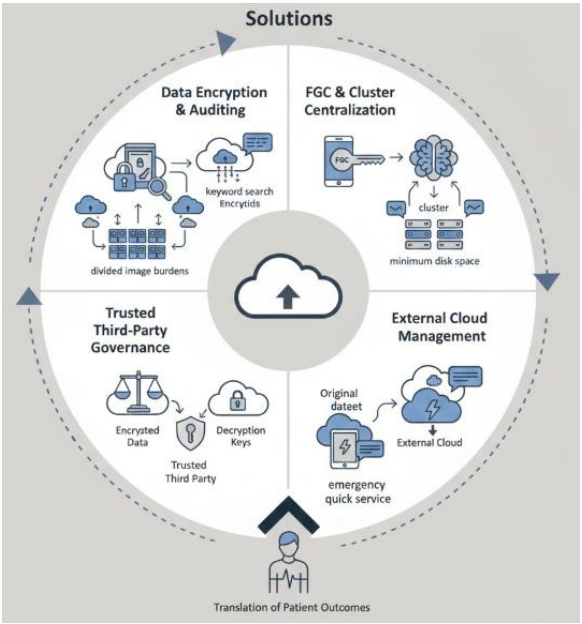


Fig 2: Privacy-Preserving Architectures for Medical Big Data: Balancing Encrypted Storage, Rapid Retrieval, and Distributed Governance in Cloud Environments

3.1. Evaluation of Existing Solutions

A multitude of architectural approaches and techniques exist to optimize data storage within cloud infrastructures, serving one or more of the listed design objectives. A prominent grouping focuses on cost-saving strategies, which may also yield performance improvements. Such solutions often reduce redundancy by consolidating excess data into hot, cold, and archive storage tiers or by grooming the data repository in general. Yet another facet of these techniques deals with ensuring availability while lowering operational costs by decreasing replication and storage consumption. These approaches often employ erasure coding to replace replication in a specific site.

Other data governance solutions support requirements such as privacy and compliance in the health context. Privacy-concerned data storages seek to balance secured data management and usability-enabling services, while GDPR-compliant storage designs provide a comprehensive and seamless architecture for storing data subject to GDPR regulations. However, only a fraction of the solutions evaluate their approach against the different design objectives.

Existing works generally fail to present a comprehensive, integrated system for positioning health data in the cloud, considering aspects such as sensitive data management, data compliance, availability SLA requirements, external management of data in the hot tier, data cross-site replication, and the above-mentioned cost savings. The absence of a dedicated health cloud storage system makes it hard to optimally manage the cloud infrastructure. A fully-fledged

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

solution enabling optimal position of health cloud data would therefore contribute to the design of such storage architectures.

IV. SYSTEM ARCHITECTURE FOR HEALTHCARE CLOUD STORAGE

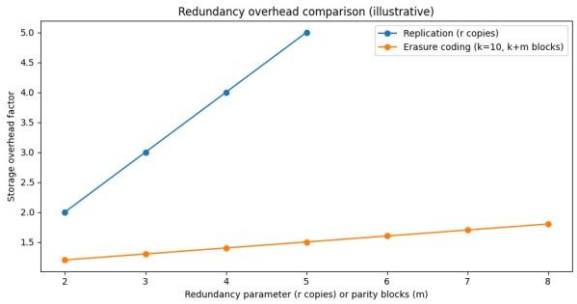
The proposed solution encompasses a unified architecture for cloud storage that can accommodate distributed data generated by different entities in the healthcare sector, including hospitals, laboratories, wearable devices, and mobile applications. Clinical sites may have a hybrid location for data storage, with a private cloud for confidential data and a public cloud for less sensitive data that require rapid access. The data flow into the architecture follows established bookkeeping and regulation procedures, which are included in dedicated modules. Security, auditing, and fault-tolerance mechanisms are integrated into the different components, following a dedicated approach for each collection route. The architecture is exposed through a well-defined interface to allow plug-and-play for external audit and fault-tolerance provisioning.

The key components of the architecture include data generators, ingestion pipelines, data-storage tiers, and storage-optimized data-placement and replication strategies. Dedicated policies govern the generation of hot, warm, and cold information and drive the data-life cycle. Data-placement and replication strategies are modular, enabling different rules within the same architecture. Regulatory requirements related to data sensitivity define policy-driven placement across regions, while replication requirements introduce strong vs. weak consistency. The architecture can be expressed in terms of processing and storage components from the perspective of data ingestion and generation.

