International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices

Nihar Malali
Independent Researcher, University of Texas, USA
blitznihar@gmail.com

doi: https://doi.org/10.37745/ijirm.14/vol12n15073 Published April 21, 2025

Citation: Malali N. (2025) Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices, *International Journal of Interdisciplinary Research Methods*, *Vol*.12, No.1, pp.50-73

Abstract: *The emergence of Cloud-native technologies helps life and annuity insurance companies run faster and grow better while providing better services to their customers. As business moves to cloud-native technologies, they face major security dangers from outside parties along with internal staff while meeting GDPR HIPAA SOX, and PCI DSS requirements. This research explains security dangers that insurance companies face and suggests Zero Trust, ID & Access control, data encryption, and SIEM as effective defenses. The plan describes how to face compliance needs by auditing regulations, inspecting external risks, and data placement to match different regulations worldwide. The paper uses actual industry events and industry practice information to show how AI creates security challenges and how blockchain helps protect systems. This study presents helpful advice that lets insurers safely build cloud-native systems together with meeting regulatory requirements and strengthening stakeholder trust.*

Keywords: Cloud-native security, compliance, life and annuities insurance, regulatory frameworks, cloud computing in insurance**.**

INTRODUCTION

Cloud computing is transforming the insurance industry in general and life and annuities insurance in particular. It presents immense benefits of scale, agility, and cost efficiency. Nevertheless, it comes with a major security and compliance burden when it comes to protecting sensitive customer data. As a part of this study, we try to understand how the challenges and best practices of cloud native security and compliance can be applied to the life and annuities insurance domain.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Background: Cloud Computing in the Insurance Industry

Innovative solutions offered by cloud computing across the board in the insurance sector such as increased operational efficiency, improved data management and better customer experience, are revolutionising the insurance sector. Usually, insurers relied on fixed it infrastructures located in their premises, which were expensive, rigid and it was difficult to scale. Cloud technologies, particularly cloud native applications, enable insurers to process big data in actual time, integrate artificial intelligence and machine learning for risk rating, and automate the client interactions.

Key Drivers of Cloud Adoption in Insurance:

- **Scalability and Flexibility**: Cloud services enable insurers to scale their operations as per demand fluctuations.
- **Cost Savings**: Migrating to cloud-based infrastructures gives you lower capital expenditures on hardware and software among other things to optimize IT costs.
- **Data-Driven Decision Making**: Cloud platforms enable the use of big data analytics, AI, and ML to assess risk, detect fraud, and personalise insurance products.
- **Regulatory Compliance Support**: All major cloud providers offer security features as part of their offering so that insurer do not have to deal with the security and compliance features on their own, but this doesn't mean that it is the same in compliance.

While these benefits make the case for using cloud to create insurance applications, the move to the cloud brings with it enormous security and compliance issues. Insurers are dealing with the most sensitive personal and financial data, which requires having data protection and regulatory compliance guaranteed.

Problem Statement: Security and Compliance Challenges in Cloud-Native Insurance Applications

The cloud native applications bring in better performance and diversification, but it is accompanied by new level of threat and regulatory challenges to the life and annuities insurers.

Security Challenges

- **Data Breaches and Unauthorised Access**: Cloud cater to cybercriminals due to the absorbed of large volume of data that is confidential or sensitive in nature which contain PII, Financial data, health data.

- **Insider Threats**: Whenever current or former workers, contractors and/or third-party vendors have authorised access to the cloud-based insurance applications, the public faces dangers if sufficient access management entries are lacking.
- **Shared Responsibility Model**: Cloud providers secure infrastructure, but insurers remain responsible for securing their applications and data. Misconfigurations can lead to vulnerabilities.
- **Identity and Access Management (IAM) Issues**: IAM Issues tend to compromise the general security level by allowing invalid authentication and having ineffective access control plans.

Compliance Challenges

- **Regulatory Complexity**: Insurance companies must comply with various regulatory frameworks, such as:
    - **General Data Protection Regulation (GDPR)** (for European customers)
    - **Health Insurance Portability and Accountability Act (HIPAA)** (for health-related insurance)
    - **Sarbanes-Oxley Act (SOX)** (for financial reporting compliance)
    - **Payment Card Industry Data Security Standard (PCI DSS)** (for credit card transactions)
    - **State-Specific Regulations** (such as the California Consumer Privacy Act - CCPA)
- **Data Sovereignty and Residency Requirements**: Data Sovereignty and residency require that customer data be held within certain geographical locations and thus complicate the deployment of cloud.
- **Audit and Reporting Challenges**: For new-age cloud applications, specialised techniques are needed in the realm of monitoring and logging to meet the compliance and response needs.
- **Third-Party Risk Management: Most** insurance organisations use third-party cloud service providers that require strong contracts and regular assessments.

Given these challenges, what security strategies and best practices can insurers adopt to protect sensitive customer data while maintaining compliance?

Research Questions

For the purposes of this research that aims at focusing on cloud security and compliance of cloud-native applications in life and annuities insurance the following key questions will be used:

1. What are the major security threats facing cloud-native insurance applications?

2. How can the institutions using insurance gain approval to deploy the cloud technologies?
3. What are the best practices that can be adopted in the improvement of cloud native security in life and annuities insurance organisations?
4. How do cloud service providers contribute to security and compliance in the insurance sector?
5. What role do emerging technologies (e.g., AI, blockchain) play in improving cloud security for insurance companies?

These questions will help the study in establishing the strategies to be used in cloud security taking into consideration the compliance levels needed.

Objectives: Identifying the Challenges and Best Practices of Cloud-Native Security and Compliance in Life and Annuities Insurance

The purpose of this paper is to determine the practices of cloud security and compliance within the life and annuities insurance industry. Specifically, it aims to:

1. Discuss the security risks involved in cloud environments with specific regard to native insurance applications.
2. provide an analysis of the regulatory environment of the use of cloud services in the insurance segment with reference to GDPR, HIPAA, SOX, and other regulative acts.
3. Evaluate cloud security strategies such as encryption, Zero Trust Architecture, Identity and Access Management (IAM), and Security Information and Event Management (SIEM).
4. Identify compliance measures that insurance companies can adopt while seeking to achieve regulatory requirement with cloud structure.
5. Prescribe improved ways of protecting customers' sensitive data and Compliance through the effective implementation of proper technical measures.

