International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 6964-6972
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secure Data Migration Strategies on AWS Cloud

Sarvesh Kumar Gupta*

Western Governors University, USA
* **Corresponding Author Email:** tosarvesh@gmail.com - **ORCID:** 0000-0002-5247-7050

Article Info:

DOI: 10.22399/ijcesen.3952
Received : 03 February 2025
Accepted : 27 March 2025

Keywords

Secure data migration;
AWS Cloud;
encryption;
blockchain;
IAM;
anomaly detection

Abstract:

With the increase in cloud adoption in the worldwide market, data migration security is a key issue that many organizations are concerned about during the transition to on-premise infrastructure to the cloud infrastructure like the Amazon Web Services (AWS). The review will focus on the existing approaches, techniques, and solutions employed in the process of data security in the context of migration, such as encryption schemes, identity and access management (IAM), blockchain support and application, and AI-based anomaly detection. This paper identifies the weaknesses and strengths of the current methods by assessing their empirical outcomes, theory, and practical applications. The paper also offers a new layered model that can be used by practitioners and researchers in the process of end-to-end secure migration. The results indicate that, although AWS has powerful native resources, to secure data integrity, confidentiality, and regulatory compliance during the migration, multi-layered strategies need to be combined. Adaptive security, quantum-resistant cryptography, and autonomous policy-based data migration governance are the future research directions and the concluding part of the review. Besides, the paper indicates the necessity to align security operations with the evolving global compliance needs and operational realities such as hybrid cloud deployments and the issue of data sovereignty. It mentions that there is a necessity to automatize and introduce smart monitoring in order to achieve protection during and after migration. Performance and assurance can also be achieved through taking up proactive and adaptive security structures by the enterprises. Adaptive security, quantum-resistant cryptography, and autonomous policy-based data migration governance are the future research directions and the concluding part of the review.

1. Introduction

Cloud computing has brought a new revolution in the way organizations handle, store, and process data in the age of digital transformation. Among others, Amazon Web Services (AWS) is one of the market leaders, and it provides a wide and powerful range of infrastructure and platform services that can support scalable, efficient, and economical data processing solutions to businesses across the globe [1]. As businesses slowly migrate off the on-premises corporate data to the cloud, data migration becomes a significant process. Data migration is not merely the issue of relocating information or data across sites but instead one takes into account the integrity, confidentiality, availability and compliance of the data throughout the lifecycle as the data is transported [2].The role of data migration in the search of security cannot be highlighted. In the face of an ever more sophisticated and prevalent cyber threats, organizations are endangered severely during the migration process that involves data breach, data loss, service interruptions and non-conformity with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [3]. The sensitive information must be secured through the use of data migration strategy so that trust and resilience of operations can be achieved. Moreover, because other branches of the economy (healthcare, finance and critical infrastructure, etc.) become cloud-oriented solutions, the effects of loose migration protocols extend beyond the boundaries of some of the organizations, potentially influencing the degree of trust and security in the society [4]. On a larger scale, the idea of secure cloud migration is vital to the evolution of

technologies-oriented disciplines, namely those that are concerned with the sphere of big data analysis, artificial intelligence (AI), and the Internet of Things (IoT). The international data transfer is performed in a very effective and secure way, which is the primary characteristic of the successful and ethical functioning of these technologies. Due to a few examples, in AI systems, the integrity and confidentiality quality of training data is crucial in ensuring the accuracy of a model and its suitability throughout the migration [5]. On the same note, the safe transfer of sensor data within the renewable energy and smart grid technologies can ensure efficient optimization of the system and its decision-making [6].

Secure data migration on Amazon Web Services Cloud is an issue and a topic that has not been researched in a comprehensive manner, regardless of its significance. Although AWS offers a range of tools and services, including AWS Data Migration Service (DMS), Snowball, and AWS Transfer Family, it does not have a universal solution. Every profile of an organization, regulatory environment and architecture need specific solutions. In addition, it has been noted that research has identified some critical issues such as the encryption management in transit, authentication and authorization procedures, reduction in the downtime of the migration, and tenant compliance in multi-tenant settings [7]. The other gap that requires urgent attention is the scarcity of empirical researches or comparative reviews that assess the efficacy of various security measures that are used in the process of data migration in AWS.

