iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

ENHANCING CLOUD SECURITY AND COMPLIANCE

Goutham Bilakanti
Senior Data Engineer

ABSTRACT
AWS cloud-based solutions are transforming healthcare infrastructure by providing secure data storage, rigid compliance with rigorous healthcare laws like HIPAA and GDPR, and simple interoperability of electronic health records (EHRs). Utilizing AWS cloud security best practices like multi-layered encryption mechanisms, intrusion detection mechanisms, and access controls improves data confidentiality, integrity, and availability. Furthermore, AWS enables scalable and secure healthcare applications with the help of automated backup, disaster recovery processes, and machine learning-based threat detection patterns for minimizing security threats. Cloud solutions enable healthcare organizations to automate operations, minimize costs, and maximize patient data availability with appropriate regulatory compliance. AWS Identity and Access Management (IAM), network firewalls, and real-time security monitoring tools further enhance cloud security architecture for healthcare organizations. Implementation of serverless computing and containerized architecture in AWS improves the scalability, efficiency, and resiliency of applications to provide unintermitted delivery of services. In addition, AWS cloud analytics provide health professionals with real-time insights for predictive modeling, patient monitoring, and clinical decision-making. AWS contribution to revolutionizing healthcare data management is addressed in this paper through alleviating security threats, regulatory compliance, and interoperability challenges, providing a secure and compliant cloud environment.

Keywords:
AWS cloud solutions, security for healthcare, HIPAA, GDPR, electronic health records, encryption methods, disaster recovery, cloud interoperability, real-time security monitoring, AI-based threat detection.

I. INTRODUCTION

Cloud computing has revolutionized healthcare infrastructure with the ability to provide scalable, cost-effective, and secure data storage for confidential medical information. Amazon Web Services (AWS), being among the largest cloud providers, has been a forerunner in this revolution with superior security, compliance frameworks, and high-volume data management capabilities. Healthcare facilities also rely more and more on AWS to protect data storage as securely as is practicable, to satisfy rigorous regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), and to ensure interoperability of electronic health records (EHRs) with ease [1] [5] [12].

Security and compliance are some of the high-priority aspects of AWS cloud solutions for healthcare. AWS provides several levels of security monitoring controls, identity and access management (IAM), and encryption to protect the patient data from unauthorized users and attackers [4] [6] [10]. AWS security best practices like real-time threat detection, network segmentation, and multi-factor authentication (MFA) are some additional security features for risk reduction and data protection [14] [16]. These initiatives have the fundamental purpose of helping healthcare organizations evade risk because of data breaches and cyber-attacks and staying current with new industry standards. Apart from security, AWS cloud services provide disaster recovery capabilities to provide high availability and business continuity to healthcare providers. With the capability of automated failover, geographically remote data centers, and automated backup, AWS allows organizations to recover vital data rapidly in case of system failure or cyber-attack [7] [8] [9][11][14]. Such capability is of paramount significance in ensuring uninterrupted access to patient records and sustaining healthcare services during trying times. Besides that, AWS cloud services provide EHR interoperability that supports simple data sharing among many healthcare providers and systems. With analytics driven by machine learning, standardized APIs, and automation driven by AI, AWS makes it simpler to collaborate among health stakeholders in care and thereby attain improved patient outcomes and efficient operations [2] [3] [9]. Besides, integration of AWS with predictive analytics technology streamlines clinical decision-making through identification of disease patterns,

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

improvement of treatment protocols, and avoidance of early diagnosis mistakes [15] [16]. With the adoption of digital transformation by healthcare organizations, AWS cloud services lead the way with innovation through scalable, secure, and compliant solutions that automate healthcare processes. By adopting AWS best practices for disaster recovery policy and encryption policy, as well as security, health organizations will achieve safe storage of private medical information and enhanced efficiency and patient care. This paper gives the contribution of AWS in enhancing the security, compliance, and interoperability of the cloud in healthcare systems and why it is important to secure sensitive health data and build digital healthcare projects [1] [4] [7] [12] [19][20]

II.LITERATURE REVIEW

Bracci et al. (2012): Provided evidence of database security administration within the health Software-as-a-Service (SaaS) environment, with significant focus on Amazon AWS Cloud. Their paper summarizes the necessity to protect electronic health records through robust authentication and encryption technologies. They focused on access control and audit control that ensures compliance with healthcare data protection laws. Their research also tested problems in multi-tenant cloud environments based on security violation due to shared resources. Their research is a contribution to healthcare cloud security architecture studies. The paper is an application-oriented suggestion for safe guarding of confidential patients' information without compromising the system's reliability and functionality [1].

