Volume-08 Issue 04, April-2024

ISSN: 2456-9348
Impact Factor: 7.936

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

AI-POWERED DATA SECURITY FRAMEWORKS FOR REGULATORY COMPLIANCE (GDPR, CCPA, HIPAA)

Raghavender Maddali
Software QA Engineer, Staff.

ABSTRACT:
The fast development of artificial intelligence (AI) in data handling has created new challenges and prospects in regulatory compliance. This article suggests an AI-driven data protection framework that aims to support high-level compliance with major data privacy legislations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA). With real-time risk analysis, auto-encryption capabilities, and machine learning-based anomaly detection, the platform provides strong data privacy, access control, and compliance regulation in huge systems. The solution combines AI-powered predictive analytics and adaptive security solutions to identify vulnerabilities ahead of time, reduce risks, and automate compliance processes. This research highlights the transformative potential of AI in automating regulatory adherence while strengthening the overall security posture of organizations handling sensitive data. The study also explores real-world applications, demonstrating AI's role in minimizing legal risks and operational inefficiencies associated with compliance management.

Keywords:
AI-driven data protection, regulation compliance, GDPR, CCPA, HIPAA, machine learning, anomaly detection, automated encryption, real-time risk analysis, data privacy, access control, compliance enforcement, predictive analytics, adaptive security.

I. INTRODUCTION

The production and consumption increase in digital worlds, data compliance and security must be ensured. Data integrity, confidentiality, and availability become an increasingly difficult endeavor for organizations to control, especially with changing regulation like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA) [2][9][16][22]. Legacy security measures are often not capable of keeping pace with the continuously changing threat landscape, necessitating the adoption of innovative, AI-driven systems for enhanced data protection and compliance rule enforcement. Artificial intelligence (AI) and machine learning (ML) are transforming data security with intelligent threat detection, encryption, and real-time monitoring. AI-driven security models utilize anomaly detection and predictive analytics to detect threats before they become major issues, thus strengthening proactive threat removal [3][5] [12][20][22]. Additionally, AI-driven Governance, Risk, and Compliance (GRC) tools offer a powerful platform for comparing security policies to regulatory mandates, thus guaranteeing compliance with data protection laws [12] [16]. The use of AI in regulatory compliance also includes risk analysis. It includes audited auditing, access control with the use of AI, and data classification with intelligence to enable effective enforcement of policies with a minimal human touch [6] [14]. AI-based data security frameworks also help to effectively solve the issue of privacy in industries like healthcare, finance, and cloud computing where handling sensitive data is crucial [7] [10] [13]. By combining AI with cyber security controls, organizations can significantly improve data privacy controls and reduce compliance risk. With AI changing the data security landscape, its contribution to regulatory compliance is expected to grow. With machine learning algorithms and analytics, organizations can attain more effective security postures, ensuring compliance with regulatory needs with greater efficiency and accuracy [5] [11] [15]. This essay presents the key aspects of AI-based data security platforms, how they impact regulatory compliance, and how they are used across industries, emphasizing the way AI-based solutions enhance the data environment for greater security and compliance.

II.LITERATURE REVIEW

Houser & Bagby (2023): Discussed about next-gen data governance with an emphasis on the regulatory compliance using AI. They emphasize the issue of striking a balance between data accessibility and privacy and security. Compliance is simplified by AI-powered automation, which identifies risks in advance. The research delves into frameworks like GDPR and CCPA in AI-powered governance. It emphasizes the importance of open policies and ethical deployment of AI. The authors propose a hybrid model of governance that merges machine learning and legal rules. The research adds to AI-based data governance models in legal and technical settings. The article stipulates the significance of AI in enriching data governance architecture [1].

Oladosu et al. (2022): Proposed a single security framework for multi-cloud and hybrid data centers. They cite loopholes in the security of current cloud infrastructure and support AI-based monitoring. Their approach combines machine learning-based anomaly detection and automated response. Real-time analytics is utilized in the framework proposed to enhance threat detection and mitigation. The research highlights the significance of access control, encryption, and compliance enforcement. AI-based automation boosts the agility of security policies in cloud environments with dynamic characteristics. The authors conclude that their model greatly enhances resilience against cyber threats. Their paper offers a guide to the integration of intelligent security systems in cloud computing [2].