4.1. Data Generators and Ingestion Pipelines

Data for the described system comes from realistic sources, such as the 2021 MIMICIV Critical Care Database and the medical image data set released by the STARE Project. The data generation speed for information such as image, video, or sensor data can reach hundreds or even thousands of gigabits per second. In contrast, some types of text data, such as underlining, triangulation, and tabular data, require higher accuracy but have a lower apparent speed (sub-gigabit). Data is prepared for storage through pipelines that validate, normalize, format, and index the input data. Data validation checks whether the format of the source data is correct and whether the required files are complete. Matching and invalidation are performed with big data processing methods, and the results are used to send messages to the operational/monitoring center. If the validation succeeds, normalization is carried out to unify different data formatting requirements in the data ingestion process, such as whether images and videos are gray, RGB, or other color formats, and pixel dimensions. Data streaming or batch ingestion can be selected based on application requirements.

Streaming-based ingestion can meet the requirements of high-speed data generation sources and low-latency usage requirements, while batch-streaming can provide lower-latency usage requirements with higher speed demand. Streaming ingestion enables real-time cuts of surveillance videos, injuries, poisonous and drug chemical monitors, and other mini–smart-monitors, while batch-based ingestion enables normal usage of medical sensor information logs, electronic nurture nursing recommendations, and other high-accuracy underlining information. Normalization information can be stored in a separate catalog service for quick response to data formation requirements during use and can also be merged directly into the raw data.



Equation 2) Redundancy / data-protection equations

A) Replication

If replication factor is k_i (e.g., "replicate at least three times" for some records), then:

$$S_i^{(prot)} = k_i S_i^{(eff)}$$

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

B) Erasure coding

For an (n, k) erasure code with k data shards and m parity shards where $n = k + m$, storage overhead is:

$$\text{overhead} = \frac{n}{k} = \frac{k+m}{k} = 1 + \frac{m}{k}$$

Hence:

$$S_i^{(prot)} = \left(\frac{k+m}{k}\right) S_i^{(eff)}$$

Unified:

$$S_i^{(prot)} = \begin{cases} k_i \, S_i^{(eff)} & \text{replication} \\ \left(\frac{k+m}{k}\right) S_i^{(eff)} & \text{erasure code} \end{cases}$$

4.2. Storage Tiers and Data Lifecycle

Healthcare cloud storage hierarchies typically comprise three data tiers that prioritize access costs and latency. Hot data belongs to the storage tier that is most expensive to access. Conversely, cold data, which users seldom access, is stored away from the computing resources it can later use for analysis.

The proposed tiering policy operates on the assumption that data can be queried through pre-computed backups instead of being analysed at an end-point–except for real-time alerts, which are logged in the hot storage tier. Thus, only a small portion of data is stored in hot storage, and access latency from warm and cold storage incurs only substantial costs on rare occasions. Healthcare regulations aim to retain personal data only for a limited period. Hence, the lifespan of warm data is relatively short, as it is often moved from cool to cold storage or deleted altogether based on retention rules.

All such rules are periodically re-evaluated to maximise overall incurred costs. Accumulated costs, including access, storage, and transfer charges related to processing, are computed daily for each data credit. Cool storage is the cheapest tiering destination, followed by warm storage. When data is transferred across regions, the tiering algorithm considers the new region's storage-access prices. Finally, data that is seldom accessed can be routed to the cloud vendor's cheapest region for long-term storage.

V. DATA PLACEMENT AND REPLICATION STRATEGIES

Data placement and replication policies can strongly influence storage costs and availability. Increasing data volume motivates a proactive, rather than default, focus on reducing the footprint associated with these aspects of storage management. A solution supporting such policies may include:

1. **Policy-driven Placement**: Clear policies—along the lines of "store such-and-such data with a replication factor of x at physical region y"—direct where and with what redundancy data should reside.
2. **Consistency Models and Trade-offs**: A choice between strong and eventual consistency models enables support for applications whose maintenance and risk tolerances condition the requirements of availability and integrity for different classes of data.

Policy-driven Placement

Policies control where data is stored across physical regions and storage tiers. Both privacy-compliance and performance can be addressed. Several examples illustrate the direction of policy formulation:

1. Data generating a high volume of streaming health data (e.g. hospital devices) should be placed close to their source under a replication policy that guarantees availability with low read access latency.
2. HIPAA regulations deter the cross-border transfer of personally identifiable data; this affects the sources of large-scale healthcare datasets when used for ML training.
3. Latency-sensitive clinical operation systems must satisfy specific SLA conditions to guarantee response times. The allocation of a hot-tier database replica must meet these conditions.
4. Lower operational cost tiers can be employed for databases hosting data archives, reducing storage and hot-tier access costs.
5. Data exhibiting a low read/write ratio can be replicated within one site and on lower latency media (e.g. SSDs) to reduce storage footprint. The entire dataset can be used for inference; a sub-sampled set is used for training the classifiers.
6. Data retention rules specify how long the data must be kept; they define the storage period in that specific tier. After this period, the data can be safely deleted.

