IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Mitigating Data Security And Compliance Risk In AWS Cloud Migration For The Banking And Finance Sector

(Data Encryption and Protection: Advanced Techniques within AWS for Banking Data)

[1]Sivakumar Ponnusamy,

[1]Senior Data Engineer, Cognizant Technology Solutions, Richmond, Virginia, USA

Abstract: Transferring data to cloud platforms like AWS has gained momentum, particularly in the Banking and Finance sectors of the digital age. While offering advantages, this migration also carries significant data safety and regulatory concerns. This paper investigates the difficulties in ensuring data protection and adherence to regulations while migrating banking and finance organizations to the AWS Cloud. By methodically examining the legal and regulatory framework, we discovered that it encompasses Title V, PCI DSS, GDPR, and CCPA. This framework investigates the relevant laws and guidelines covering industry participants, including S.E.C. Rule 17-a-4(f), Reg-S.C.I., EU Data Protection Directives, FedRAMPs, FIPS 140-2, and NIST-800-171. And thereby, a detailed inquiry brings to complicated web of laws and vulnerabilities. Navigating this terrain requires a suite of tactics based on the collective wisdom of industry experts, AWS best practices, and triumphant real-world examples. This publication offers essential support for companies undergoing cloud migration in the banking and finance industry, shedding light on their challenges and providing actionable recommendations to ensure compliance and robust data protection. These insights might help shape the legislation that aligns with cloud services' compliance requirements.

Index Terms **– Data Security, Data privacy, AWS, Cloud Migration, Banking & finance ,PCI-DSS, SEC Rule 17-a-4(f), Reg-SC.I, EU-Data-Protection-Directives, FedRAMPs, GDPR, FIPS-140-2, and NIST-800-171.**

I. INTRODUCTION

The advent of digital platforms has sparked a significant overhaul of business processes. Dynamic, pliable, and prolific ones supersede classic business modes. The Banking and Finance sectors have escaped the impact of these developments undiminished. This transition towards digital evolution involves the widespread adoption of AWS cloud solutions to bolster operational effectiveness, flexibility, and end-user value [1]. Furthermore, the migration to a digital landscape comes with obstacles. Among these issues, ensuring the protection of sensitive information ranks highest. As more sensitive client information is processed online, safeguarding this data has become crucial. In addition, the Banking and Finance sector faces an array of legal guidelines that dictate the appropriate management of customer data [2]. The legal and regulatory environment includes requirements like Title V of the Gramm-Leach’s-Bliley Acts, which mandates financial institutions safeguard the privacy and security of non-subscribed personal data [3]. Furthermore, it encompasses the Payments Cards Industry Data Security Standards (P.C.I.-DSS), which affect organizations managing, processing, or transmitting cardholder data. Again, other regulatory frameworks such as GDPR and CCPA are also applicable, providing guidelines for the handling and safeguarding personal information [4]. Confronted by these risks, this investigation aims to investigate the dangers related to data security and adherence during AWS Cloud migration within the banking and finance industries. The research examines practical solutions to overcome the identified problems. The goal is to craft an all-encompassing manual tailored to organizations desiring to successfully traverse the intricate terrain of cloud migration while maintaining rigorous data safety and adherence to relevant laws and standards. In the following passage, we investigate the origins of AWS Cloud and its application in the Banking and Finance domain. In addition to our primary topic, we investigate the importance of safeguarding data integrity