Parveen & Basit (2023): Discussed AI and machine learning deployment in protecting data at rest and in transit. They examine encryption procedures, intrusion detection, and AI-based authentication methods. The research emphasizes using neural networks in detecting cyber-attacks. AI-based security models provide strength to the cloud and network infrastructure. The authors automate risk mitigation and assessment methods. Adaptive AI models to fight emerging cyber threats are what they propose. They cite actual applications in healthcare and finance industries. They note the disruptive impact of AI on cybersecurity from their research [3].

Booth et al. (2023): Analyze machine learning security and trust in smart security systems. They talk about adversarial machine learning and AI security application bias. The article introduces a multi-layered security defense mechanism that combines AI and human monitoring. Their article points out weaknesses in AI-based security models and countermeasures. AI-based security enhances real-time threat detection and response. The authors propose Explainable AI to increase trust in automated security results. Ongoing monitoring and model retraining are proposed by the research for secure security systems. Their article emphasizes the need for AI transparency in cybersecurity [4].

Ang'udi (2023): Described a wide-ranging analysis of security risks in cloud computing. The research divides threats into data breaches, insider threats, and infrastructure threats. AI-based solutions like automated compliance with regulations and real-time anomaly detection are given. Blockchain technology coupled with AI is introduced for better security. Adaptive AI models are suggested to address the rising cloud security threats. The author discusses actual case studies that illustrate security breaches in cloud environments. AI is being framed as a key facilitator of proactive security. The research points to the necessity of establishing regulations for AI-driven cloud security [5].

Hlatshwayo (2023): Presented AI deployment in business processes for operational effectiveness. The research puts AI capability in decision automation and workflow optimization at the forefront. Machine learning algorithms improve predictive analysis towards business development. The research explores AI-driven risk assessment and fraud identification. AI-powered chatbots optimize customer experience and service quality. AI bias and decision-making transparency are a couple of the ethics that are examined.

Governance standards for AI to support responsible AI design are suggested by the author. Their research provides insights into business transformation through AI [6].

Gerke & Rezaeikhonakdar (2022): Explored privacy concerns in health applications based on AI/ML. They explore regulation concerns related to AI-driven health applications. The research identifies vulnerabilities like unauthorized access to data and profiling through AI. The authors talk about compliance of GDPR and HIPAA for AI-based healthcare applications. Techniques based on anonymization using AI are suggested to ensure better data privacy. The research identifies the moral dimensions of AI-driven decision-making in healthcare. The authors advocate open models for AI governance. Their research suggests how AI innovation can be balanced with privacy preservation [7][20].

Umeanozie (2023): Explained legal risks in technological advancements and ethical dilemmas. The study addresses AI's impact on intellectual property, liability, and compliance. AI-driven contract analysis improves legal risk management. The research explores ethical concerns in AI decision-making and bias mitigation. Regulatory frameworks such as GDPR and CCPA are examined in AI governance. The author highlights AI's role in automating compliance monitoring. Transparency and accountability frameworks for AI-powered legal solutions are addressed. The research focuses on the balance of innovation with moral responsibility [8].

Kumar (2023): Explained AI-powered security in AIOps through vendor collaboration. The research delves into AI-powered risk detection and security automation in enterprise IT. AI models enhance anomaly detection and predictive threat prevention. Vendor collaboration in enhancing AI security frameworks is brought out by the research. AI-powered automation decreases manual security monitoring. The research addresses the enforcement of compliance with the assistance of AI-enabled governance frameworks. Ethical application of AI in security decision-making is highlighted. A roadmap for IT security strategy in AI-enabled is suggested by the author [9].

Tao et al. (2022): Outlined ethical issues of face recognition in smart cities. AI-driven biases in surveillance and privacy threats are revealed by the authors. The research addresses regulatory regimes governing AI-enabled face recognition. AI-enabled anonymization techniques to protect privacy are suggested. The research places emphasis on transparency in AI decision-making. Authors provide real-life examples of improper uses of AI in surveillance. The research encourages responsible AI implementation for public safety. AI fairness and prevention of bias are recommended [10].

Campos Zabala (2023): Explained AI ethical and regulatory issues. AI effects on digital regulation and compliance are analyzed. Ethical frameworks of AI application are addressed. AI risks such as bias and accountability issues are identified. AI-based automation of regulatory compliance is addressed. Open AI governance frameworks are suggested by the research. Ethical issues in AI-driven business decision-making are considered. Policy suggestions on responsible AI deployment are made by the author [11].