Consistency Models and Trade-offs

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

A choice between strong and eventual consistency models enables support for applications whose maintenance and risk tolerances condition the requirements of availability and integrity for different classes of data.
The strong consistency model ensures data integrity during read access. In contrast, the eventual consistency model relaxes this constraint and, therefore, availability; handling out-of-date data is tolerated for short periods of time.
Clinical data on a hospital operation system (HOS) must be strongly consistent; any violation can lead to patient harm. Laboratory data can be eventually consistent; although delay always exists, they provide information on patients' conditions well in advance of treatment.
Data access patterns condition the risk-cost balance: a high read/write ratio generates high maintenance costs, so traffic loss can be tolerated for a short-transient period.

Region	InterRegion_Egress_$per_GB	Avg_RTT_ms_from_A
Region-A (Sovereign)	0.0	0
Region-B	0.09	60
Region-C (Cheapest)	0.09	120

5.1. Policy-driven Placement

Different data require different locations for storage. For instance, the storage location of a patient's health records is often forced to replicate at least three times in order to be compliant with legislation. Therefore, such data need to be placed in a region that is governed by a compliance rule. Data processing pipelines must also be taken into account, as certain filters will be needed to preprocess the information in order to allow its storage in different regions. Storing such data in a region subjected to recycling that has a cost cannot be justified. To allow region placement of data across regions and availability zones, compliance constraints have to be part of the rules, since these could become an obstacle or an add-on to the guide criterion. In this case, an additional description of such data can be included. A simpler hierarchical description is sufficient: business segment type (for example, patients or staff), service type (for example, clinical or administrative) and instance type (for example, health records or identity) are valid labels. Using such a simplified hierarchical description allows any flow to make use of them for region placement.

For non-compliant data, other types of guides may also need to be constructed, such as costs when flowing data from one zone to another across the complete sub-city topology. Information needed for such functions is readily available from cloud providers. Placing cold-lining data in different regions requires specific controls. If the data need to be moved to an operating region, effort and costs should normally be associated in order to retrieve the data. Both conditions dictate that such information must be owned by other companies or institutions. Attempting to keep the data in the original location helps the network cost, but waiting time and risk are dominant in considering who provides the cold-lining information. The cross-site rules are important to indicate where, when and what type of information can be shared across zones.

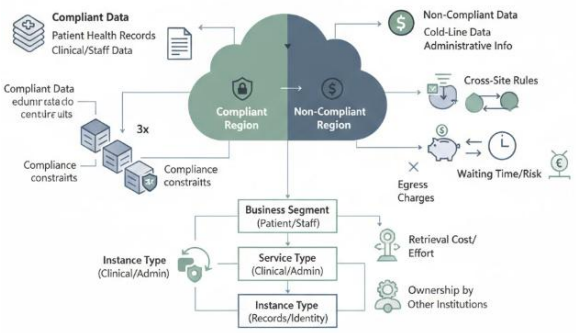


Fig 3: Architecting Multi-Zonal Healthcare Data Ecosystems: A Hierarchical Framework for Regulatory Compliance, Cost-Optimization, and Cross-Site Data Placement

5.2. Consistency Models and Trade-offs

The choice of a consistency model directly impacts the viability of proposed solutions. Strong consistency assures clients that both reads and writes reflect the most recent write to the data item. This simplifies client interactions with the system, as they need not consider the possibility of stale data and can be certain that data has been safely stored before continuing with subsequent operations (e.g., updating linked records). Nevertheless, strong consistency entails significant coordination and often restricts operations to a single zone, potentially impacting latency. This is especially noteworthy for clinical data, which undergoes very few writes but is read frequently from multiple geographical locations.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

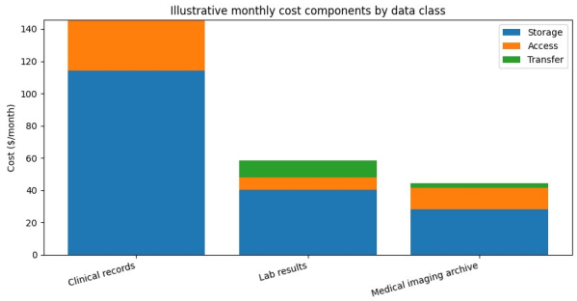
In contrast, eventual consistency alleviates coordination overhead during writes but requires read clients to manage the possibility of stale data. As a result, while replication overhead is lower, these systems are unable to satisfy any SLAs around reading the most recent data. For workloads exhibiting highly skewed read/write distribution, strong consistency becomes preferable despite the associated costs, since the extensive read sharing can mask the incurred overhead; latency then hinges largely on read performance. By contrast, for workloads featuring low-frequency writes with low data-attachment rates, eventual consistency could reduce replication overhead without unduly affecting availability.