1.1 BACKGROUND

AWS, a robust and widely utilized cloud infrastructure provider, boasts an extensive library of over 200 feature-rich services from multiple data center locations worldwide. Both small and large organizations are taking advantage of AWS to achieve economic efficiencies, enhance their responsiveness, and hasten their capacity for creativity. As more organizations within the banking and finance space discover the potential of cloud services, they are turning to AWS and other public cloud platforms with increased frequency [5]. Multiple reasons have led to the embrace of AWS Cloud in this field. AWS scalability facilitates the rapid adaptation of educational institutions to altering student requirements, sparing them from significant financial burdens related to IT infrastructure updates. Moreover, AWS supplies a variety of assets and capabilities that permit enhanced data analysis, resulting in

more astute business choices [6]. While these services offer numerous benefits, they also introduce significant concerns about information safety and legal conformity. The Cloud computing platform of AWS accommodates vast amounts of susceptible client data. Preserving the security of this information is not merely an issue of corporate standing but a legally mandated responsibility [7]. Upholding legal and regulatory requirements is vital in these industries. As stipulated in Title V, financial institutions must ensure the safety and privacy of their customers' information, equivalent to the standards upheld by PCI DSS for companies dealing with credit card data. Furthermore, legal frameworks like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) specify how individual data should be managed and protected [8]. Abiding by these standards is indispensable; any departure can attract hefty punishment. Our analysis will delve deeper into this legal and regulatory framework, examining the laws governing AWS Cloud adoption in the Banking and Finance sectors [9]

1.2 Problem Statement

Accurately identifying and mitigating bot-driven activities, unauthorized activities and malicious IPs while ensuring seamless user access and privacy presents a significant challenge [3].

1.3 Research Objectives

The research objectives of this paper are threefold:

1. To investigate the legal and regulatory framework governing AWS Cloud adoption in the Banking and Finance sector, including Title V, PCI DSS, GDPR, CCPA, S.E.C. Rule 17-a-4(f), Reg-S.C.I., EU Data Protection Directives, FedRAMPs, FIPS 140-2, and NIST 800-171.
2. To identify the primary data security and compliance challenges organizations face during AWS Cloud migration.
3. To propose actionable recommendations and strategies to mitigate data security and compliance risks during AWS Cloud migration for the Banking and Finance sector.

1.4 Paper Structure

To ensure a comprehensive examination of the subject matter, existing research structure-wise looks like this: Section 2 will focus on the legal and regulatory framework; Section 3 will explore research methodologies (challenges in reducing data security and compliance risk); Section 4 will discuss results and discussion such as strategies to overcome challenges; section 5 will explore about ethical consideration; section 6 highlight future trends and advancement and finally, the paper will conclude in Section 7.

II. Legal and Regulatory Framework

The regulatory landscape for Banking and Finance includes strict laws and rules mandating the security and privacy of consumer data. This becomes even more critical when organizations migrate to cloud platforms like AWS, where the digital nature of data storage and transmission exposes them to heightened risks. Here, we will elaborate on the fundamental laws in question [10].

2.1 The Titles-V of the Gramm-Leach-Bliley Acts (GLBA)

The law ensures customers' confidentiality and security of non-public personal data. The AWS cloud platform is subject to the GLBA, and AWS delivers tools for organizations to conform to these regulations [11].

2.2 Payments Cards Industries Data-Securities Standards (P.C.I-D.S.S.)

This is a globally recognized information security standard for organizations that handle cardholder information for significant debits, credits, prepaid, e-purses, ATMs, and POS cards. This standardization enables AWS to accommodate transactions of varying magnitudes [12] seamlessly.

2.3 General Data Protection Regulations (GDPR)

This EU directive covers the utilization and security of personal data about EU citizens, regardless of the location where the data is handled. This framework affords users extensive autonomy over their information and compels companies to secure it diligently. The platform provides the necessary resources to help customers adhere to GDPR rules [13].

2.4 California Consumer Privacy Act (CCPA)

The law provides expanded rights to California residents regarding handling their personal information. AWS offers features to assist organizations in aligning with the C CPA's privacy and security requirements.
Besides these, several vital standards and regulations apply to the Banking and Finance sector:

2.5 SEC Rule 17-a-4(f)

This rule requires certain business records to be in a non-rewriteable, non-erasable format. AWS supports this through features like Object Lock in S3 services [14].