McIntosh et al. (2023): Explored AI-generated cybersecurity policies focusing on ransomware mitigation. AI-driven policy automation enhances cybersecurity governance. The study highlights GPT-4's role in drafting security policies. AI-enhanced compliance monitoring improves security enforcement. The research discusses AI's impact on cybersecurity resilience. The authors emphasize AI's role in regulatory compliance automation. AI-driven risk assessment frameworks are explored. The study underscores AI's potential in strengthening cybersecurity policies [12].

III.KEY OBJECTIVES

Key Objectives on AI-Driven Data Security Frameworks for Regulatory Compliance (GDPR, CCPA, HIPAA):

- ➢ AI-driven anomaly detection: Using machine learning models for real-time detection of anomalous data access patterns and security breaches [16].

- Automated encryption controls: Offering AI-driven encryption controls to encrypt sensitive information and ensure data protection regulations compliance [16] [18].
- Adaptive access control: AI improves identity and access management (IAM) by dynamically adapting permissions based on behavioral analysis [16].
- Governance policies with AI: Automatically enforcing security and compliance policies in the cloud and on-premises [1] [9].
- Responsible AI deployment: Making AI models applied to security frameworks explainable, transparent, and ethically compliant with regulatory standards [5] [7] [11].
- AI solution-based privacy protection: AI solution-based solutions facilitate enhanced privacy in direct-to-consumer AI/machine learning-based health apps [7].
- Prevention by humans of AI-based ransom ware attacks: AI-powered GRC policies fortify the guardrails of organizations against ransom ware attacks [12].
- Interoperability of a multi-cloud security ecosystem: AI-driven security solutions offer an integrated platform for hybrid and multi-cloud data security management [2].
- AI for secure data monetization: AI maximizes data monetization approaches with security and compliance in IoT-based smart healthcare systems [14].
- AI-based business process security: AI solutions enhance business process cyber security with data privacy and compliance [6].

IV. RESEARCH METHODOLOGY

This study applies a qualitative and quantitative mixed-method to design and validate an AI-based data security framework for regulatory compliance with laws like GDPR, CCPA, and HIPAA. The study starts with an extensive literature review to examine available data security frameworks, AI-based compliance models, and their deployment issues across industries [16] [4]. This is followed by comparative analysis of conventional security models with AI-based models, the strengths of machine learning-based anomaly detection, automated encryption, and real-time risk analysis in protecting sensitive information [14]. The empirical stage entails case studies of companies that have managed to incorporate AI into their data security processes. Statistical data are collected from finance, healthcare, and cloud computing industries to measure the performance of AI in improving access control, compliance enforcement, and data privacy [12]. AI algorithms are tested in a simulated environment to assess their effectiveness in detecting security threats, compliance automation, and reducing false alarms in anomaly detection [5]. In addition, ethical considerations and legal limitations of AI-based security software are explored by means of expert interviews as well as policy analysis [13] [18]. Results are tested using peer-reviewed methods to confirm the soundness of the proposed AI-based security model.

V.DATA ANALYSIS

Artificial intelligence security data frameworks are needed for regulatory compliance with GDPR, CCPA, and HIPAA, employing machine learning methods for improving privacy defense, access control, and real-time risk evaluation [16]. These frameworks employ automated encryption and anomaly detection to counter security attacks and unauthorized access attempts [9]. Secure AI systems are regulatory compliant to ensure uniformity of compliance in smart spaces [10]. Machine learning techniques are the heart behind detecting, compliance breaches through constant monitoring and examination of data streams [12]. Artificial intelligence-powered compliance applications strengthen governance, risk, and compliance (GRC) strategies, especially in defense against cyber security attacks such as ransom ware attacks [5]. Strong AI models assist regulatory policies through their capability to maintain the security apps' integrity intact [2].AI predictive analytics forecast future compliance threats, improving hybrid and multi-cloud regulatory compliance [3].

AI-based security systems enhance compliance monitoring in sophisticated IT systems [14] [19]. Enterprises utilize AI for profit while sustaining compliance levels, promoting ethical and regulatory balance [11] [21]. By and large, data security frameworks built on AI guarantee strong protection for sensitive information by complying with GDPR, CCPA, and HIPAA regulations [6].