By addressing these objectives, this study is expected to enhance the understanding of the cloud-native security and compliance within life and annuities insurance. It will be useful to current and prospective buyers, risk managers, insurers, and policymakers interested in risk management, data security in cloud services, and compliance with regulatory standards in industries.

LITERATURE REVIEW

To synthesis the current scholastic findings for implementing cloud computing in the insurance industry, this paper includes the following subtopics: the emerging benefits of cloud computing the insurance industry, the security measures that can be employed in the implementation of cloud computing system, and the tariffs formulated by regulatory authorities for cloud computing system in the insurance industry. To achieve

this, the following information is compiled from scholarly articles, industry reports, and regulatory guidelines about cloud-native security and compliance in the life and annuities insurance.

Cloud Computing in the Insurance Industry: Benefits and Challenges

The topic of Cloud in the Insurance Industry is a must-touch sensitive issue because indeed cloud is one of the significant success drivers for digital insurance transformation. This increases the opportunities of insurers to analyse massive amounts of data in real time with the help of cloud-native architectures, integrate the necessary weighty analytics for risk assessment of policies, and develop AI-driven solutions for engaging customers. Still, there are great risks associated with security and compliance as insurers undertake these benefits.

Benefits of Cloud Computing in Insurance

- **Scalability and Flexibility**
    a. In essence, cloud-native architectures help insurers grow their infrastructure at the customer and business contingents without a hitch.
    b. Elastic computing resources provide a client with the capability to minimise his/her expenses on IT infrastructures and equipment maintenance.
- **Enhanced Data Analytics and AI Integration**
    c. Real-time information handling is made possible by the cloud so that big data analysis, ML, and AI can be applied by insurers in the detection of fraud, assessment of the risks, and recommendations on policies.
    d. Insurers can use predictive analytics in the process of risk assessment and decision-making concerning policyholders.
- **Improved Disaster Recovery and Business Continuity**
    e. In cloud environments, the backups and disaster recovery or DR operations are automatically carried out, thus allowing for minute downtimes, should there be an attack or system failure.
    f. Multi-region redundancy makes it possible to meet the intended objectives especially when abrupt failures occur within the infrastructure.
- **Enhanced Customer Experience**
    g. Insurers connect with their customers on a digital device used in self-service, mobile applications, and AI chatbots.
    h. This allows quick processing of claims and issuance of polices increases the level of satisfaction among the customers.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

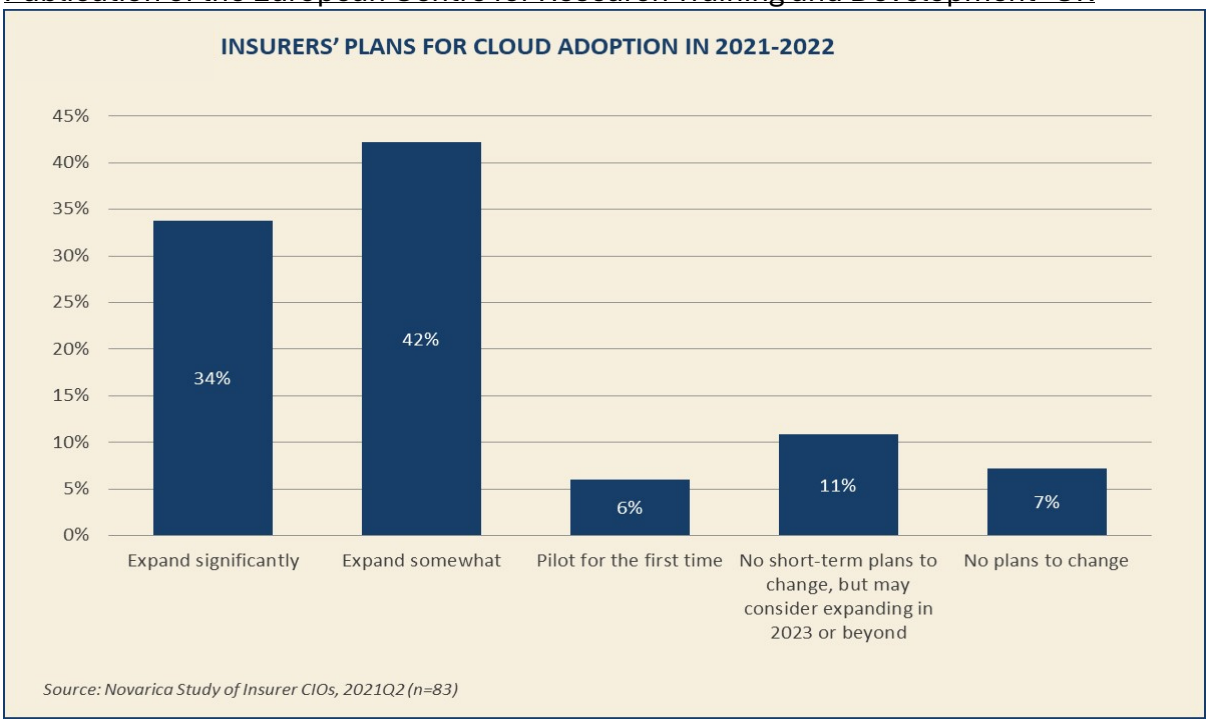

Figure 1: Cloud Computing Adoption in the Insurance Industry

Challenges of Cloud Computing in Insurance

While cloud computing presents much value in business, it also comes with various risks relating to security and compliance.

- **Data Security Risks**
  a. It is alarming that insurance companies deal with Personally Identifiable Information (PII) and financial information that may be compromised.
  b. This paper seeks to explain why misconfiguration of cloud storage ultimately poses great risks in allowing unauthorised access and public exposure of data.
- **Regulatory Compliance Complexity**
  c. The insurers operating in the cloud environments are facing many regulatory complexities from one country to another that include General data protection regulation, Health Insurance portability and accountability act and the Sarbanes-Oxley act.
  d. Cloud providers can place data in several locations; thus, issues with data jurisdiction and location arise.