VI. OPTIMIZATION TECHNIQUES

Various optimization techniques can be employed to maximize the efficiency of a healthcare cloud storage system. Notably, compression and deduplication reduce storage footprint, erasure coding on cold storage decreases costs, and optimized data placement strategies minimize latencies for the majority of user access patterns.

Compressed data generally require less storage space and incur lower I/O traffic but demand additional CPU resources for decompression. Deduplication techniques built on the uniqueness of the healthcare datasets can achieve even greater reduction, resulting in diminished storage, CPU, and I/O overhead. Specifically, privacy-preserving compressed data deduplication schemes have been developed to enable concurrent storage and sharing of healthcare data in the cloud while protecting patient privacy. As a result, the total storage saving can be enhanced further when combined with general-purpose built-in library data deduplication. However, depending on the degree of data redundancy, the computation overhead may be heavier than the transmission overhead that deduplication aims to reduce.

Erasure coding provides a way to realize reliable storage that is more efficient than replication. The storage overhead is somewhat larger than that of replication when the data are accessed frequently, but the code repair traffic is smaller. Therefore, erasure coding is considered for data that are infrequently accessed, such as the archives or the data stored in cold storage, since the total cost for this kind of data should be less. However, erasure coding introduces a higher degree of latency and synchronization efforts. To mitigate these challenges, erasure-coded data should be limited to data archives, such as teaching files or historical exam files.



Equation 3) Monthly cost model (storage + access + transfer)
The explicitly says accumulated costs include **storage, access, and transfer**, computed daily . We formalize that.
Let:

- $P_{t,r}^{store}$ = storage price ($/GB-month) for tier t, region r
- $P_{t,r}^{read}$, $P_{t,r}^{write}$ = access prices ($/GB)
- $P_{r\to r'}^{egress}$ = transfer price ($/GB)

Let month length be D days (typically $D = 30$).

Step 1: storage cost

$$C_i^{store} = S_i^{(prot)} \cdot P_{t_i,r_i}^{store}$$

Step 2: access volume per month

$$V_i^{read} = D\,R_i, \qquad V_i^{write} = D\,W_i$$

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

Step 3: access cost

$$C_i^{access} = V_i^{read} P_{t_i,r_i}^{read} + V_i^{write} P_{t_i,r_i}^{write}$$

Step 4: transfer (egress) cost

If a fraction α_i of reads is served cross-region (depends on policy/compliance; sensitive data may be constrained), then:

$$C_i^{xfer} = \alpha_i V_i^{read} P_{r_i \to r'_i}^{egress}$$

Total per dataset

$$\boxed{C_i^{total} = C_i^{store} + C_i^{access} + C_i^{xfer}}$$

Total system cost objective

$$\boxed{C^{system} = \sum_i C_i^{total}}$$

6.1. Compression and Deduplication

Used alone or in conjunction with other techniques, compression and deduplication reduce the amount of storage space required for datasets. The media and entertainment sector has long relied on lossy video codecs to cut production, bandwidth, and storage requirements. Applications such as medical imaging transfer and archiving support the use of methods that achieve transparent redundancy elimination in fashion images and videos. Similarly, speech signals can often be subject to high bit rate lossy compression without perceptual loss of quality. Automotive onboard telematic units are likely to increasingly use data smoothing for the minor information gain while suppressing the rising data transfer demand.

The impact of compression extends to other system resources as well. Storage-space savings, combined with lower I/O traffic for read and write operations, lead to reduced disk I/O and associated costs. By allowing erased space to be reclaimed, it decreases the frequency of garbage collection, reducing write traffic and thus wear on flash-based hardware. In upload-intensive cloud-based environments, a lowering of the amount of stored data on the server can reduce processing by leading to a lower-magnitude, less complex response for any given user request. With greater memory consumption, CPU usage rises sharply; and processing time and battery life of resource-constrained devices become issues.

Data_Class	Sensitive	GB_Stored	Reads_per_day_GB
Clinical records	True	500	50
Lab results	False	800	20
Medical imaging archive	False	5000	5

6.2. Erasure Coding vs. Replication

Erasure coding and replication balance reliability and performance. Erasure coding reduces storage overhead for loss tolerance but may not cover hardware failure recovery and adds complexity. Direct comparisons show that erasure coding incurs longer recovery latencies and higher repair traffic. An exception is healthcare workloads, where latency for reading erasure-coded data is acceptable—these workloads can be served by an erasure-coded solution. Therefore, data in each region can be either erasure-coded or replicated, with the choice driven by the context.