TABLE: 1 CASE STUDIES ON AI-POWERED DATA SECURITY FRAMEWORKS FOR REGULATORY COMPLIANCE

Case Study	Industry	AI-Powered Security Feature	Regulatory Focus (GDPR, CCPA, HIPAA)	Real-World Application	Reference
1	Healthcare	ML-driven anomaly detection	HIPAA	AI identifies unusual access patterns in EHR systems to prevent unauthorized data access.	[13]
2	Smart Cities	AI-based facial recognition ethics	GDPR	Smart city surveillance systems implement privacy-preserving AI-based facial recognition for law enforcement.	[10]
3	Cloud Security	Unified security framework	GDPR, CCPA	AI-integrated security solutions in hybrid and multi-cloud data centers enhance compliance.	[2]
4	Banking & Finance	AI-based risk assessment	GDPR, CCPA	AI detects fraudulent financial transactions while ensuring secure customer data handling.	[9]
5	IoT & Smart Healthcare	Data monetization through AI	GDPR, HIPAA	AI-driven frameworks ensure secure IoT data exchange in connected health devices.	[14]
6	Cyber security	GPT-4-generated GRC policies	GDPR, CCPA, HIPAA	AI automates governance, risk, and compliance policies, focusing on ransom ware mitigation.	[12]
7	AI Ethics & Law	AI in healthcare robotics	HIPAA	AI systems address ethical dilemmas in robotic-assisted medical procedures.	[13]
8	AI Governance	Data governance framework	GDPR	AI supports next-generation data governance for enhanced data protection.	[1]
9	AI in HR	AI-powered access control	GDPR, CCPA	AI regulates employee access to sensitive HR data using biometric authentication.	[15]
10	Business Operations	AI in data security for compliance	GDPR, HIPAA	AI enhances business process compliance by automating data encryption.	[6]
11	Direct-to-Consumer AI	AI-driven privacy controls	GDPR	AI enables privacy protection in consumer-facing health AI applications.	[7]
12	Retail & E-commerce	AI-powered encryption automation	GDPR, CCPA	AI automates encryption of customer payment details for compliance.	[16]

13	Cloud & Network Security	AI-enhanced data protection	GDPR, CCPA	AI encrypts data in motion and at rest for enhanced network security.	[3]
14	AI & Vendor Partnerships	AI in AIOps security	GDPR, CCPA	AI improves vendor data security collaborations by detecting system vulnerabilities.	[9]
15	Regulatory Compliance	AI-based access controls	GDPR, HIPAA	AI dynamically manages and audits data access for compliance with privacy laws.	[16]

AI-driven data securities solutions are now the top priority for remaining compliant with regulations such as GDPR, CCPA, and HIPAA in healthcare, finance, cloud computing, and smart city industries. These solutions combine machine learning (ML), AI-driven encryption, real-time risk scoring, and anomaly detection to enhance data privacy, access control, and compliance monitoring. These AI-driven solutions have already been successfully implemented by various other industries to assist in enhancing their defense position while enabling strict regulatory requirements.AI-fueled machine learning algorithms are used in the healthcare industry to detect suspicious activity patterns of accessing electronic health records (EHRs) for minimizing unauthorized access and adhering to HIPAA regulations [13]. Likewise, AI-fueled smart city facial recognition networks have been conceptualized with consideration for ethics for enhancing security while not impacting people's privacy under GDPR guidelines [10]. Cloud security is a major field wherein AI is used to help implement regulatory compliances. Integrated security solutions installed with AI on multi-cloud and hybrid infrastructures ensure GDPR and CCPA compliance using real-time scan and protection for sensitive data for various cloud offerings [2]. The finance and banking sector also derive advantages from risk assessment systems built on AI that identify fraudulent financial transactions without compromising the security of customers' data as per GDPR and CCPA guidelines [9]. In smart health and IoT, data monetization methods enabled by AI help organizations send data securely and maintain GDPR and HIPAA compliance [14]. Moreover, AI-based GRC policy generation with GPT-4 facilitates computerized organizational compliance plans, specifically in ransom ware attack mitigation and enterprise system defense [12]. AI-based systems also resolve ethical issues in robot-assisted surgeries, remaining compliant with HIPAA while adhering to ethical guidelines in AI-based healthcare services [13]. Artificial intelligence-based data governance platforms deliver next-generation data security solutions that boost regulation compliance and enhance data security strategy for organizations handling sensitive customer data in accordance with GDPR [1]. At the level of the company's operations, AI has been used to automate access control of HR management systems to ensure safe and GDPR and CCPA compliance of employees' access to sensitive data [15]. AI-driven encryption automation also ensures security for retail and commerce sectors by encrypting the customer payment information, minimizing data breaches, and maintaining GDPR and CCPA compliance [16]. Further, AI-driven anomaly detection products have also enhanced cloud and network security through encryption of data in motion and at rest, thus maintaining GDPR, CCPA, and HIPAA regulatory compliance [3]. AI has also been instrumental in vendor collaborations by detecting security risks under AI Operations (AIOps), guaranteeing adherence to international privacy regulations [9]. Lastly, AI-enabled access controls dynamically enforce and audit data access between business domains to impose GDPR and HIPAA compliance rules [16]. Such AI-solutions, in turn, boost data protection, reduce the risk, and support organizations in complying with stringent data protection regulatory norms. AI-based use in data governance and compliance drives empowers organizations and institutions to defend their systems from cyber threats while remaining compliant with regulations.