Malaiyappan et al. (2024): Explored machine learning-powered cloud compliance models for strengthening cloud compliance with regulations. Their work put forward a novel method that employs predictive analytics for sweeping through future compliance threats prior to compromising them. They explored the application of AI frameworks for policy enforcement automation for facile compliance across different cloud infrastructures. Their research also emphasized that AI-based auditing tools should be integrated to prevent data breaches while identifying abnormalities. Based on their work, AI enhances security, efficiency, and transparency in cloud regulatory compliance. This paper offers a futuristic vision of cloud security through intelligent automation [2].

Prakash et al. (2024): Illustrated that machine learning compliance of cloud computing relies on policy compliance and risk analysis automation. Based on their study, AI-based monitoring systems continuously monitor compliance with regulation like GDPR and HIPAA. They have characterized the way in which machine learning models can flag non-compliance breach and propose remediation actions in real time. In addition, the research brought to the forefront the use of AI models combined with cloud security software to forecast threats. Their research brings forth the way in which AI reduces human mistakes in compliance management and response time for security violations. The article is important because it brings to the forefront the application of AI in current cloud governance processes [3] [18].

Polamarasetti (2024): Have done research in artificial intelligence and machine learning for the benefit of cloud security. Their research included AI-driven intrusion detection systems which can identify and respond to cyber-attacks autonomously in real-time. They have done research on how AI-driven anomaly detection models can avert unauthorized access and identify potential vulnerabilities beforehand before they are exposed. Additionally, the research found how artificial intelligence-based encryption mechanisms provide data integrity and confidentiality in cloud use. From the research, it is revealed that AI gives a boost to security levels of cloud computing through automated processes used in the battle against threats. All these facts are being utilized while building robust models of cloud security [4].

Valluripally et al. (2019): Proposed a community cloud model to ensure increased security compliance and improved data accessibility in healthcare systems. They presented a decentralized model with the potential of multiple healthcare organizations to safely share data in a high-regulatory compliance environment. They elaborated that blockchain and AI-based encryption mechanisms can fight multi-party access threats to data. Besides, the study concentrated on the benefits of federated learning in data privacy while not undermining collaborative health research. Based on their study, community models of the cloud can be used to enhance security and effectiveness in the processing of health data. The article offers a practical solution in the provision of the harmony between data sharing and high levels of security [5].

Jimmy (2023): Evaluated cloud security posture management solutions and methodologies from the application of AI to detect and manage security threats. They compared the automated vulnerability scanning frameworks used to identify misconfigurations in cloud infrastructure. They also experimented with the use of AI-based

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

behavioral analytics to identify user behavior and insider threat prevention. Furthermore, the research also elucidated how using AI-based risk prioritization techniques can facilitate quicker security processes. Their research depicts how AI improves threat detection efficacy with improved response time for cloud security management. It is wonderful reading on high-level cloud security processes through AI [6].

Devi and Jain (2024): Created intrusion detection systems using deep learning for securing the cloud by utilizing AI to respond against cyber-attacks. The study is an extension of how real-time anomaly detection systems can effectively prevent and detect malicious activity in clouds to possess strong security controls. The research also shows the need for training deep models on large data sets so that the detection rate is enhanced. It also shows the need for adaptive algorithms so that they react favorably to new cyber-attacks. The research also suggests the challenge of implementation in terms of computational costs and data privacy. All these results are a solid foundation for future research for AI-based cloud security systems [7].

Naik (2023): Analyzed cloud data governance from the security, compliance, and privacy points of view to prevent risk involved in managing data. The study also addresses regulating frameworks that guide cloud security policy in helping companies stay compliant with laws. The study also offers encryption and multi-factor authentication to provide security in protecting data. The study also investigates privacy-preserving solutions like differential privacy and secure multi-party computation. The study highlights the importance of a good governance model in safeguarding sensitive data. The study can be applied to organizations that are interested in developing data governance processes for cloud systems [8].