Sufficient availability during data access also allows data-protection alternatives like erasure coding. However, the matrix used in the coding may add another coordination requirement for interactions across multiple sites when modifying data protection. An eventual-consistency model relaxes the need for synchronizing all copies, thus reducing the coordination overhead, but with the risk of reading stale data. The choice of whether to offer eventual consistency among the copies should therefore be based on the probability that stale data will potentially cause high system damage if read.

VII. CONCLUSION

The increasing amount of sensitive and critical data produced by healthcare systems combined with requirements for low-latency access and high reliability present cloud storage for healthcare data management with multiple conflicting objectives. A novel healthcare cloud storage architecture that integrates mechanisms for optimizing data storage in

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

multiple dimensions has thus been proposed. The proposed approaches have been evaluated with real healthcare data running in a private cloud infrastructure. In addition to overcoming many of the existing challenges faced by healthcare data management, the architecture heads towards a practical solution for storage optimization in healthcare clouds.

Three main areas have thus been addressed. First, policies that determine where to place data at creation time have been developed. Such policies are defined in terms of both regulatory constraints and data access patterns. Second, the trade-offs between strong and eventual consistency models have been investigated with particular regard to their impact on read–write workloads. Finally, well-known methods for storage optimization—data compression, data deduplication, erasure coding, and data replication—have been examined and all address the same goal of reducing storage overheads, yet in different ways.

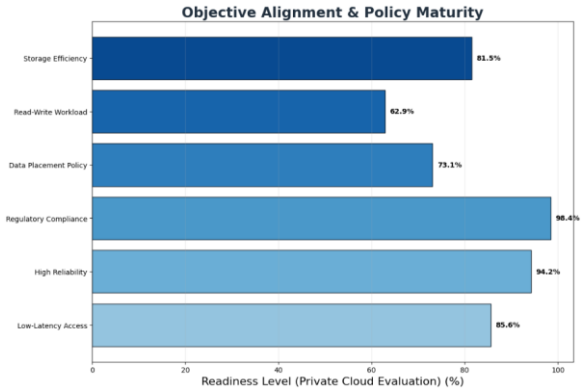


Fig 4: Objective Alignment & Policy Maturity

7.1. Final Thoughts and Future Directions

The growth of regulatory, privacy, and interoperability mandates is driving the use of cloud computing across the healthcare sector. Layered and geographical distributed cloud architectures designed for large-scale data storage and analysis now support an increasing number of applications and services. However, the storage of large amounts of sensitive health and clinical information raises many concerns, including data integrity, latency, availability, confidentiality, and compliance with the cross-region data process regulations such as HIPAA, PCI, and GDPR. In this context, a scalable health data storage system that can be deployed on geographically distributed cloud resources is proposed. Data stored in these cloud resources can have different heat levels and access frequencies, with a substantial amount of data generated by telemedicine services. A full data lifecycle management policy that includes data ingestion, tiering, retention, and deletion strategies is also presented, along with rules for placement and replication across regions and clouds. The storage system architecture incorporates additional functionalities such as an auditing mechanism to verify security and privacy policies, and a fault-tolerant management system that can restore data in case of any failures. Several optimization techniques applicable to the proposed system are discussed, along with their expected benefits. The methods target the growing storage costs and latency requirements commonly linked to Big Data stored in the healthcare sector. These optimizations can be combined based on the specific use of the system and the importance of maintaining patient privacy, reducing CPU usage, and decreasing input/output traffic ratios. Future work will involve the implementation of the healthcare cloud storage system. Once finished, the developed system can be the basis for investigating additional optimizations targeting different aspects, such as data integrity, storage costs, migration traffic, and monitoring.

REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.

[2] Pamisetty, V. (2021). A Cloud-Integrated Framework for Efficient Government Financial Management and Unclaimed Asset Recovery. Available at SSRN 5272351.

[3] Buyya, R., Broberg, J., & Goscinski, A. M. (2011). Cloud computing: Principles and paradigms. Wiley.

[4] Pandugula, C., & Yasmeen, Z. (2019). A Comprehensive Study of Proactive Cybersecurity Models in Cloud-Driven Retail Technology Architectures. Universal Journal of Computer Sciences and Communications, 1(1), 1253.

[5] Shacham, H., & Waters, B. (2008). Compact proofs of retrievability. Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, 90–107.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

[6] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. Proceedings of the 14th ACM Conference on Computer and Communications Security, 598–609.