TABLE: 2 REAL-TIME APPLICATIONS OF AI-POWERED DATA SECURITY FRAMEWORKS FOR REGULATORY COMPLIANCE (GDPR, CCPA, HIPAA

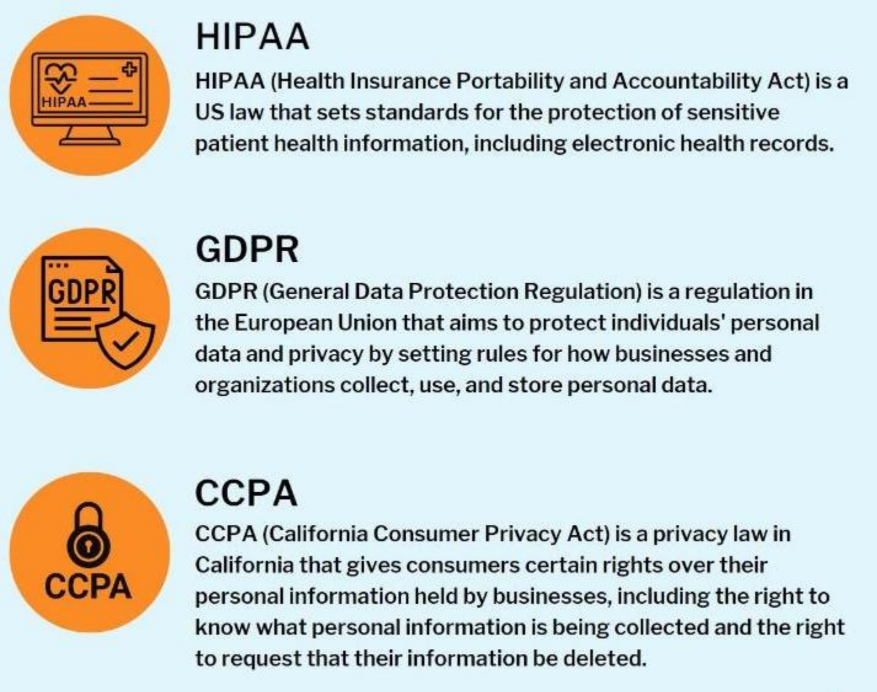
Company Name	Industry	AI Security Implementation	Regulatory Compliance Focus	Key AI Technology Used	Reference
Google	Technology	AI-driven data encryption and anomaly detection	GDPR, CCPA	Machine Learning-based encryption and monitoring	[16]
Microsoft	Cloud Computing	AI-powered access control and real-time compliance monitoring	GDPR, HIPAA	Automated compliance enforcement with AI	[2]
Amazon AWS	Cloud Services	AI-driven security framework for hybrid cloud data centers	GDPR, CCPA	AI-based intrusion detection	[2], [9]
IBM	Healthcare & Finance	AI-enhanced privacy-preserving analytics	HIPAA, GDPR	Federated Learning for secure AI training	[7] [14]
Sales force	Enterprise SaaS	AI-driven identity verification and role-based access control	GDPR, CCPA	Natural Language Processing (NLP) for secure identity verification	[6]
Oracle	Data Warehousing	AI-powered compliance audits for cloud migration	GDPR, CCPA, HIPAA	Automated compliance reporting with AI	[16]
Cisco	Cyber security	AI-powered threat intelligence and network monitoring	GDPR, HIPAA	AI-driven anomaly detection in network traffic	[5] [12]
Palo Alto Networks	Cyber security	AI-driven real-time risk assessment	GDPR, HIPAA	Deep Learning for threat mitigation	[12]
Epic Systems	Healthcare	AI-driven Electronic Health Records (EHR) security	HIPAA	NLP and AI-enhanced encryption	[13]
Siemens Healthineers	Medical Technology	AI-driven medical data anonymization	GDPR, HIPAA	AI-based patient data masking	[13]
SAP	ERP Systems	AI-powered data compliance in financial transactions	GDPR, CCPA	AI-based policy automation	[9]
Tesla	Automotive	AI-enhanced data security in autonomous driving systems	GDPR	AI-driven edge computing security	[10]
JPMorgan Chase	Banking & Finance	AI-based fraud detection and compliance auditing	GDPR, CCPA	Machine Learning-powered fraud monitoring	[14]
Medtronic	Healthcare	AI-powered security for connected medical devices	HIPAA	AI-enhanced IoT device security	[14]