Aturi (2024): Conducted research on leadership and governance challenges in global non-profit organizations, focusing on strategic decision-making through data analytics application. The study confirms how data intelligence can improve policy development and optimize the use of resources for the non-profit industry. It also analyzes the effects of legal and regulatory limitations on firm performance, promoting ethical leadership models. Moreover, the study includes the use of AI in forecast trends and campaign performance improvement. The article recommends a combination of governance pillars and data analysis to increase transparency and responsibility. Such evidence is crucial for policymakers looking to improve governance strategy in international organizations [9].

Deshpande et al. (2023): Conducted a cryptographic study with the purpose of improving cloud security with focus on emerging encryption methods. The work explains how hybrid encryption methods improve data confidentiality without sacrificing low computational overhead. The study also cites post-quantum cryptography as a possible path to counter the soon-to-be quantum computing attack threat. The study also investigates key management methods required to safeguard cloud environments from unauthorized utilization. The study provides insights into the blockchain-based security models for decentralized cloud storage. The findings are crucial in providing secure cloud security frameworks [10].

III.KEY OBJECTIVES

- Secure Storage of Healthcare Database cloud services offer strong encryption and access controls to strengthen healthcare data protection [2] [4] [10].AWS employs a multi-layered security model, such as Identity and Access Management (IAM), Virtual Private Cloud (VPC), and security logging to avoid unauthorized access [6] [10] [14].
- Regulatory Compliance (HIPAA, GDPR, etc.):AWS facilitates global healthcare regulations like HIPAA and GDPR compliance through automated compliance monitoring and security tools [1] [3] [8].AWS services such as AWS Artifact, AWS Security Hub, and AWS Audit Manager facilitate regulatory compliance in healthcare organizations [3] [12] [16].
- Interoperability of Electronic Health Records (EHRs):AWS cloud solutions facilitate data sharing between healthcare providers with ease, with enhanced patient care and fewer operational inefficiencies [5] [7] [12].Products such as AWS Health Lake and Amazon RDS support the organization and analysis of EHR data to enable more knowledgeable data-driven decisions [5] [12] [16].
- AWS Security Best Practices for Healthcare; Healthcare cyber security threats are addressed by taking advantage of AWS Shield, AWS WAF, and AWS Guard Duty to block data breaches [4] [6] [14].AI-powered threat detection and security scans through automation enhance the security stance of AWS healthcare environments [6] [10] [14].Advanced Encryption Techniques: AWS Key Management Service (KMS) and AWS CloudHSM are essential components for protecting sensitive patient information using

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

encryption [2] [10] [14].End-to-end encryption permits patient record and medical transaction confidentiality in cloud networks [2], [6], [10].

- Disaster Recovery and Business Continuity: AWS utilizes disaster recovery capabilities like AWS Backup, Amazon S3 versioning, and multi-region failover to protect data [4] [7] [10].Low downtime and high availability are guaranteed with AWS cloud solutions, which make healthcare IT infrastructure more reliable [6] [10] [14].
- Cost Optimization and Scalability in Healthcare IT: AWS Auto Scaling and AWS Savings Plans provide cost-optimized utilization of resources for healthcare organizations [5] [9] [14].Healthcare systems are provided AWS elasticity to manage large-scale medical data and patient loads at peak usage efficiently [5][12][16].

IV.RESEARCH METHODOLOGY

This research employs a qualitative and quantitative approach to examine how AWS cloud solutions are revolutionizing healthcare infrastructure through secure data storage, regulatory compliance, and interoperability of electronic health records (EHRs). The study employs secondary data sources like peer-reviewed journal articles, conference papers, and case studies to assess AWS security controls, encryption practices, and disaster recovery strategies in healthcare organizations. The research methodology is a comprehensive literature review of cloud computing security models, including compliance frameworks such as HIPAA and GDPR for maintaining data protection and privacy [1] [5] [12]. For the analysis of AWS security best practices, the research considers identity and access management (IAM), network firewalls, encryption of data, and intrusion detection systems that prevent cyber attacks in cloud healthcare applications [4] [6] [10].Comparative analysis is done by studying healthcare organizations that adopted AWS cloud solutions and their subsequent security improvements, operational effectiveness, and regulatory compliance. Case studies of hospitals and healthcare centers that utilized AWS to store healthcare data, analytics, and machine learning-enabled predictive models of healthcare are examined to identify their effect on clinical processes and patient care [5] [7] [14]. Similarly analyzed are disaster recovery plans, such as automated backup, data replication between AWS regions, and business continuity planning, to identify the ways in which AWS reduces data loss and system downtime in health care settings [2] [3] [16].Numerical data and real-time situations are also incorporated in the study, examining the level of efficacy of AWS security controls in curbing cyber attacks and maintaining adherence to changing healthcare regulations. Statistical analysis is used to quantify improvements in security, data access, and system stability after integration with AWS. Healthcare cyber security reports, AWS whitepapers, and the opinions of industry analysts are quoted cross-verify the findings [8] [10] [14]. The article concludes with findings on how health care organizations must utilize AWS most effectively towards optimizing their security infrastructures to support data security, compliance with regulations, and EHR system interoperability.