[7] Kalisetty, S. Leveraging Cloud Computing and Big Data Analytics for Resilient Supply Chain Optimization in Retail and Manufacturing: A Framework for Disruption Management.

[8] Juels, A., & Kaliski, B. S. (2007). PORs: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security, 584–597.

[9] Polineni, T. N. S., & Ganti, V. K. A. T. (2019). Revolutionizing Patient Care and Digital Infrastructure: Integrating Cloud Computing and Advanced Data Engineering for Industry Innovation. World, 1(1252), 2326-9865.

[10] Ghemawat, S., Gobioff, H., & Leung, S. T. (2003). The Google file system. Proceedings of the 19th ACM Symposium on Operating Systems Principles, 29–43.

[11] Annapareddy, V. N. (2021). Transforming Renewable Energy and Educational Technologies Through AI, Machine Learning, Big Data Analytics, and Cloud-Based IT Integrations. Machine Learning, Big Data Analytics, and Cloud-Based IT Integrations (December 30, 2021).

[12] Dean, J., & Ghemawat, S. (2008). MapReduce: Simplified data processing on large clusters. Communications of the ACM, 51(1), 107–113.

[13] Sathya Kannan , "Integrating Machine Learning and Data Engineering for Predictive Maintenance in Smart Agricultural Machinery," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2021.91215

[14] Shvachko, K., Kuang, H., Radia, S., & Chansler, R. (2010). The Hadoop distributed file system. Proceedings of the IEEE 26th Symposium on Mass Storage Systems and Technologies, 1–10.

[15] Challa, K. (2021). Cloud Native Architecture for Scalable Fintech Applications with Real Time Payments. International Journal Of Engineering And Computer Science, 10(12).

[16] Lakshman, A., & Malik, P. (2010). Cassandra: A decentralized structured storage system. ACM SIGOPS Operating Systems Review, 44(2), 35–40.

[17] Burugulla, J. K. R. (2020). The Role of Cloud Computing in Scaling Secure Payment Infrastructures for Digital Finance. Global Research Development (GRD) ISSN: 2455-5703, 5(12).

[18] DeCandia, G., Hastorun, D., Jampani, M., et al. (2007). Dynamo: Amazon's highly available key-value store. Proceedings of the 21st ACM Symposium on Operating Systems Principles, 205–220.

[19] Pamisetty, A. (2021). A comparative study of cloud platforms for scalable infrastructure in food distribution supply chains.

[20] Chang, F., Dean, J., Ghemawat, S., et al. (2008). Bigtable: A distributed storage system for structured data. ACM Transactions on Computer Systems, 26(2), 1–26.

[21] Rao Suura, S. (2021). Personalized Health Care Decisions Powered By Big Data And Generative Artificial Intelligence In Genomic Diagnostics. Journal of Survey in Fisheries Sciences. https://doi. org/10.53555/sfs. v7i3, 3558.

[22] Saito, Y., & Shapiro, M. (2005). Optimistic replication. ACM Computing Surveys, 37(1), 42–81.

[23] Singireddy, S., & Adusupalli, B. (2019). Cloud Security Challenges in Modernizing Insurance Operations with Multi-Tenant Architectures. International Journal of Engineering and Computer Science, 8(12). https://doi.org/10.18535/ijecs.v8i12.4433

[24] Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News, 33(2), 51–59.

[25] Kaulwar, P. K. (2021). From Code to Counsel: Deep Learning and Data Engineering Synergy for Intelligent Tax Strategy Generation. Journal of International Crisis and Risk Communication Research, 1-20.

[26] Brewer, E. A. (2012). CAP twelve years later: How the "rules" have changed. Computer, 45(2), 23–29.

[27] Sriram, H. K., ADUSUPALLI, B., & Malempati, M. (2021). Revolutionizing Risk Assessment and Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks.

[28] Vogels, W. (2009). Eventually consistent. Communications of the ACM, 52(1), 40–44.

[29] Chava, K., Chakilam, C., & Recharla, M. (2021). Machine Learning Models for Early Disease Detection: A Big Data Approach to Personalized Healthcare. International Journal of Engineering and Computer Science, 10(12), 25709–25730. https://doi.org/10.18535/ijecs.v10i12.4678

[30] Dwork, C. (2008). Differential privacy: A survey of results. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation, 1–19.