2.6 Regulation Systems Compliance and Integrity (Reg SCI)

With an emphasis on enhancing the technological framework of US security exchanges, AWS offers resources designed to ensure conformity with regulatory requirements.

2.7 EU Data Protection Directive

All EU citizen personal data, as gathered or compiled, is protected by this directive. AWS abides by this guideline, affording appropriate client information safeguards [15].

2.8 Federal Risk and Authorization Management Program (FedRAMP)

Multiple AWS services have FedRAMP authorization, giving customers peace of mind regarding security [16].

2.9 Federal Information Processing Standards (FIPS) 140-2

AWS provides FIPS 140-2 validated endpoints for a range of services for the convenience of US government entities [17].

2.10 NIST 800-171

These procedures concern the security of Privileged Information outside federal channels. NIST 800-171 compliance is achieved through AWS's extensive portfolio of secure services [18]

As cloud migration continues to rise in the Banking and Finance sectors, understanding and complying with these legal and regulatory frameworks is paramount. AWS has taken considerable steps to provide services that align with these regulations, helping organizations navigate this complex landscape. However, it is ultimately the responsibility of the organizations themselves to ensure they are using these services in a compliant manner [19].

III. Research Methodologies

Although cloud migration has the potential to bring about numerous advantages for organizations in the Banking and Finance sector, there are specific challenges related to data security and compliance with regulations. Some of the primary methodologies that arise are listed below [20].

3.1 Data Protection and Privacy

With vast amounts of sensitive customer data being stored and processed in the cloud, ensuring its protection becomes a significant challenge. AWS Cloud provides robust security features; however, misconfigurations can expose data to breaches. Moreover, privacy regulations like GDPR and CCPA mandate stringent controls on data handling, posing additional compliance challenges [21].

3.2 Shared Responsibility's Models:

In AWS's distributed model, AWS takes charge of securing the cloud environment, while clients accept responsibility for protecting their resources in the cloud. Confronting this challenge involves ensuring that clients deploy sufficient safety mechanisms [22].

3.3 Compliance Management

The Banking and Finance sector is heavily regulated, with laws like GLBA and standards like PCI DSS applying to institutions. Ensuring consistent compliance with these regulations, especially during the migration process, is a significant challenge [23].

3.4 Legacy Systems

Many organizations in the Banking and Finance sector operate on legacy systems. Transferring these systems to the cloud can be complex and unsafe, putting data integrity at risk [24].

3.5 Vendor Lock-In

Committing to one cloud Services Company can have potential consequences during any subsequent transfer [7].

3.6 Lack of Expertise

The AWS Cloud platform features a complex array of tools and resources that necessitate specialized expertise for proper configuration and optimization regarding security and conformity. The absence of skill can invite threats to adherence [9].

3.7 Data Sovereignty

Legal frameworks like GDPR enforce limitations on moving sensitive information beyond the EU's boundaries. AWS's global presence makes it hard to abide by data independence regulations and administrate data residence requirements.

Banking and Finance difficulties illustrate the significance of a deliberate strategy when moving to the AWS Cloud. The following chapter explores diverse approaches to address these obstacles and maintain robust data security and adherence [11].

3.8 Theoretical framework

This research paper's theoretical foundation encompasses the legal and regulatory environment governing AWS Cloud adoption in the banking and finance industries, including Title V of the Gramm-Leach-Bliley Acts, PCI DSS, GDPR, and CCPA, along with sector-specific standards such as SEC Rule 17-a-4(f), Reg SCI, EU Data Protection Directives, FedRAMP, FIPS 140-2, and NIST 800-171. This system incorporates cloud computing concepts, highlighting the collective accountability framework while utilizing AWS security features and tools for data safeguard. Moral principles are inherent in the structure, emphasizing the significance of data security, openness, and conscientious AI utilization. The framework provides techniques to overcome challenges associated with conformity management, legacy system compatibility, and vendor independence. Emerging developments and innovations are evaluated, envisaging augmented cloud safety protocols, Blockchain integration, and eco-friendly cloud computing procedures to guide companies during their transition to the AWS Cloud while maintaining rigorous data security, compliance, and moral standards within the banking and finance industries.