- **Shared Responsibility Model**
    e. Security for the infrastructure is provided by the cloud service providers, while the insurance sector alone is expected to be more secured for the applications, data, and access control.
    f. Laxity in security measures or poor contents of access mean that an organisation is likely to be at the mercy of hackers.
- **Third-Party Risks and Vendor Lock-In**
    g. Using third-party cloud vendors entails certain risks associated with customers' personal information protection, disruption of cloud services, compatibility with laws and regulations.
    h. This makes it quite cumbersome for insurers to change providers since it is likely to cause some disruption in their operations.

Current studies show that issues of security must be effectively addressed along with the regulatory requirements aiming at their solution.

Cloud Security Strategies: Overview of Existing Research

Measures for Information security are important when dealing with risks associated with cloud-native Applications in Insurance sector. Previous literature describes various effective measures and guidelines in preserving customers' privacy and meeting the rules and regulations.

❖ **Zero Trust Architecture (ZTA)**

- The **Zero Trust model** states that there is no inherent trust in any applications, users, or networks even if they are within the corporate network.
- According to the research, it is recommended to use several factors at once to authenticate the cloud, use the principle of least authority and perform constant monitoring.
- ZTA also reduces the threats posed by other risks like insiders and others who can easily gain unauthorised access.

❖ **Encryption and Data Protection**

- **End-to-end encryption (E2EE)** ensures that sensitive data remains protected both at rest and in transit.
- Homomorphic encryption concept enables computations on encrypted data and does not reveal the actual information.
- The rules like PCI DSS contain requirements for encryption to safeguard the data of financial records.

❖ **Identity and Access Management (IAM)**

- IAM solutions dictate how much power a user has, and they can limit the amount of access granted to him/her depending on the role assigned.
- Some focus is given to adaptive authentication since the system assesses the behavior of users to identify any deviations from the norm.
- Insurers adopt the use of biometric authentication and password less authentication solutions for the purposes of security.

❖ **Cloud Security Posture Management (CSPM)**

- By the means of using CSPM it is easy to discover misconfigurations, control and enhance compliance with specific policies, and carry out security audit in a more efficient manner.
- The consultants opine that the outlook for CSPM is positive, and more organisations will implement the tool as a preventive solution to numerous cloud attacks.

❖ **Security Information and Event Management (SIEM)**

- SIEM solutions deal with the combination of the collected security logs for the identification and execution of the security threats in real-time.
- numerous sources confirm that incorporating the SIEM solutions with the support of artificial intelligence can enhance threat intelligence as well as automate the processes of incident handling.

❖ **Compliance as Code (CaC)**

- In CaC, compliance controls are incorporated into automated cloud security policies, and there is less chance of human inkling and tremendously consistent compliance.
- Some of these are Sentinel from HashiCorp, and AWS ECS. Insurers can use these in governing compliance in Cloud Native Infrastructures.

If implemented in unison, these strategies provide a strong layered security solution to improve data security and the satisfaction of regulations when it comes to insurance applications developed in the cloud-native environment.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Regulatory Requirements for Cloud Computing in Insurance: Overview of Relevant Laws and Regulations

The insurance industry is supervised strictly to regulate collection and security of customers' information and to ensure appropriate financial handling mechanisms. The emergence of the Cloud has, therefore, brought in new compliance issues, which insurers must address from a geographical and sector perspective.

❖ **General Data Protection Regulation (GDPR) – European Union**

- GDPR requires data protection measures, the consent, and the right of subjects to be forgotten for the citizens of the EU.
- Consumer rights should also be protected, get breach notification within 72 hours of the incident, and uncertainties about cross-border data transfer.

❖ **Health Insurance Portability and Accountability Act (HIPAA) – United States**

- HIPAA being an attempt to regulate the industry addresses situations involving insurers that deal with PHI information.
- Entails data encryption, restricted access to data, paperwork, and security check-ups to minimise on leakages.

❖ **Sarbanes-Oxley Act (SOX) – United States**

- Mainly used to protect the shareholders' interests of shareholders in public held insurance firms.
- Requires **audit trails, data retention policies, and strict access controls** to prevent fraud.

❖ **Payment Card Industry Data Security Standard (PCI DSS)**

- Regulates the usage of credit cards in the insurance payments.
- Makes new requirements for implementation of principles of encryption; access control; network and system monitoring by insurers.

❖ **California Consumer Privacy Act (CCPA) – United States**

- Empowers Californians to manage their personal data and make insurers report the data collection process.
- Evaluating conformity penalties, there are coupled steep fines and penalties for non-compliance.

❖ **Insurance Industry-Specific Compliance Standards**

- NAIC Model Laws are guidelines acknowledged by U.S. insurers that refer to the security of companies' data.
- Cloud computing solvency II directive in the EU has directed that insurers should implement adequate risk management measures on cloud aspects.

Key Compliance Challenges:

- Data localization mandates that the data of insurers must remain within those countries, and this poses a challenge for the efficient use of cloud services around the world.
- Over the years there has been a lot of changes in regulations hence requires constant changes in methods of compliance.
- The insurance industry requires compliance assessment of third-party vendors to check that cloud providers are in harmony with the required set standards.

METHODOLOGY

Cloud Security Challenges in Life And Annuities Insurance

The life and annuities insurance depend largely on data as they require large volumes of customer information that includes PII, customer's financial details and health records. The change towards more cloud-native approach improves the organizational effectiveness but creates substantial security concerns. This section discusses the risks that are unique to the insurer in relation to the cloud computing environment.

Data Breaches and Cyber Attacks

It has established that data breaches are among the severe risks that affect cloud systems. The insurance firm industry entails handling significant amounts of valuable data – this put the firm in an unusually risky location for cyber attackers. Challenges associated with cloud-based infrastructure are as follows:

- **Unauthorized Access:** Poor methods of identification and insecure cloud parameters pose risks of the misappropriation of necessarily sensitive information.
- **Malware and Ransomware Attacks:** Cyber attackers break into cloud networks and install malware that encryptions customer's data and then demand for a ransom to unlock it.
- **Insider Threats:** These include employees of the firm as well as other third parties who have authorised access to the company's network and data may leak the information intentionally or through negligence.