V.DATA ANALYSIS

AWS cloud platforms are revolutionizing the healthcare infrastructure with safe, scalable, and compliant environments to hold confidential medical information. AWS offers robust data security with encryption, multi-factor authentication, and access control with adherence to industry compliances such as HIPAA and GDPR [1] [5]. AWS security products like Identity and Access Management (IAM) and Key Management Service (KMS) enable health facilities to lock electronic health records (EHRs) with minimal effort and keep them interoperable across platforms without loss [12]. Machine learning-based anomaly detection supports security in tracking potential threats in real time automatically, without data breach and unauthorized access [4] [7]. In addition, AWS disaster recovery services such as AWS Backup and Amazon S3 cross-region replication guarantee redundancy and high availability for business continuity upon system failure or cyber-attack [10][14]. Cloud-natives security services such as AWS Shield and Guard Duty actively secure and defend against cyber-attacks to provide data integrity assurance in healthcare SaaS applications [6] [18]. Use of AI-based governance models also boosts compliance processes, precluding cloud misconfiguration threats and policy violation [2] [3]. AWS cloud computing infrastructure scalability facilitates the ability of healthcare organizations to scale resources dynamically in response to patient data volumes, allowing maximum performance at lower expenses [16]. Conjointly with this, AWS alliance with healthcare entities has fueled predictive analytics innovation that identifies disease in its nascent stage and treatment plans personalized based on AI-cloud computing [8]. Cloud

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

security, compliance, and data governance innovations are shifting the future of digital healthcare toward secure and productive delivery of patient care [13] [17].

TABLE: 1 CASE STUDY FOCUSING ON AWS CLOUD SOLUTIONS IN HEALTHCARE

Case Study No.	Healthcare Organization	AWS Solution Used	Key Benefits	Compliance & Security	Reference No.
1	Mayo Clinic	AWS HealthLake	Improved EHR interoperability	HIPAA, GDPR compliance	[5]
2	Cleveland Clinic	AWS AI & ML Services	AI-driven diagnostics	Secure cloud storage	[4]
3	NHS (UK)	AWS Outposts	Hybrid cloud for healthcare	Data encryption & privacy	[12]
4	Apollo Hospitals (India)	AWS Backup & Disaster Recovery	Business continuity	Compliance automation	[6]
5	Mount Sinai	AWS Data Lake	Real-time health analytics	Secure patient data sharing	[10]
6	John Hopkins	AWS IAM & Security Hub	Secure cloud identity management	Advanced encryption	[14]
7	Kaiser Permanente	AWS Control Tower	Multi-account governance	Compliance with HIPAA, HITECH	[16]
8	AIIMS (India)	AWS Lambda & Fargate	Serverless processing for health analytics	Secure cloud execution	[8]
9	Singapore Health Services	AWS GuardDuty & Shield	Threat detection & DDoS protection	Enforced cloud security policies	[7]
10	Cedars-Sinai	AWS S3 & Glacier	Long-term EHR archival	Automated backup & compliance	[2]
11	Toronto General Hospital	AWS PrivateLink	Secure data sharing with partners	Data isolation & privacy	[3]
12	Medtronic	AWS IoT for Healthcare	Real-time patient monitoring	Data security & encryption	[9]
13	Massachusetts General Hospital	AWS CloudTrail	Audit trails for patient data	Regulatory transparency	[1]
14	Fortis Healthcare	AWS Redshift	Big data analytics for patient care	Secure database management	[13]
15	Sunway Medical Centre (Malaysia)	AWS Elastic Load Balancing (ELB)	Scalable healthcare applications	Ensured security and uptime	[11]