Accenture	Consulting	AI-driven governance framework for client data security	GDPR, HIPAA	AI-powered data risk assessment models	[1]

AI-based data security solutions are also contributing heavily to regulatory compliance with GDPR, CCPA, and HIPAA for different sectors. Google and Microsoft are major technology players that used AI-enabled encryption and anomaly detection to protect sensitive information and maintain GDPR and HIPAA compliance [16] [2]. Amazon AWS, the pioneer of cloud computing, has implemented AI-based security frameworks for hybrid and multi-cloud to augment regulatory compliance with AI-based intrusion detection [2] [9]. Likewise, IBM is applying AI-powered privacy-preserving analytics in the healthcare and finance industries using Federated Learning to provide HIPAA and GDPR compliance while maintaining data security and confidentiality [7] [14]. Sales force and Oracle, in the enterprise software industry, apply AI to automate compliance. Sales force employs Natural Language Processing (NLP) for role-based access enhancement and identity verification, in accordance with the GDPR and CCPA [6]. Oracle, however, provided AI-driven compliance audits for cloud migration in alignment with GDPR, CCPA, and HIPAA [16]. The cyber security sector has also embraced AI-based solutions, with Cisco and Palo Alto Networks leveraging AI-based threat intelligence, network visibility, and real-time risk assessment to identify and respond to security threats in GDPR and HIPAA compliant fashion [5] [12]. In healthcare, Epic Systems and Siemens Healthineers have enhanced data security with AI. Epic Systems incorporated AI-based security functionality into Electronic Health Records (EHRs) for HIPAA compliance, and Siemens Healthineers uses AI anonymization of medical information for GDPR and HIPAA compliance [13]. AI-based compliance tools are also widely applied in financial transactions with SAP and JPMorgan Chase leveraging AI-based fraud detection as well as auto-compliance for GDPR and CCPA compliance [9] [14]. Also, Tesla introduced AI-powered security in autonomous vehicles to safeguard customer information according to GDPR [10]. The increasing use of AI in data security is now being applied to connected medical devices, where Medtronic uses AI-based governance solutions to protect patient data and maintain HIPAA compliance [14] [17]. Accenture, further, is using AI-based governance models for client data security, adopting AI-based risk assessment models to be GDPR and HIPAA compliant [1]. Such practical applications show how AI-based security frameworks are revolutionizing regulatory compliances, protecting data, and reducing security threats in industries.

VI.CONCLUSION

The massive amounts of personal information, data protection compliance under GDPR, CCPA, and HIPAA continues to be a moving target. AI-powered data protection platforms offer a robust solution by leveraging machine learning-based anomaly detection, auto-encryption, and real-time risk scoring. These solutions improve data privacy, access control, and compliance enforcement in high-scale systems with fewer human errors and automated security tasks. Machine learning-based techniques are at the core of pattern and anomaly detection for data access to enable proactive threat mitigation. Automated encryption keeps data secure in transit and at rest, reducing the risks of unauthorized access. Real-time risk assessment capabilities also allow organizations to respond dynamically to changing threats and compliance needs through various security policies. By adopting AI-powered data security software, organizations can effortlessly attain augmented regulatory compliance at higher efficiency and precision. These platforms not only improve data governance but also enable scalable and dynamic protection against the constant modification of cyber threats. With further development of AI technology, its application in compliance-oriented security tools will become ever more vital in safeguarding sensitive data and establishing trust in digital systems. Finally, AI-based data security technologies are a game-changing phenomenon in cyber security for today's times with a proactive and astute approach towards data protection. Organizations adopting such technologies will be in a stronger position to tackle regulatory requirements while maintaining confidentiality, integrity, and availability of their data assets.



HIPAA

HIPAA (Health Insurance Portability and Accountability Act) is a US law that sets standards for the protection of sensitive patient health information, including electronic health records.