Example: Flagstar Bank – an insurance service provider company – had about 1.5 million customers impacted by a data breach in 2021 after the cloud's misconfiguration.

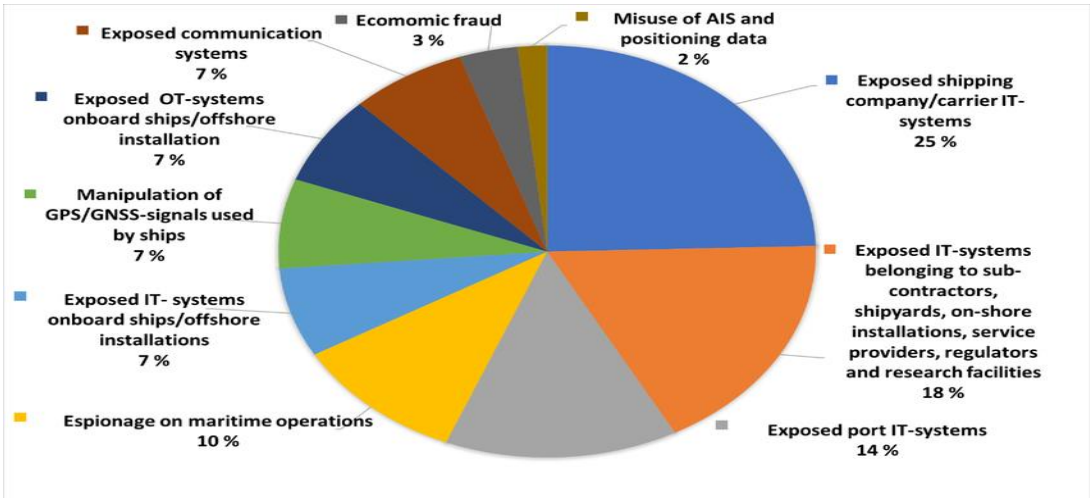

Figure 2: Common Cloud Security Threats in Insurance

Mitigation Strategies:

- Locker at the user level – There should not be any assumption of trust on either the users or the devices as you adopt ZTA.
- Encrypt your data at the sharing stage and at the storage stage to add security at the different stages of data flow.
- Utilize Intrusion Detection and Prevention Systems (IDPS) to perform vigilance and ensure that prolific activities are kept at bay.

Compliance with Regulatory Requirements (e.g., GDPR, HIPAA)

Insurance fields interact with various regulations according to the place where such companies operate. The following reasons explain why compliance becomes more challenging to achieve in the cloud environments:

- **Data Residency and Sovereignty Issues:** In line with GDPR for example, it is mandatory that customer's data be located within certain boundaries, this is an issue for cloud-based storage.
- **Third-Party Compliance:** CSPs are required to firstly meet legal standards; however, insurers are always liable for compliance.
- **Dynamic Regulatory Changes:** The compliance rule which is pertinent to the environment change often necessitates frequent changes in the laws which in turn put pressure on the insurers to constantly update their security policies.

Key Regulations:

Regulation	Region	Requirement
GDPR	EU	Data protection, confidentiality of data, obtaining consent from the users, notification of any data breach not later than seventy-two hours.
HIPAA	US	Protection of health-related data, strict access control
PCI DSS	Global	Secure handling of payment transactions
CCPA	US (California)	Consumer data privacy rights and transparency

Mitigation Strategies:

- Schedule a check for compliance regulation through Compliance as Code (CaC).
- Conduct monthly audits and integrate an outside-in type of risk evaluation process.
- Partner with cloud providers that can provide certifications such as ISO 27001, SOC 2 etc.…

Ensuring Data Privacy and Confidentiality

Preserving the rights of data involves all spheres of insurance as policyholders surrender their financial, health or other privately owned information to the insurance companies. There are several privacy risks that has been posed by cloud environments:

- **Unsecured APIs:** Most unsecured APIs, expose the confidential information to the external parties due to poor API configuration.
- **Multi-Tenancy Risks:** When the cloud architecture accommodates multiple users or companies, there are higher chances of cross-sharing of information.
- **Cloud Service Provider (CSP) Access:**There is also the problem of some CSPs gaining access to the customer data and processing it in some way.

Mitigation Strategies:

- Deploy **Privacy-Enhancing Technologies (PETs)** such as **homomorphic encryption** and **secure multi-party computation**.
- To address this issue, ensure that you implement measures against Data Loss Prevention (DLP) to prevent the unauthorized transfers of any information.
- However, for secure identification across cloud services adoption of federated identity management (FIM) should be done.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Managing Identity and Access Control

That is why one of the major issues of cloud-native environments is to give permission to access critical systems and applications to specific users only. Some of the repercussions of such negative approaches are as follows:

- **Account Takeovers:** Attackers will use several acquired credentials and unguarded passwords to compromise an account.
- **Excessive User Privileges:** Any employee, with a full access to specified system may be a dangerous character if his/her login details get into wrong hands.
- **Lack of Centralized Identity Management:** IT administrators of various insurance companies have not had a single point that would allow them to control access rights as well as revoke them.

Mitigation Strategies:

- Adopt IAM solutions together with the RBAC model.
- MFA should be adopted alongside other means of authentication like biometric instead of passwords.
- Implementing PAM tools to reduce the amount of access to cloud systems for administrators.

Table 1: Cloud Security Challenges in Life and Annuities Insurance

Security Challenge	**Description**	**Mitigation Strategies**
Data Breaches & Cyber Attacks	Unauthorised access, ransomware, insider threats	Zero Trust Architecture, encryption, Intrusion Detection Systems
Regulatory Compliance	Complex, evolving global regulations (GDPR, HIPAA, PCI DSS)	Compliance automation, audits, third-party risk management
Data Privacy & Confidentiality	API vulnerabilities, multi-tenancy risks, CSP access issues	Privacy-enhancing technologies, Data Loss Prevention (DLP), federated identity management
Identity & Access Control	Account takeovers, excessive privileges, lack of centralized management	IAM frameworks, MFA, role-based access control (RBAC)

As the life and annuities insurance department starts adopting cloud-native structures, it can face various security and compliance issues. Security issues like data breaches,

compliance, privacy, and identity are still imminent. It is, therefore, paramount for the insurers to adopt and apply stringent security frameworks, encrypting IAM solutions, and compliance automation to improve the protection, regulation, and customers' trust in cloud solutions.