IV. RESULTS AND DISCUSSION

An organized strategy is indispensable to effectively navigating the data protection and compliance concerns of the AWS Cloud transition. The following systems (table - 1) can assist in mitigating these challenges [12].

Table 1: Strategies for Data Protection and Compliance in AWS Cloud Migration for Banking and Finance Industries.

Strategy	Results
Understanding the Shared Responsibility Model	A shared security model guides AWS' operations. AWS assumes responsibility for defending its cloud ecosystem against potential threats. Consumers must guarantee the safety of their online content, apps, systems, and networks 'within' the cloud. Grasping and applying this framework can minimize potential security threats [13].
Leveraging AWS Security Services and Features	The platform offers various services designed to ensure the safety of user data. Among these services are IAM and Security Hub, providing control over authentication and authorization through IAM and a unified view of security alerts through Security Hub. Harnessing these services can fortify data protection [14].
Regular Compliance Audits	Frequent reviews are essential to maintaining compliance with the relevant laws and standards governing the sector. By leveraging this tool, organizations may automate compliance and danger management evaluation [15].
Training and Awareness	Companies should allocate funds toward providing training on AWS tools and associated security protocols. AWS offers resources like whitepapers, tutorials, and training programs to enhance knowledge and skills [16].
Data Encryption	The robust offerings of AWS include KMS and Certificate Manager, enabling secure data management. Secure encryption of data during both storage and transmission reduces the likelihood of security vulnerabilities [17].
Engage Expert Assistance	Given the complexity of AWS Cloud and the regulatory landscape, it can be beneficial to engage expert assistance. AWS has a network of partners specializing in security and compliance that can provide valuable guidance [18].
Resilience and Disaster Recovery Planning	AWS assists with preserving, recovering, and preparing for potential failures. One can maintain continuous business operations even if an incident occurs by consistently backing up crucial information and crafting a thorough contingency strategy [19].
Data Sovereignty Management	Organizations can choose where their data is stored using AWS's infrastructure, which spans multiple geographic regions and availability zones worldwide. This can help meet data sovereignty requirements [20].

These tactics furnish actionable measures for navigating complex data security concerns while migrating to the AWS Cloud within the banking and finance sectors. Proper implementation of these methods can lead to a more robust and trustworthy cloud landscape, thereby enabling the successful deployment of AWS services without compromising sensitive information. By employing these techniques successfully, significant risks related to cloud migration in the Banking and Finance industries can be reduced. Subsequently, we will reiterate the primary insights and speculate about potential research directions [20]

V. Ethical Considerations

Ethical considerations are of paramount importance in the context of AWS Cloud migration for the Banking and Finance sector. As organizations transfer sensitive financial and personal data to the cloud, it is crucial to uphold ethical principles that safeguard the privacy, security, and rights of individuals and stakeholders involved [21].

5.1 Data Privacy and Protection

Ensuring the protection of sensitive customer data and respecting individuals' privacy rights is of utmost importance. Organizations must implement robust data privacy policies, obtain proper consent for data usage, and adopt encryption and secure data storage practices to safeguard customer information [22].

5.2 Transparency and Informed Consent

Transparent communication with customers and stakeholders regarding data collection, storage, and usage is essential. Obtaining informed consent ensures that individuals are aware of how their data will be used in the cloud environment [23]. Privacy opt-out notifications in the banking and finance sector during AWS cloud migration are critical in fostering customer control over their sensitive data. These notifications must detail the types of personal information, the purpose behind its usage, and any third parties involved in data processing or sharing. A carefully designed consent system, including clear choices and actions, enables customers to make informed decisions about their involvement. Open discussion fosters regulatory adherence and respects customers' agency. A comprehensive plan is necessary to ensure the smooth implementation of privacy opt-outs. Opportunities to change consent preferences must be accessible anytime, enabling customers to manage their privacy according to their needs and concerns. Consistent attention to client-designated preferences is crucial in fortifying mutual belief and maintaining a secure and compliant atmosphere. Carefully handling privacy preferences during opt-out notifications abides by legal standards and increases client trust, consequently augmenting the accomplishment of AWS cloud migration in the financial sector.