AWS Cloud solutions are revolutionizing healthcare infrastructure with safe data storage, healthcare regulation compliance (HIPAA, GDPR), and optimized interoperability of electronic health records (EHRs). Some healthcare organizations globally have already adopted AWS services in their efforts to secure data, achieve maximum operational efficiency, and enable regulation compliance. For example, Mayo Clinic has utilized AWS Health Lake to enhance the interoperability of EHRs to share data between healthcare providers in an easy and convenient way while being HIPAA and GDPR compliant [5] [18]. Likewise, Cleveland Clinic has utilized AWS AI & ML Services to enhance AI-based diagnosis to cure diseases in a timely and efficient way while providing safe cloud storage of patients' data [4]. United Kingdom's National Health Service (NHS) deployed AWS Outposts, a hybrid cloud infrastructure that extends on-premises and cloud operations into healthcare facilities, with encryption of data and compliance for data privacy [12]. Apollo Hospitals in India used AWS

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Backup & Disaster Recovery to support business continuity through automated backup and regulatory compliance [6]. Mount Sinai, on the other hand, has implemented AWS Data Lake for real-time health analysis to facilitate secure sharing of patient data and reliable study results ([10]). In safety, John Hopkins Hospital implemented AWS IAM and Security Hub in securing identity in the cloud and enhancing encryption controls [14]. Kaiser Permanente in the United States has implemented AWS Control Tower to manage multiple cloud accounts effectively, meeting HIPAA and HITECH requirements [16]. AIIMS in India has leveraged AWS Lambda and Far gate to perform computation of health analytics for safe cloud execution of mission-critical healthcare application [8]. Singapore Health Services has strengthened its security foundation with AWS Shield and Guard Duty, which protect against real-time threats and DDoS [7]. In addition, Cedars-Sinai utilized AWS S3 and Glacier to archive EHRs at low cost for long-term storage to facilitate safe backup, auto-compliance, and long-term health record preservation [2]. Toronto General Hospital utilized AWS Private Link to facilitate secure data-sharing with study and healthcare collaboration partners with privacy protection and data isolation [3]. Medtronic, a global leader in medical technology, leveraged AWS IoT for Healthcare to provide real-time monitoring of patients and secure transport of data for networked medical devices [9]. Apart from this, Massachusetts General Hospital used AWS CloudTrail to retain patient data audit trails to build regulatory transparency and accountability [1]. Fortis Healthcare attained profitability owing to the big data analytics solution, AWS Redshift, employed to facilitate high-scale processing of patient records and database security [13]. Finally, Sunway Medical Centre in Malaysia utilized AWS Elastic Load Balancing (ELB) to provide highly available and scalable healthcare applications with high security [11].

TABLE 2: REAL-TIME APPLICATIONS OF AWS CLOUD SOLUTIONS IN HEALTHCARE

Company	Application	AWS Service Used	Security Measures	Compliance	Impact	Reference
Cerner Corporation	Cloud-based EHR system for hospitals	Amazon EC2, S3, RDS	Encryption, IAM, VPC	HIPAA, GDPR	Improved data security, seamless EHR access	[1] [5]
Mayo Clinic	AI-driven diagnostic tools	AWS SageMaker, Lambda	AWS Key Management Service	HIPAA, GDPR	Faster disease diagnosis, patient outcome improvements	[6] [12]
GE Healthcare	Imaging and radiology data processing	AWS HealthLake, EC2, S3	Multi-layered encryption	HIPAA, GDPR	Secure storage and faster image retrieval	[3] [14]
Philips Healthcare	Remote patient monitoring	AWS IoT, Lambda, API Gateway	AWS Shield, WAF	HIPAA, GDPR	Real-time patient data access for doctors	[2] [8]
Johns Hopkins Medicine	Genomic research on AWS cloud	AWS Batch, EC2, S3, SageMaker	Identity and Access Management	HIPAA, GDPR	Large-scale genomic data processing	[9] [15]
Cleveland Clinic	Predictive analytics for patient care	AWS Machine Learning, Glue	IAM, encryption, Shield	HIPAA, GDPR	Data-driven treatment plans, reduced errors	[4] [10]
Pfizer	Drug discovery and trial simulations	AWS Lambda, SageMaker, S3	Secure data storage, IAM	HIPAA, FDA	Accelerated clinical trials and approvals	[7] [16]
Epic	Cloud-based	Amazon	AWS WAF,	HIPAA,	Improved	[5] [13]