RESULT/FINDINGS

Best Practices for Cloud-Native Security And Compliance

Based on this, there is a need to adopt updated security models in conducive support of cloud native infrastructures in the life and annuities insurance industries. They assist in establishing a broad range of customers' data protection and the achievement of the industry standards, as well as come down with the risks of cyber hacking.

Implementing a Cloud Security Architecture

A cloud security architecture should be such a design that is useful for the protection of insurance data and compliant with these laws. It must be initiated as an executive security framework where control and a monitoring program for countering cyber threats exist.

These then reveal the following potential attributes of the cloud security architecture:

- **Zero Trust Security Model (ZTA): Is** stricter in authenticating and authorising the user and all the devices that require the cloud interface since it operates under the Zero Trust Architecture (ZTA).
- **Micro-Segmentation:** It entails further division of the cloud environment to minimize adversary movement when they penetrate the network.
- **Security Information and Event Management (SIEM):** These are used for real-time monitoring of security to ensure that security breaches, unauthorised accesses, etc. are detected as soon as they are happening.
- **Cloud Access Security Brokers (CASB):** It ensures the security policies and compliance, and data security related issues will be implemented in cloud services.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

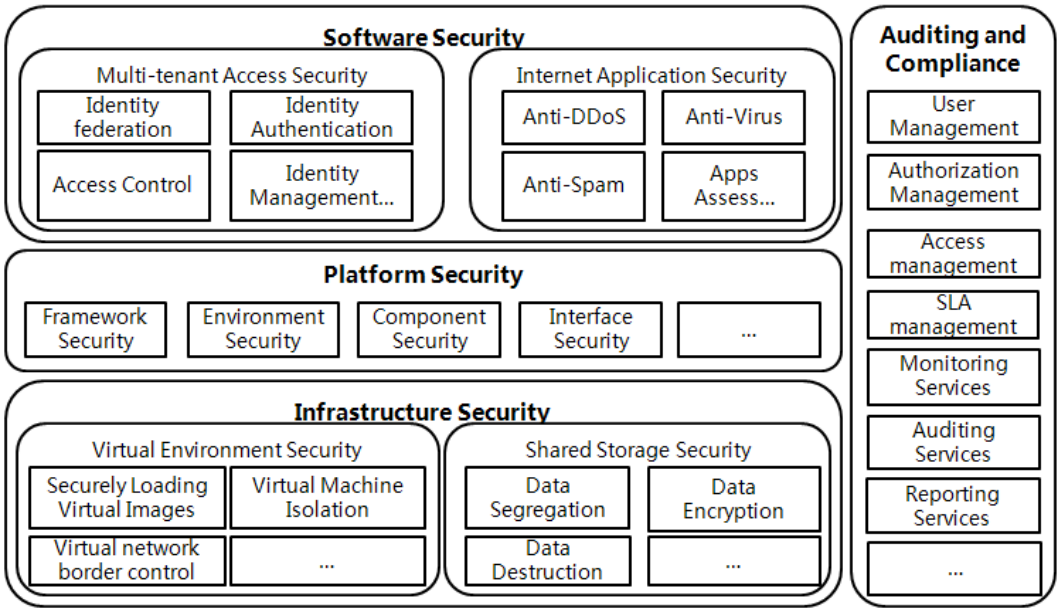

Figure 3: Cloud security architecture diagram

Implementation Strategies:

- Several levels of security address the issues with firewalls, encryption and the endpoint protection.
- Lastly, guarantee of Network Access with secure through application of Secure Access Service Edge (SASE).
- It is necessary to remember that the policies of security in the cloud level should be updated from time to time based on the provisions of the ISO 27001 and NIST-CSF guidelines.

Conducting Regular Security Audits and Risk Assessments

Security audits and risk assessment are important as the organisation must be aware of its vulnerabilities of the infrastructures it uses in the cloud and see to it that the cloud infrastructures do not contravene any laws.

Importance of Security Audits:

- This will assist to identify the various misconfigurations as well as the numerous attempts on the system.
- Also, it meets GDPR, HIPAA, and PCI DSS standards of compliance.
- Helps insurance firms in developing the plans for dealing with situations that may result to a breach.

Risk Assessment Methodologies:

- **Vulnerability Scanning:** The detection of the cloud applications and the network's weaknesses, where one can easily sneak in with a breach.
- **Penetration Testing:** Simulates cyber-attacks to test system resilience.
- **Third-Party Security Audits:** Engage the third-party security suppliers for the evaluation of the compliance and level of security.

Implementation Strategies:

- The Security Posture Management (CSPM) tools should be used to automate checks for compliance.
- Include other security providers for the evaluation on the level of compliance and security.
- Have and utilize encompassing papers in the event a legal review or probe is conducted.

Ensuring Data Encryption and Key Management

The topic of data encryption is still up to date as it can contribute to a decrease in the number of cases related to unauthorised access to the clients' information, particularly in the context of the Multiload and Hybrid cloud solutions. This means that in their bid to work under the laws of data protection, insurers are most probably on the receiving end and be arraigned as their information is purloined by hackers.

Types of Cloud Encryption:

- **Data at Rest Encryption:** To enhance the security of the firm, it protects stored data through Advanced Encryption Standard 256 bits, to ensure that unauthorised persons cannot access the information.
- **Data in Transit Encryption: Protect** data in transit across the user's applications and cloud applications through Transport Layer Security/Secure Socket Layers encryption.
- **End-to-End Encryption (E2EE):** It is the arrangement of making an information inaccessible to everyone in the communication system apart from the sender and the intended recipient.