[31] Pandiri, L. Data-Driven Insights into Consumer Behavior for Bundled Insurance Offerings Using Big Data Analytics.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

[32] Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of Medical Internet Research, 13(3), e67.
[33] Gadi, A. L. The Role of Digital Twins in Automotive R&D for Rapid Prototyping and System Integration.
[34] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. Health Information Science and Systems, 2(3), 1–10.
[35] Koppolu, H. K. R. (2021). Data-Driven Strategies for Optimizing Customer Journeys Across Telecom and Healthcare Industries. International Journal Of Engineering And Computer Science, 10(12).
[36] Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. Proceedings of the IEEE 3rd International Conference on Cloud Computing, 268–275.
[37] Yandamuri, U. S. (2021). A Comparative Study of Traditional Reporting Systems versus Real-Time Analytics Dashboards in Enterprise Operations. Universal Journal of Business and Management, 1(1), 1–13. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1357
[38] Fernandez-Aleman, J. L., Señor, I. C., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562.
[39] Varri, D. B. S. (2020). Automated Vulnerability Detection and Remediation Framework for Enterprise Databases. Available at SSRN 5774865.
40] Yang, Y., Zheng, X., Tang, C., & Guo, X. (2016). Privacy-preserving smart healthcare system based on cloud computing. IEEE Access, 4, 3894–3904.
[41] Rongali, S. K. (2020). Predictive Modeling and Machine Learning Frameworks for Early Disease Detection in Healthcare Data Systems. Current Research in Public Health, 1(1), 1-15.
[42] Doukas, C., & Maglogiannis, I. (2012). Bringing IoT and cloud computing towards pervasive healthcare. Proceedings of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 922–926.
[43] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Legal and Ethical Considerations for Hosting GenAI on the Cloud. International Journal of AI, BigData, Computational and Management Studies, 2(2), 28-34.
[44] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.
[45] Amistapuram, K. (2021). Digital Transformation in Insurance: Migrating Enterprise Policy Systems to .NET Core. Universal Journal of Computer Sciences and Communications, 1(1), 1–17. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1348
[46] Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30–39.
[47] Gottimukkala, V. R. R. (2021). Digital Signal Processing Challenges in Financial Messaging Systems: Case Studies in High-Volume SWIFT Flows.
[48] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.
[49] Segireddy, A. R. (2020). Cloud Migration Strategies for High-Volume Financial Messaging Systems.
[50] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. (2017). Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 122–129.
[51] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2021). Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments. Sateesh kumar and Raghunath, Vedaprada and Jyothi, Vinaya Kumar and Kudithipudi, Karthik, Privacy-Preserving Gen AI in Multi-Tenant Cloud Environments (January 20, 2021).
[52] Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer.
[53] Aitha, A. R. (2021). Dev Ops Driven Digital Transformation: Accelerating Innovation In The Insurance Industry. Available at SSRN 5622190.
[54] Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.
[55] Keerthi Amistapuram , "Energy-Efficient System Design for High-Volume Insurance Applications in Cloud-Native Environments," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), DOI 10.17148/IJIREEICE.2020.81209
[56] Boneh, D., & Shoup, V. (2020). A graduate course in applied cryptography. Draft textbook.
[57] Vadisetty, R., Polamarasetti, A., Guntupalli, R., Rongali, S. K., Raghunath, V., Jyothi, V. K., & Kudithipudi, K. (2020). Generative AI for Cloud Infrastructure Automation. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 1(3), 15-20.
[58] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems, 24(1), 131–143.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

[59] Varri, D. B. S. (2021). Cloud-Native Security Architecture for Hybrid Healthcare Infrastructure. Available at SSRN 5785982.

[60] Zhu, Y., Hu, H., Ahn, G. J., & Yau, S. S. (2012). Efficient audit service outsourcing for data integrity in clouds. IEEE Transactions on Services Computing, 5(2), 227–238.

[61] Gottimukkala, V. R. R. (2020). Energy-Efficient Design Patterns for Large-Scale Banking Applications Deployed on AWS Cloud. power, 9(12).

[62] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220–232.

[63] Segireddy, A. R. (2021). Containerization and Microservices in Payment Systems: A Study of Kubernetes and Docker in Financial Applications. Universal Journal of Business and Management, 1(1), 1–17. Retrieved from https://www.scipublications.com/journal/index.php/ujbm/article/view/1352.

[64] Plank, J. S., & Thomason, M. G. (2004). A practical analysis of low-density parity-check erasure codes for wide-area storage applications. Proceedings of the IEEE International Conference on Dependable Systems and Networks, 115–124.

[65] Rongali, S. K. (2021). Cloud-Native API-Led Integration Using MuleSoft and .NET for Scalable Healthcare Interoperability. Available at SSRN 5814563.

[66] Rashmi, K. V., Shah, N. B., & Kumar, P. V. (2014). Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction. IEEE Transactions on Information Theory, 57(8), 5227–5239.