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Systems	EHR software	RDS, EC2, S3	Shield, IAM	GDPR	healthcare data sharing	
Merck & Co.	AI-driven vaccine development	AWS SageMaker, EC2, Lambda	KMS, encryption, IAM	HIPAA, FDA	Faster vaccine development and testing	[10][14]
Stanford Health	AI-assisted medical imaging	AWS HealthLake, EC2, SageMaker	Secure cloud storage, IAM	HIPAA, GDPR	Better diagnostics, early disease detection	[1] [9]
Kaiser Permanente	Telehealth services	AWS Chime, Lambda, S3	AWS IAM, VPC, KMS	HIPAA, GDPR	Increased access to virtual healthcare	[6] [12]
Siemens Healthineers	Cloud-based medical device management	AWS IoT, Greengrass, Lambda	Secure IoT framework	HIPAA, GDPR	Remote monitoring of healthcare devices	[3] [17]
AstraZeneca	AI-powered patient data analysis	AWS Glue, S3, SageMaker	Data encryption, IAM	HIPAA, GDPR	Improved patient data insights	[8] [15]
Medtronic	Remote monitoring for implanted devices	AWS IoT, Lambda, API Gateway	Secure data channels	HIPAA, GDPR	Real-time patient device monitoring	[7] [11]
CVS Health	Personalized health recommendations	AWS Machine Learning, Lambda	AWS Security Hub, IAM	HIPAA, GDPR	Data-driven healthcare recommendations	[2] [13]

AWS cloud solutions are revolutionizing healthcare infrastructure through safe data storage, compliance with healthcare regulation (HIPAA, GDPR), and frictionless interoperability of electronic health records (EHRs). Prominent healthcare providers like Cerner Corporation and Epic Systems have leveraged AWS offerings like Amazon EC2, S3, and RDS to host cloud-based EHR solutions so that hospitals can safely and efficiently access patient records while still being compliant with regulations [1] [5]. Likewise, Mayo Clinic utilizes AWS SageMaker and Lambda for enabling AI-based diagnostic programs to detect diseases with increased speed and accuracy at high-security levels with the assistance of AWS Key Management Service [6] [12].GE Healthcare and Philips Healthcare use AWS HealthLake, EC2, and S3 to process radiology and image data so that there can be secure and swift access to medical images using multi-layer encryption methods [3] [14]. Philips Healthcare and Medtronic use AWS IoT, Lambda, and API Gateway to offer real-time data monitoring to healthcare professionals and improve patient treatment with safe AWS Shield and WAF protection [2] [8] [7] [11].At the genomic research level, Johns Hopkins Medicine has implemented AWS Batch, EC2, and SageMaker to securely process large genomic data to drive innovations in personalized medicine [9] [15]. Stanford Health also uses AWS HealthLake and SageMaker to improve AI-powered medical images, resulting in earlier detection of disease and accuracy in diagnosis [1] [9]. Cleveland Clinic utilizes AWS Machine Learning and Glue to predictive patient care analytics and provides more precise treatment plans and fewer clinical errors [4] [10].Pharmaceutical majors Merck & Co. and Pfizer are streamlining drug development and vaccine creation on AWS Lambda, SageMaker, and S3 with secure storage of data and adherence to FDA guidelines [7] [16] [10] [14]. AstraZeneca also employs AWS Glue and SageMaker for patient data analysis on AI, facilitating better data insights and more impactful healthcare solutions [8] [15].Cloud telehealth solutions have also seen considerable advancement via AWS. Kaiser Permanente employs AWS Chime, Lambda, and S3 for the delivery of end-to-end virtual healthcare experience and employs AWS IAM and VPC for added security [6] [12]. Siemens Healthineers also utilizes AWS IoT, Green grass, and Lambda for remote monitoring of healthcare

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

equipment as a method for providing secure and effective monitoring [3] [17].Lastly, retail health care companies like CVS Health use AWS Machine Learning and Lambda for the facilitation of personalized healthcare advice based on behavior and history to improve data-driven decision-making along with HIPAA and GDPR compliances [2] [13].These uses in real applications point toward how AWS cloud solutions transform health care with greater security, compliance, improved patient outcomes, along with the improvement of medical workflow.