International Journal of Interdisciplinary Research Methods
Vol.12, No.1, pp.50-73, 2025
Print ISSN: ISSN 2398-712X,
Online ISSN: ISSN 2398-7138
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

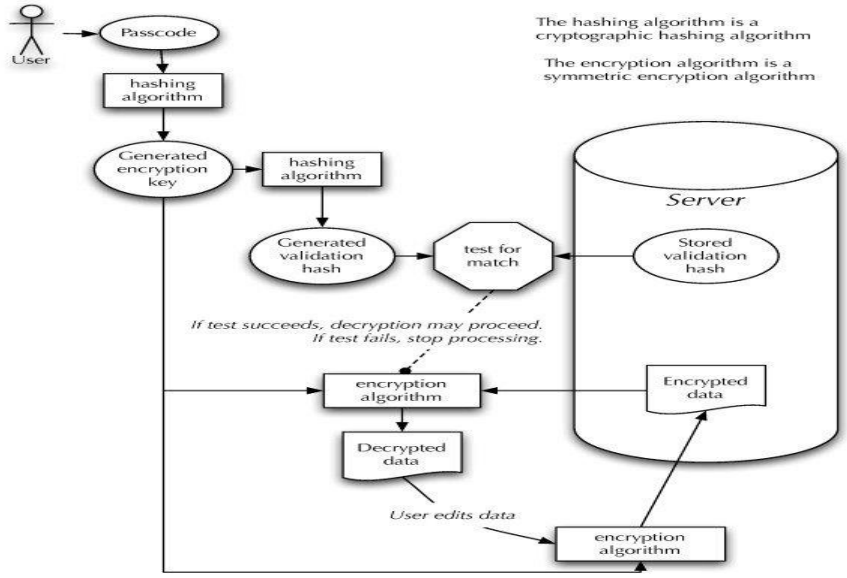

Figure 4: Data Encryption Lifecycle

Key Management Best Practices:

- For the generation and storage of the encryption key, cryptographic management with the help of HSMs should be adopted.
- Assure the implementation of the best practices of the industry of management systems key (AWS KMS, Google Cloud KMS)
- To protect the keys, it is recommended that the use of RBAC is made to regulate access to such keys.

Implementation Strategies:

- BYOK policies should be adopted to retain control of encryption keys, as they will help the organisations.
- The main advice that should be given to reduce the risk of intrusion is to advise the management to frequently change the keys used in encryption.
- Encrypt the rover at the object storage level using the tools that are offered by the cloud provider, for example, AWS S3 SSE.

Implementing Identity and Access Management (IAM) Solutions

IAM is a contract explicitly of the utmost importance in cloud computing since it is used to guarantee that only permitted customers and clients can access important cloud applications and customer information. The violations of IAM can lead to account

takeovers, internal threats, and noncompliance. This affects the organisation and its clients extremely.

Key IAM Security Measures:

- **Multi-Factor Authentication (MFA):** Requires additional authentication layers (e.g., biometric scans, OTP codes).
- **Role-Based Access Control (RBAC):** This refers to the ability of an organisation to make security decisions through the role that different users play in an organisation.
- **Privileged Access Management (PAM):** This service minimizes the access which is granted to the cloud accounts which are known to be at risk to the organization.
- **Federated Identity Management (FIM): It** allows the insurers to apply SSO across the many cloud services.

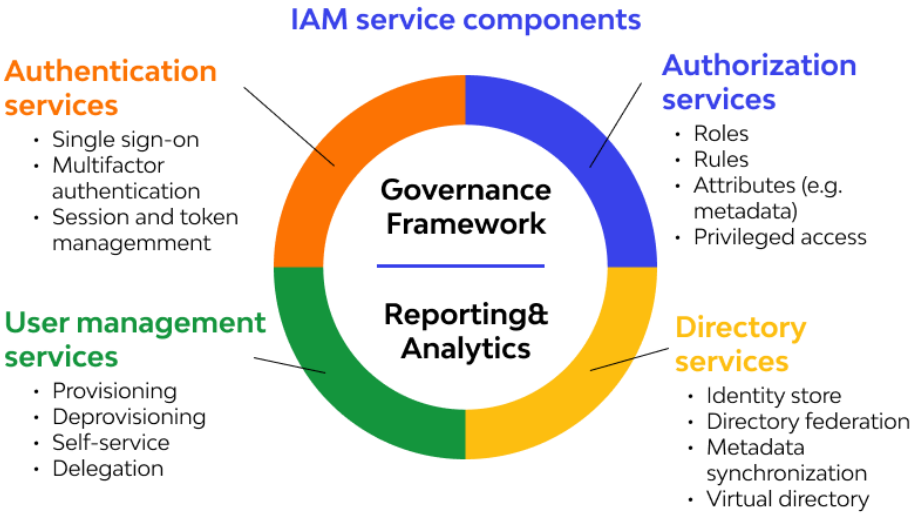

Figure 5: IAM Framework for Insurance Cloud Systems

Implementation Strategies:

- Another security control deal with the rotation of the account credential in the organisation and as much as possible, the privilege granted to more users should be restricted to the least privilege level required for the holding of their respected positions with a view to minimising the probability of authorization of access.
- To eliminate such activities that may seem like an attempt to log in in the wrong way, it is recommended to integrate adaptive authentication.

- Always incorporate IAM in the cloud software like AWS IAM, Azure AD, Google Cloud IAM, as a way of applying the user authentication naturally.

Therefore, to ensure the security of cloud-native environments, life and annuities insurers should focus on the efficiency of security architecture, cloud security checks, encryption solutions, IAM solutions, and data protection. These strategies reduce the risks of cybercrimes, enhance compliance, and provide the client with much-needed confidence in the online insurance services.

DISCUSSION

Case Studies: Cloud Security Strategies in Life And Annuities Insurance

The implementation of cloud-native security in the life and annuities insurance industry varies among companies based on risk exposure, regulatory requirements, and technological investments. This section presents two case studies of insurance companies that have successfully deployed cloud security strategies to protect sensitive customer data and comply with regulatory frameworks.