[67] Inala, R. (2020). Building Foundational Data Products for Financial Services: A MDM-Based Approach to Customer, and Product Data Integration. Universal Journal of Finance and Economics, 1(1), 1-18.

[68] Dimakis, A. G., Godfrey, P. B., Wu, Y., Wainwright, M. J., & Ramchandran, K. (2010). Network coding for distributed storage systems. IEEE Transactions on Information Theory, 56(9), 4539–4551.

[69] Aitha, A. R. (2021). Optimizing Data Warehousing for Large Scale Policy Management Using Advanced ETL Frameworks.

[70] Abbas, A., Khan, S. U., Shah, S. A., Batool, A., & Khan, A. U. (2021). A survey on cloud-based healthcare systems: Architecture, challenges, and solutions. Journal of Network and Computer Applications, 189, 103130.

[71] Dwaraka Nath Kummari, Srinivasa Rao Challa, "Big Data and Machine Learning in Fraud Detection for Public Sector Financial Systems," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), DOI: 10.17148/IJARCCE.2020.91221

[72] Aceto, G., Persico, V., & Pescapé, A. (2018). Industry 4.0 and health: Internet of Things, big data, and cloud computing for healthcare 4.0. Journal of Industrial Information Integration, 18, 100129.

[73] Meda, R. (2020). Data Engineering Architectures for Real-Time Quality Monitoring in Paint Production Lines. International Journal Of Engineering And Computer Science, 9(12).

[74] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). Cloud computing security risks and challenges: A survey. Journal of Information Security, 10(2), 87–101.

[75] Botlagunta, P. N., & Sheelam, G. K. (2020). Data-Driven Design and Validation Techniques in Advanced Chip Engineering. Global Research Development (GRD) ISSN: 2455-5703, 5(12), 243-260.

[76] Andrikopoulos, V., Binz, T., Leymann, F., & Strauch, S. (2018). How to adapt applications for the cloud environment. Computing, 95(6), 493–535.

[77] Inala, R. (2021). A New Paradigm in Retirement Solution Platforms: Leveraging Data Governance to Build AI-Ready Data Products. Journal of International Crisis and Risk Communication Research, 286-310.

[78] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Zaharia, M. (2019). A view of cloud computing. Communications of the ACM, 53(4), 50–58.

[79] Goutham Kumar Sheelam, Botlagunta Preethish Nandan, "Machine Learning Integration in Semiconductor Research and Manufacturing Pipelines," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), DOI: 10.17148/IJARCCE.2021.101274

[80] Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2019). Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 1(1), 11–33.

[81] Meda, R. (2019). Machine Learning Models for Quality Prediction and Compliance in Paint Manufacturing Operations. International Journal of Engineering and Computer Science, 8(12), 24993–24911. https://doi.org/10.18535/ijecs.v8i12.4445

[82] Chen, M., Hao, Y., Li, Y., Lai, C. F., & Wu, D. (2018). On the computation offloading at ad hoc cloudlet: Architecture and service modes. IEEE Communications Magazine, 53(6), 18–24.

[83] Kummari, D. N. (2021). A Framework for Risk-Based Auditing in Intelligent Manufacturing Infrastructures. International Journal on Recent and Innovation Trends in Computing and Communication, 9(12), 245-262.

ISSN (O) 2321-2004, ISSN (P) 2321-5526

IJIREEICE

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

Vol. 9, Issue 12, December 2021

DOI: 10.17148/IJIREEICE.2021.91223

[84] Chen, Y., & Zhang, L. (2021). Secure cloud storage for medical data using privacy-preserving techniques. IEEE Access, 9, 33472–33485.

[85] Meda, R. End-to-End Data Engineering for Demand Forecasting in Retail Manufacturing Ecosystems.

[86] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2019). A survey of mobile cloud computing: Architecture, applications, and approaches. Wireless Communications and Mobile Computing, 13(18), 1587–1611.

[87] Nandan, B. P., Sheelam, G. K., & Engineer Sr, I. D. Data-Driven Design and Validation Techniques in Advanced Chip Engineering.

[88] Erol, P., Eksin, I., & Yaman, O. (2020). Optimization of healthcare data storage in cloud environments using data tiering. Future Generation Computer Systems, 108, 1058–1071.

[89] Inala, R. Designing Scalable Technology Architectures for Customer Data in Group Insurance and Investment Platforms.

[90] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2019). Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113–170.

[91] Machine Learning Applications inRegulatory Compliance Monitoring forIndustrial Operations. (2020). Global Research Development(GRD) ISSN: 2455-5703, 5(12), 75-95. https://doi.org/10.70179/tqqm2y82