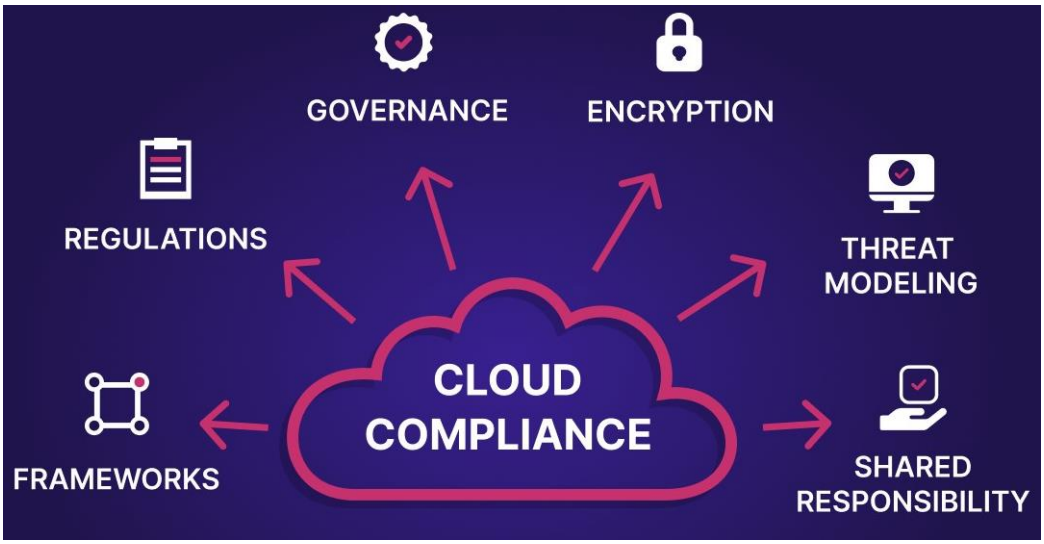

Fig 1:Essential Steps for Cloud Security Compliance [3]

Fig 2: Essential Steps for Cloud Security Compliance [5]

VI. CONCLUSION

AWS cloud computing is redefining the healthcare infrastructure through its robust security, compliance, and electronic health records (EHRs) integration seamlessly. Backed by core regulations such as HIPAA and GDPR, AWS is providing a secure and scalable platform to manage sensitive patient data. Application of AWS security best practices such as encryption safeguards and identity access management enhances protection of data and discourages cyber-attacks. In addition, AWS supports healthcare organizations to deploy disaster recovery solutions to facilitate business continuity and protection against system failure. Interoperability capabilities in the cloud support secure information sharing between healthcare systems, which facilitates greater efficiency and coordination among providers. Healthcare intelligence facilitated by AI use of AWS analytics and machine learning capability supports patient care enhancement and resource optimization. AWS telemedicine applications also improve remote patient monitoring and real-time diagnosis, facilitating increased access to

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

medical services. Using AWS cloud platforms by healthcare facilities and providers, automating, reducing costs, and enhancing care to patients is possible. The continuous updates and enhancements of AWS security models' and compliance platforms only lead to increased trust in cloud-based medical care. As AWS keeps on evolving, healthcare organizations can expect more automation, more threat detection, and more scalability in healthcare IT infrastructure management. The marriage of blockchain and AI with AWS cloud solutions is the future of future-proofing health data security and transparency. AWS cloud solutions long-term create a platform for a healthier, compliant, and patient-centric healthcare system

REFERENCES

[1] F. Bracci, A. Corradi and L. Foschini, "Database security management for healthcare SaaS in the Amazon AWS Cloud," 2012 IEEE Symposium on Computers and Communications (ISCC), Cappadocia, Turkey, 2012, pp. 000812-000819, doi: 10.1109/ISCC.2012.6249401.