Case Study 1: Prudential Financial – Cloud Security Strategy and Implementation

Background

Prudential Financial, a leading life insurance and annuities provider, undertook a cloud migration strategy to enhance scalability, customer experience, and operational efficiency. The transition to Microsoft Azure and AWS introduced new security challenges, requiring a robust cloud security framework.

Cloud Security Strategy

- **Zero Trust Security Framework:** Implemented strict identity verification policies for users and devices accessing cloud resources.
- **Data Encryption at Rest and in Transit:** Deployed AES-256 encryption and TLS 1.3 protocols to secure sensitive customer information.
- **Cloud Access Security Broker (CASB):** Monitored cloud data movement and prevented unauthorised file sharing.
- **Automated Compliance Audits:** Integrated AI-driven compliance checks to adhere to GDPR, PCI DSS, and HIPAA.
- **Multi-Factor Authentication (MFA):** Enforced biometric authentication and adaptive access controls.
- **Incident Response Automation:** Used Security Information and Event Management (SIEM) for real-time threat detection and mitigation.

Results

- 35% reduction in security breaches through enhanced identity and access controls.
- Improved compliance efficiency, reducing audit costs by 40%.
- Faster threat response, detecting and mitigating malware attacks within minutes.

Case Study 2: MetLife – Cloud Security Strategy and Implementation

Background

MetLife, a global insurance provider, migrated to a hybrid-cloud model, leveraging Google Cloud Platform (GCP) and AWS for data storage and policy management. Given the company's regulatory exposure across multiple jurisdictions, a multi-layered security approach was necessary.

Cloud Security Strategy

- **Micro-Segmentation & Network Isolation:** Used virtual private clouds (VPCs) to separate critical workloads and prevent lateral attacks.
- **End-to-End Encryption with Bring Your Key (BYOK):** Allowed full control over encryption keys, ensuring customer data sovereignty.
- **Cloud-Native Security Analytics:** Integrated Google Chronicle Security Operations for AI-driven threat intelligence.
- **Privileged Access Management (PAM):** Restricted administrative rights with just-in-time (JIT) access policies.
- **Automated Patch Management:** Used AI-driven vulnerability detection to deploy security patches without downtime.
- **Regulatory Compliance as Code (CaC):** Automated compliance checks for SOX, CCPA, and GDPR.

Results

- 50% decrease in unauthorised access attempts through PAM implementation.
- Improved cloud security visibility, reducing response time to cyber threats by 60%.
- Higher customer trust due to strong privacy and compliance measures.

Table 2: Comparison of Cloud Security Strategies in Case Studies

Security Measure	Prudential Financial	MetLife
Cloud Provider	Microsoft Azure, AWS	Google Cloud, AWS
Security Framework	Zero Trust, CASB, SIEM	Micro-Segmentation, PAM, AI-driven Security
Data Encryption	AES-256, TLS 1.3	End-to-End Encryption, BYOK
Identity & Access Management	MFA, Adaptive Access Control	JIT Access, Privileged Access Management
Compliance Strategy	Automated Compliance Audits	Compliance as Code (CaC)
Threat Detection	Incident Response Automation	AI-driven Threat Intelligence
Results	35% reduction in security breaches, 40% lower audit costs	50% fewer unauthorized access attempts, 60% faster response time

Both Prudential Financial and MetLife have implemented comprehensive cloud security measures to protect customer data and meet compliance standards. While Prudential focused on Zero Trust Architecture and compliance automation, MetLife leveraged AI-driven security analytics and privileged access controls. These case studies highlight how advanced cloud security strategies enhance data protection, regulatory adherence, and operational efficiency in the life and annuities insurance industry.

Implication To Research and Practice

The adoption of cloud-native security tools for life and annuities insurance affects both research studies and industry practice development. Our latest research approach shows how security designs in enterprise meet cloud systems under regulatory controls. Research can explore safe development practices and trust-based protection systems, plus write-compliant standards into actual implementation for insurance-sector rules.

Insurers can adapt their security system quickly through this data to create better protection while effectively meeting new industry rules. Cloud-native techniques help organizations deploy insurance policies faster plus run continuous risk checks while their teams work successfully between underwriting claims and compliance divisions. Research-practice collaboration produces important insights that show how evidence-driven security solutions should be introduced to digital insurance systems.

CONCLUSION

Security and compliance in the cloud environments are essential when it comes to protecting customers' information as well as staying afloat with the regulations prevalent in the life and annuities insurance sector. Taking this into consideration, it is

equally important to capture the different types of issues that arise when insurers opt to move their systems to the cloud.

Such risks can be addressed effectively using security benchmark strategies such as Zero Trust security, encryption of data, audits, and identity management solutions. This paper provides examples of insurance companies to show that preventive measures and risk analysis based on artificial intelligence strengthen data protection and adherence to the regulations.

In the prospects, it is crucial for the insurance industry to enhance security further and to adopt innovative approaches like automation, threat intelligence, as well as modern compliance practices to cope with the specified threats. Secure cloud will not only help to guard the customers' trust but also will be the key to business sustainability in the environment of the digital threat.

Future Research

Our research shows necessary security methods and design models for cloud-native life and annuities work, but we still need to conduct new explorations. Research should measure how much more or less organizations will spend when moving systems to cloud-native versus their current setup. Empirical tests that examine how insurers adopt cloud technologies together with regulatory changes and cloud vendor risk can help all participants achieve better results.

The effectiveness of computer systems in monitoring compliance standards and finding threats needs extensive research examination. Research projects that check privacy rules between different nations will improve academic understanding and make global implementation easier.