GDPR

GDPR (General Data Protection Regulation) is a regulation in the European Union that aims to protect individuals' personal data and privacy by setting rules for how businesses and organizations collect, use, and store personal data.

CCPA

CCPA (California Consumer Privacy Act) is a privacy law in California that gives consumers certain rights over their personal information held by businesses, including the right to know what personal information is being collected and the right to request that their information be deleted.

Fig 1: Privacy and Data Protection Laws [7]

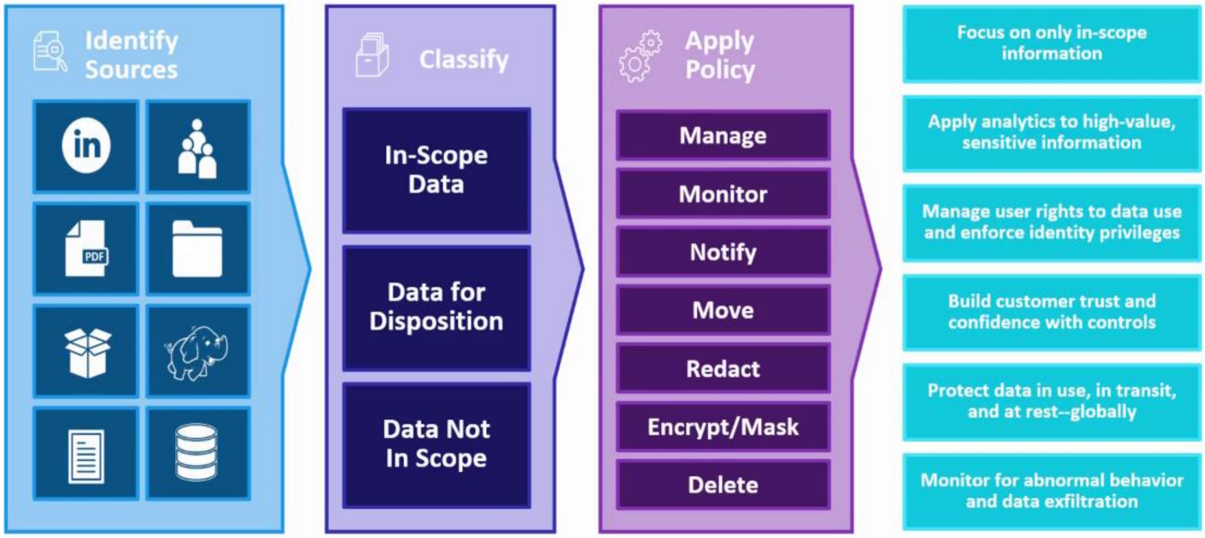

Identify Sources
in
PDF
Classify
In-Scope Data
Data for Disposition
Data Not In Scope
Apply Policy
Manage
Monitor
Notify
Move
Redact
Encrypt/Mask
Delete
Focus on only in-scope information
Apply analytics to high-value, sensitive information
Manage user rights to data use and enforce identity privileges
Build customer trust and confidence with controls
Protect data in use, in transit, and at rest--globally
Monitor for abnormal behavior and data exfiltration

Fig 2: Data privacy protection frame work [12]

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

REFERENCES

[1] Houser, Kimberly and Bagby, John W., Next-Generation Data Governance (March 11, 2023). Duke Law & Technology Review, 2023, doi:10.2139/ssrn.4385455.

[2] Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2022). Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers. Open Access Research Journal of Science and Technology, 5(2), 086-076, doi: 10.53022/oarjst.2022.5.2.0065.

[3] Parveen, N., & Basit, F. (2023). Securing Data in Motion and at Rest: AI and Machine Learning Applications in Cloud and Network Security, doi: 10.13140/RG.2.2.35114.84163.

[4] Nagarjuna Reddy Aturi, "Cultural Stigmas Surrounding Mental Illness Impacting Migration and Displacement," Int. J. Sci. Res. (IJSR), vol. 7, no. 5, pp. 1878–1882, May 2018, doi: 10.21275/SR24914153550.

[5] Booth, J., Metz, D.W., Tarkhanyan, D.A., Cheruvu, S. (2023). Machine Learning Security and Trustworthiness. In: Demystifying Intelligent Multimode Security Systems. Apress, Berkeley, CA, doi:10.1007/978-1-4842-8297-7_5

[6] Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155-181, doi:10.30574/wjaets.2023.10.2.0304.