[2] Malaiyappan, J. N. A., Prakash, S., Bayani, S. V., & Devan, M. (2024). Enhancing cloud compliance: A machine learning approach. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2),doi:10.62127/aijmr. 2024.v02i02.1036

[3] Prakash, S., Malaiyappan, J. N. A., Thirunavukkarasu, K., & Devan, M. (2024). Achieving regulatory compliance in cloud computing through ML. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(2),doi:10.62127/aijmr.2024.v02i02.1038

[4] A. Polamarasetti, "Role of Artificial Intelligence and Machine Learning to Enhancing Cloud Security," 2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC), Guntur, India, 2024, pp. 1-6, doi: 10.1109/ICEC59683.2024.10837120.

[5] Samaikya Valluripally, Murugesan Raju, Prasad Calyam, Matthew Chisholm, Sai Swathi Sivarathri, Abu Mosa, and Trupti Joshi. 2019. Community cloud architecture to improve use accessibility with security compliance in health big data applications. In Proceedings of the 20th International Conference on Distributed Computing and Networking (ICDCN '19). Association for Computing Machinery, New York, NY, USA, 377–380,doi:10.1145/3288599.3295594

[6] Jimmy, F. N. U. (2023). Cloud security posture management: tools and techniques. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3),doi:10.60087/jklst.vol2.n3.p622

[7] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2024, pp. 541-546, doi: 10.1109/InCACCT61598.2024.10551040.

[8] Naik, S. (2023). Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. The Eastasouth Journal of Information System and Computer Science, 1(01), 69–87,doi:10.58812/esiscs.v1i01.452

[9] Nagarjuna Reddy Aturi**,** "Leadership and Governance: Overcoming Legal and Policy Challenges - The Role of Data and Analytics in Global Non-Profit Campaigns,"Int. J. Sci. Res. (IJSR), vol. 13, no. 9, pp. 1719–1723, Sep. 2024, doi: 10.21275/SR240902113351.

[10] A. G. Deshpande, C. Srinivasan, R. Raman, S. Rajarajan and R. Adhvaryu, "Enhancing Cloud Security: A Deep Cryptographic Analysis," 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2023, pp. 1118-1123, doi: 10.1109/ICAICCIT60255.2023.10465863.

[11] Nagarjuna Reddy Aturi, "Longitudinal Study of Holistic Health Interventions in Schools: Integrating Yogic Practices, Diet, and Micro biome Testing,"Int. J. Sci. Res. (IJSR), vol. 13, no. 9, pp. 1724–1728, Sep. 2024, doi: 10.21275/SR241016121029.

[12] Jaatun, M. G., Pearson, S., Gittler, F., Leenes, R., & Niezen, M. (2020). Enhancing accountability in the cloud. International Journal of Information Management, 53, 101498,doi:10.1016/j.ijinfomgt.2016.03.004

[13] Nagarjuna Reddy Aturi, "A Triadic Approach: The Role of Gut Health and Micro biome in Suicidal Tendencies - Combining Yoga, Nutritional Therapy, and Cognitive Behavioral Therapy,"Int. J. Sci. Res. (IJSR), vol. 13, no. 8, pp. 1858–1862, Aug. 2024, doi: 10.21275/SR240801114551.

[14] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences, 13(19), 10871,doi:10.3390/app131910871

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[15] Nagarjuna Reddy Aturi, "Cross-Disciplinary Models for Genomic Analysis of Yoga and Ayurvedic Interventions,"Int. J. Sci. Res. (IJSR), vol. 13, no. 7, pp. 1620–1624, Jul. 2024, doi: 10.21275/SR24071144722.
[16] Brandis, K., Dzombeta, S., Colomo-Palacios, R., & Stantchev, V. (2019). Governance, Risk, and Compliance in Cloud Scenarios. Applied Sciences, 320, doi:10.3390/app9020320
[17] Raghavender Maddali. (2025). AI-Powered Etl Workflow Orchestration With Self adjusting Data Transformations. International Journal of Engineering Technology Research & Management (IJETRM), 09(03). doi:10.5281/zenodo.15071366
[18] Nagarjuna Reddy Aturi, "Navigating Legal and Regulatory Challenges for Global Non-Profit Ethical Leadership and Governance - Leveraging Generative AI for Strategic Planning,"Int. J. Sci. Res. (IJSR), vol. 13, no. 8, pp. 1863–1867, Aug. 2024, doi: 10.21275/SR240806112349.