5.3 Responsible AI and Algorithmic Bias

If AI and machine learning algorithms are utilized in the cloud, organizations must address concerns related to algorithmic bias and ensure fair and unbiased decision-making processes [24].

5.4 Employee Welfare and Training

Cloud migration may impact the workforce. Ethical considerations involve providing adequate training and support to employees to adapt to changes and avoid any adverse effects on job security and well-being [7].

5.5 Data Sovereignty and Compliance

Respecting data sovereignty laws and adhering to international data protection regulations, such as GDPR, demonstrates ethical data governance practices and respect for individual data rights [12].

5.6 Ethical Use of AI

As AI technologies become more prevalent in cloud services, organizations must address ethical concerns related to AI algorithms, potential biases, and responsible AI usage to ensure fair and transparent outcomes for customers.

5.7 Regular Security Audits and Penetration Testing

Regular security audits and penetration testing are critical to ensure the safe migration of banking and finance data to the AWS cloud. This process enables institutions to proactively identify and address potential vulnerabilities, thus significantly reducing the risk of data breaches and compliance issues. Regular security audits comprehensively evaluate the existing security architecture and protocols. This entails the review of access restrictions, encryption techniques, firewalls, intrusion detection systems, and several other security measures. The objective is to guarantee practical functionality and adherence to relevant regulatory obligations, such as GDPR, CCPA, or PCI DSS, for all these measures. Penetration testing encompasses the execution of simulated assaults on a system to identify vulnerabilities that hostile actors might potentially exploit. These tests, carried out by cybersecurity experts often referred to as "ethical hackers," provide a pragmatic assessment of the system's security, uncovering possible weaknesses that may not be discernible just from theoretical research. Incorporating regular security audits and penetration testing is critical for financial institutions transitioning to the AWS cloud as a fundamental aspect of their security strategy. They help ensure data security and maintain the trust of customers and stakeholders, which is crucial in the banking and finance sector. Additionally, performing these checks not just once but regularly is recommended, given that new vulnerabilities might arise as systems and threats evolve. AWS offers various tools to facilitate these processes, like AWS Security Hub for continuous security checks and AWS Penetration Testing for simulated cyber-attacks. Organizations should make the most of these tools while considering third-party audits and tests for an unbiased view of their security stance. It's also worth mentioning that AWS adheres to numerous global and industry-specific compliance programs, so it's essential to ensure that your organization aligns its practices with these standards to avoid penalties and other negative consequences.

Organizations will need to address ethical concerns related to data usage, AI algorithms, and potential biases to ensure responsible and ethical use of AI technologies.

VI. Future Trends and Advancements

The future of AWS Cloud migration in the Banking and Finance sector is expected to witness significant advancements and innovations that further enhance data security and compliance. These trends will shape the landscape of cloud adoption, allowing organizations to embrace cutting-edge technologies while maintaining stringent data protection measures [15].

6.1 Enhanced Cloud Security Measures

Advancements in cloud security technologies, such as zero-trust architecture, continuous monitoring, and threat detection, will bolster the overall security posture of cloud environments [16]. AWS is expected to continuously improve its security services and features to stay ahead of emerging threats and comply with evolving regulations. Automation and AI-driven solutions will play a more significant role in detecting and responding to security incidents effectively [18].