REFERENCES

Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. (2017, November). Leveraging cloud native design patterns for security-as-a-service applications. In *2017 IEEE International Conference on Smart Cloud (SmartCloud)* (pp. 90-97). IEEE https://doi.org/10.1109/SmartCloud.2017.21

Chung, S. M., Shieh, M. D., & Chiueh, T. C. (2019, November). A SaaS-native wildcard searchable encryption scheme for protecting privacy in cloud services. In *2019 IEEE 5th International Conference on Big Data Intelligence and Computing (DATACOM)* (pp. 178-184). IEEE. https://doi.org/10.1109/DataCom.2019.00035

Vadlamudi, S., & Sam, J. (2021, November). A Novel Approach to Onboarding Secure Cloud-Native Acquisitions into Enterprise Solutions. In *2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON)* (Vol. 1, pp. 228-233). IEEE. https://doi.org/10.1109/CENTCON52345.2021.9688193

Paxton, N. C. (2016, November). Cloud security: a review of current issues and proposed solutions. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)* (pp. 452-455). IEEE. https://doi.org/10.1109/CIC.2016.066

Jayakody, J. A. D. C. A., Perera, A. K. A., & Perera, G. L. A. K. N. (2019, December). Web-application security evaluation as a service with cloud native environment support. In *2019 International Conference on Advancements in Computing (ICAC)* (pp. 357-362). IEEE. https://doi.org/10.1109/ICAC49085.2019.9103414

Alm, J. (2019). What motivates tax compliance?. *Journal of economic surveys*, *33*(2), 353-388. https://doi.org/10.1111/joes.12272

Sandoval-Norton, A. H., Shkedy, G., & Shkedy, D. (2019). How much compliance is too much compliance: Is long-term ABA therapy abuse?. *Cogent Psychology*, *6*(1), 1641258. https://doi.org/10.1080/23311908.2019.1641258

Hu, X., Yeo, G., & Griffin, M. (2020). More to safety compliance than meets the eye: Differentiating deep compliance from surface compliance. *Safety science*, *130*, 104852. https://doi.org/10.1016/j.ssci.2020.104852

Loibl, G. (2021). Compliance procedures and mechanisms. In *Research handbook on international environmental law* (pp. 293-319). Edward Elgar Publishing. https://doi.org/10.4337/9781786439710.00021

Kalfa, S., Wilkinson, A., & Gollan, P. J. (2018). The academic game: Compliance and resistance in universities. *Work, employment and society*, *32*(2), 274-291. https://doi.org/10.1177/0950017017695043

Alpman, B., & Ünal, D. (2020). Accelerating the premiums for annuities, life annuities and life insurance. *Communications in Statistics-Theory and Methods*, *49*(7), 1665-1694. https://doi.org/10.1080/03610926.2018.1564329

Ezra, D. (2016). Most people need longevity insurance rather than an immediate annuity. *Financial Analysts Journal*, *72*(2), 23-29. https://doi.org/10.2469/faj.v72.n2.3

Shoeb Ali Syed. (2022). AI-POWERED CYBERCRIME: THE NEW FRONTIER OF DIGITAL THREATS. International Journal of Engineering Technology Research & Management (IJETRM), 06(02). https://doi.org/10.5281/zenodo.15128508

Ramsay, C. M., & Oguledo, V. I. (2018). The annuity puzzle and an outline of its solution. *North American Actuarial Journal*, *22*(4), 623-645. https://doi.org/10.1080/10920277.2018.1470936

Dzingirai, C., & Chekenya, N. S. (2020). Longevity swaps for longevity risk management in life insurance products. *The Journal of Risk Finance*, *21*(3), 253-269. https://doi.org/10.1108/JRF-05-2019-0085

Kintzel, D., & Turner, J. A. (2020). Provision of Longevity Insurance Annuities. *Financial Analysts Journal*, *76*(4), 119-133. https://doi.org/10.1080/0015198X.2020.1809903

Gai, K., Qiu, M., & Hassan, H. (2017). Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. *Concurrency and Computation: Practice and Experience*, *29*(7), e3856. https://doi.org/10.1002/cpe.3856

Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing. In *2016 IEEE 3rd international conference on cyber security and cloud computing (CSCloud)* (pp. 295-300). IEEE. https://doi.org/10.1109/CSCloud.2016.46

Liu, W., Yu, Q., Li, Z., Li, Z., Su, Y., & Zhou, J. (2019, December). A blockchain-based system for anti-fraud of healthcare insurance. In *2019 IEEE 5th International Conference on*

Computer and Communications (ICCC) (pp. 1264-1268). IEEE. https://doi.org/10.1109/ICCC47050.2019.9064274

Elnagdy, S. A., Qiu, M., & Gai, K. (2016, June). Cyber incident classifications using ontology-based knowledge representation for cybersecurity insurance in financial industry. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 301-306). IEEE. https://doi.org/10.1109/CSCloud.2016.45

Gai, K., Qiu, M., & Elnagdy, S. A. (2016, April). A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 171-176). IEEE. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.65

Sony, M., & Naik, S. (2020). Industry 4.0 integration with socio-technical systems theory: a systematic review and proposed theoretical model. *Technology in society*, *61*, 101248. https://doi.org/10.1016/j.techsoc.2020.101248

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, *25*(2), 196-208. https://doi.org/10.1108/JFRC-08-2016-0068

Diel, K., Grelle, S., & Hofmann, W. (2021). A motivational framework of social comparison. *Journal of Personality and Social Psychology*, *120*(6), 1415. https://psycnet.apa.org/doi/10.1037/pspa0000204

Machireddy, J. (2022). Data Analytics in Health Insurance: Transforming Risk, Fraud, and Personalized care. *Fraud, and Personalized care (June 01, 2022)*. https://dx.doi.org/10.2139/ssrn.5159635

Larson, D. B., Harvey, H., Rubin, D. L., Irani, N., Tse, J. R., & Langlotz, C. P. (2021). Regulatory frameworks for development and evaluation of artificial intelligence–based diagnostic imaging algorithms: summary and recommendations. *Journal of the American College of Radiology*, *18*(3), 413-424. https://doi.org/10.1016/j.jacr.2020.09.060

Machireddy, J. R. (2021). Data-Driven Insights: Analyzing the Effects of Underutilized HRAs and HSAs on Healthcare Spending and Insurance Efficiency. *Journal of Bioinformatics and Artificial Intelligence*, *1*(1), 450-469.

Zhang, D., Hussain, A., Manghwar, H., Xie, K., Xie, S., Zhao, S., ... & Ding, F. (2020). Genome editing with the CRISPR-Cas system: an art, ethics and global regulatory perspective. *Plant biotechnology journal*, *18*(8), 1651-1669. https://doi.org/10.1111/pbi.13383