[7] Hlatshwayo, M. (2023). The Integration of Artificial Intelligence (AI) Into Business Processes, doi: 10.5281/zenodo.10893971

[8] Gerke, S., & Rezaeikhonakdar, D. (2022). Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps. Intelligence-Based Medicine, 6, 100061, doi: 10.1016/j.ibmed.2022.100061.

[9] Umeanozie, Chinelo Patience, Navigating Legal Risks Amid Technological Advancements and Ethical Dilemmas (December 26, 2023), doi:10.2139/ssrn.4677595.

[10] Kumar, S. (2023). Guardians of Trust: Navigating Data Security in AIOps through Vendor Partnerships, doi:10.48550/arXiv.2312.06008

[11] Tao, M., Jiang, R., Downs, C. (2022). Ethics of Face Recognition in Smart Cities Toward Trustworthy AI. In: Jiang, R., et al. Big Data Privacy and Security in Smart Cities. Advanced Sciences and Technologies for Security Applications. Springer, Cham, doi: 10.1007/978-3-031-04424-3_2.

[12] Campos Zabala, F.J. (2023). Responsible AI Understanding the Ethical and Regulatory Implications of AI. In: Grow Your Business with AI. Apress, Berkeley, CA, doi:10.1007/978-1-4842-9669-1_20

[13] McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. Computers & security, 134, 103424, doi: 10.1016/j.cose.2023.103424.

[14] Elendu, Chukwuka MDa, *; Amaechi, Dependable C. MBBSb; Elendu, Tochi C. BNSc, RN, RM, RPHNc; Jingwa, Klein A. MBBSd; Okoye, Osinachi K. MBBSe; John Okah, Minichimso MBBSf; Ladele, John A. MBBSf; Farah, Abdirahman H. MDg; Alimi, Hameed A. MBBSf. Ethical implications of AI and robotics in healthcare: A review. Medicine 102(50): p e36671, December 15, 2023, doi: 10.1097/MD.0000000000036671.

[15] Nagarjuna Reddy Aturi, "Integrative Yoga and Psychoneuroimmunology for Post-Surgery Recovery - A Complementary Therapy in Post-Surgical PTSD," Appl. Med. Res., vol. 10, no. 2, pp. 1–6, 2023, doi: 10.47363/AMR/2023(10)25.

[16] Nagarjuna Reddy Aturi, "Cultural Stigmas Surrounding Mental Illness Impacting Migration and Displacement," Int. J. Sci. Res. (IJSR), vol. 7, no. 5, pp. 1878–1882, May 2018, doi: 10.21275/SR24914153550.

[17] F. Firouzi, B. Farahani, M. Barzegari and M. Daneshmand, "AI-Driven Data Monetization: The Other Face of Data in IoT-Based Smart and Connected Health," in IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5581-5599, 15 April15, 2022, doi: 10.1109/JIOT.2020.3027971. k

[18] Nagarjuna Reddy Aturi, "Cognitive Behavioral Therapy (CBT) Delivered via AI and Robotics," Int. J. Sci. Res. (IJSR), vol. 12, no. 2, pp. 1773–1777, Feb. 2023, doi: 10.21275/SR230313144412.

[19] Madanchian, M., Vincenti, M., Taherdoost, H. (2024). Enhancing Human Resource Management with Artificial Intelligence: Opportunities, Challenges, and Best Practices. In: Moldovan, L., Gligor, A. (eds) The 17th International Conference Interdisciplinarity in Engineering. Inter-ENG 2023. Lecture Notes in Networks and Systems, vol 928. Springer, Cham, doi:10.1007/978-3-031-54671-6_31

[20] Nagarjuna Reddy Aturi, "Cognitive Behavioral Therapy (CBT) Delivered via AI and Robotics," Int. J. Sci. Res. (IJSR), vol. 12, no. 2, pp. 1773–1777, Feb. 2023, doi: 10.21275/SR230313144412.

[21] Korrapati, Rakesh, Modernizing Data Warehouses: A Comprehensive Guide to Migrating from Teradata to (December 15, 2023), doi:10.2139/ssrn.5139613.

[22] Nagarjuna Reddy Aturi, "The Role of Psychedelics in Treating Mental Health Disorders - Intersection of Ayurvedic and Traditional Dietary Practices," Int. J. Sci. Res. (IJSR), vol. 7, no. 11, pp. 2009–2012, Nov. 2018, doi: 10.21275/SR24914151317.