6.2 Blockchain for Secure Data Sharing

As data breaches become more sophisticated, the adoption of blockchain technology for secure data sharing and authentication may increase in the Banking and Finance sector. Integration of blockchain technology into cloud platforms will enable secure and immutable data sharing, fostering trust among multiple parties while maintaining data integrity [19]

6.3 Cloud-Native Compliance Tools

Cloud providers *(AWS, Azure, and Google Cloud)* are likely to develop specialized compliance tools that automate adherence to regulatory requirements, simplifying the compliance process for organizations [20].

6.4 Hybrid/Multi-Cloud Strategies

Advancements in hybrid and multi-cloud strategies will offer organizations more flexibility in optimizing their cloud usage and adhering to data residency requirements, [21] providing a more agile and adaptable cloud environment Banking and finance organizations may adopt hybrid and multi-cloud strategies to distribute data and workloads across multiple cloud providers, reducing vendor lock-in and enhancing business continuity/availability in case of infrastructure failures with one cloud solution provider [22].

6.5 Green Cloud Computing

As environmental concerns grow, cloud providers may invest in eco-friendly data centers and adopt sustainable practices, offering "green" cloud services that align with organizations' corporate social responsibility goals [23].

To sum up, prioritizing ethical considerations ensures responsible cloud migration and data handling, while keeping abreast of future trends and advancements empowers organizations to leverage the full potential of AWS Cloud while maintaining robust data security and compliance [24]. Embracing ethical and innovative practices will lead to a more secure, sustainable, and customer-centric cloud environment for the Banking and Finance sector [25]

VII. Conclusion

In conclusion, Cloud migration, specifically to Amazon Web Services (AWS), has been recognized as a critical enabler of digital transformation in the Banking and Finance sectors. Despite its potential advantages, including lower costs, greater scalability & agility, and enhanced customer engagement, this shift presents significant hurdles involving data protection and conformity with legal standards. Our analysis has revealed the labyrinthine nature of regulatory requirements and security risks related to AWS Cloud migration. This research has exhaustively examined legal structures such as Title-V of the Gramm-Leach-Bliley Acts, the Payments Cards Industry's Data Securities Standards (PCI DSS), the General Data Protection Regulations (GDPR), and the California Consumer Privacy Act (CCPA), alongside sector-specific guidelines, including Securities and Exchange Commission (SEC) Rules 17-a-4(f), the Security Exchange Commission (Reg SCI), the European Union's Data Protection Directives, and the Federal Risks and Authorizations Management Programs (Fed-RAMP), Federal Information Processing Standard (FIPS) 140-2, and National Institute of Standards and Technology (NIST) 800-171. Furthermore, we have recognized crucial obstacles that companies may encounter when migrating to the AWS Cloud, such as safeguarding sensitive information and maintaining data privacy, comprehending the shared accountability framework, managing conformity, integrating old systems, averting vendor captivity, and resolving data independence problems. In response to these obstacles, we have developed strategies like adopting a shared duty approach, making use of AWS's extensive security portfolio services, conducting frequent compliance audits, investing in staff training and consciousness programs, encrypting information, collaborating with outside authorities, and creating plans for resilience and disaster recovery. This study offers a valuable guide for organizations in the Banking and Finance sectors embarking on their AWS Cloud migration journey. It also provides a foundation for future research on this topic. As cloud services evolve and the regulatory landscape adjusts in response, ongoing research will be crucial to navigate this dynamic environment effectively. Future research could explore sub-sector specific *(Retail, commercial, mortgage, investments)* case studies of successful AWS Cloud migrations, delving into the challenges and strategies employed to overcome them. Such insights would further enrich the practical guidance for organizations planning cloud migration journeys.

References

[1] Amazon Web Services, "What is Cloud Computing?" [Online]. Available: https://aws.amazon.com/what-is-cloud-computing/. [Accessed: Aug. 3, 2023].

[2] "Best Practices for Mitigating Risks in Virtualized Environments," IEEE Security & Privacy, vol. 18, no. 3, pp. 50-58, 2020, Cloud Security Alliance.

[3] A. Rahim, X. Huang, and V. Sharma, "A comprehensive review on the data security and privacy protection in cloud computing," IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1003-1018, 2021.

[4] U.S. Congress, "Gramm-Leach-Bliley Act," [Online]. Available: https://www.ftc.gov/system/files/documents/plain-language/pdf-0133_glba-plain-english.pdf. [Accessed: Aug. 3, 2023].

[5] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," IEEE Transactions on Information Forensics and Security, vol. 17, no. 6, pp. 1690-1703, 2022.

[6] PCI Security Standards Council, "PCI Security," [Online]. Available: https://www.pcisecuritystandards.org/pci_security/. [Accessed: Aug. 3, 2023].

[7] H. Khurana and M. Chandrasekaran, "Data Security in Cloud Computing," IEEE Potentials, vol. 40, no. 2, pp. 26-32, 2021.

[8] European Commission, "Data protection in the EU," [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. [Accessed: Aug. 3, 2023].

[9] S. Chaudhary, J. Son, M. Shojafar, and A. Jolfaei, "Quantum-Resistant Cryptography for Securing Cloud Data in the Post-Quantum Era," IEEE Cloud Computing, vol. 9, no. 3, pp. 54-63, 2022.

[10] State of California, "California Consumer Privacy Act (CCPA)," [Online]. Available: https://oag.ca.gov/privacy/ccpa. [Accessed: Aug. 3, 2023].

[11] U.S. Securities and Exchange Commission, "SEC Rule 17a-4(f)," [Online]. Available: https://www.sec.gov/rules/final/34-47806.htm. [Accessed: Aug. 3, 2023].

[12] U.S. Securities and Exchange Commission, "Regulation SCI: Final Rule," [Online]. Available: https://www.sec.gov/rules/final/2014/34-73639.pdf. [Accessed: Aug. 3, 2023].

[13] European Commission, "Directive 95/46/EC," [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046. [Accessed: Aug. 3, 2023].

[14] Federal Risk and Authorization Management Program, "FedRAMP Overview," [Online]. Available: https://www.fedramp.gov/about/. [Accessed: Aug. 3, 2023].

[15] National Institute of Standards and Technology, "FIPS PUB 140-2," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf. [Accessed: Aug. 3, 2023].

[16] National Institute of Standards and Technology, "NIST SP 800-171," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf. [Accessed: Aug. 3, 2023].

[17] Amazon Web Services, "Shared Responsibility Model," [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/. [Accessed: Aug. 3, 2023].

[18] Amazon Web Services, "AWS Compliance Resources," [Online]. Available: https://aws.amazon.com/compliance/resources/. [Accessed: Aug. 3, 2023].

[19] Amazon Web Services, "AWS Security Best Practices," [Online]. Available: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf. [Accessed: Aug. 3, 2023].

[20] Amazon Web Services, "Architecting for the Cloud: AWS Best Practices," [Online]. Available: https://d1.awsstatic.com/whitepapers/aws-architecting-best-practices.pdf. [Accessed: Aug. 3, 2023].

[21] Amazon Web Services, "Security Overview of AWS Lambda," [Online]. Available: https://d1.awsstatic.com/whitepapers/Security/Security_Overview_of_AWS_Lambda.pdf. [Accessed: Aug. 3, 2023].

[22] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on RSA," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 333-346, 2021.

[23] A. Alshammari, A. Simpson, and S. Zeadally, "Cloud Computing Security and Privacy: Research Challenges and Opportunities," IEEE Access, vol. 11, pp. 2630-2643, 2023.

[24] V. Thakur and D. S. Kushwaha, "A Review on Security and Compliance in Cloud Services," IEEE Cloud Computing, vol. 7, no. 5, pp. 30-38, 2020.

[25] Amazon Web Services, "AWS & Financial Services," [Online]. Available: https://aws.amazon.com/financial-services/. [Accessed: Aug. 3, 2023].