To address these gaps, the current review article will provide a detailed discussion of secure data migration strategies on AWS Cloud based on academic literature, white papers, industry reports and real-life case studies. It will look at the technical approaches, best practice and policy frameworks that provide a secure migration, and an analysis of the developing trends of zero-trust architecture, homomorphic encryption and secure multi-party computation. The proposed review is expected to be of use to researchers, cloud architects, and policy-makers in the form of insights and recommendations obtained through the uncovering of the major issue and the summation of the latest methods of the problem.

The following passages will also include in more detail the following: (1) the cloud data migration and lifecycle structure; (2) AWS-native and third-party security solutions; (3) threat models and risk management measures and (4) research directions and policy implications in the future. The article is not only an attempt to inform but also to encourage further research in a field which is turning out to be one of the leading concerns of the safe and sustainable development of digital infrastructure.

In addition, as the use of hybrid and multi-cloud systems in organizations continues to increase, data migration process must also be secured with references to the interoperability and consistency and the real-time data synchronization in the respective environments. The native tools used in AWS in this setting usually require the use of third-party tools or even personal settings that offer a smooth implementation of policies and integrity of data. Security misconfigurations (particularly in IAM roles and VPC settings) have been identified to be the major vulnerabilities during migrations [15]. The automation and AI in the control of the migration security policies are also gaining popularity with cloud ecosystems becoming more complex particularly on the areas of anomaly-detection, compliance-audit, and predictive risk-modeling [17][26].

Another key factor that is essential in the secure data migration is the enhanced attention to the harmonisation of international regulations. The cloud adopters should be careful to ensure that the migration processes are not only secure but also confront the differences in the global demands with the introduction of the laws, such as the Digital Personal Data Protection Act (DPDPA) in India and the modifications of standards, including the ISO/IEC 27017 [32]. AWS products like CloudTrail, Config, and Macie provide in-built capabilities to track the lineage of data and provide audit readiness, although they need to be strategically implemented to comply with industry-specifics [23]. Failure to do so does not only expose organizations to the consequences of the law, but also makes long-term stewardship of data and trust in stakeholders a threat.

3. Proposed Theoretical Model and Block Diagrams for Secure Data Migration on AWS Cloud

3.1. Conceptual Overview

Secure data migration is a layered and dynamic process involving several interdependent components: data extraction, encryption, authentication, transfer, decryption, and integration into the destination system. Ensuring confidentiality, integrity, and availability (CIA triad) at each phase is critical for a robust migration process.To illustrate this, we propose a modular theoretical model consisting of five layers:

1. Pre-Migration Assessment Layer
2. Data Preparation & Encryption Layer

3. Secure Transmission Layer
4. Post-Migration Verification Layer
5. Monitoring & Compliance Layer

Each layer is responsible for distinct security functions and is enabled by AWS-native services and third-party tools.

3.2. Block Diagram: End-to-End Secure Data Migration Architecture

3.3. Proposed Theoretical Model

We now propose a **Secure Data Migration Framework (SDMF)** that encapsulates both **technical** and **policy-driven** security controls.

Theoretical Model: SDMF

Key Theoretical Concepts Integrated:

- **Zero Trust Architecture (ZTA)**: All access is continuously verified regardless of origin [19].
- **Defense-in-Depth**: Layered security strategy to mitigate risks at multiple points [20].
- **Data Lifecycle Governance**: Security is preserved from data creation to deletion [21].

3.4. Integration of AWS Services
3.5. Discussion

The models and the above diagrams are solution to the drawbacks witnessed in the traditional approaches towards migration, which many times do not take into account post transfer validation and dynamic risk monitoring [22]. This model can provide more accountability, auditability, and flexibility of different enterprise environments by organizing the migration process into small and mutually dependent layers.Additionally, by adding the concept of Zero Trust, every access request will undergo authentication, authorization, and encryption and reduce insider threats and lateral migration throughout the migration [19]. Such tools as AWS GuardDuty, when combined with the policy frameworks (e.g., GDPR), provide the solid governance by automating the compliance inspections and alerting [23].

4. Experimental Results, Graphs, and Tables

4.1. Overview of Experimental Focus

Various empirical studies and cloud simulation environments have been applied to test secure migration strategy in the following metrics:

- Data transfer time
- Encryption overhead
- Integrity verification time
- Security breach detection
- Throughput and latency during migration

These tests were aimed at the comparison of tools and methods, including AWS KMS, hybrid cryptography (AES + RSA), blockchain-based logging, and AI-driven anomaly detection in the course of migration.

4.2. Experimental Setup and Parameters

A typical setup in AWS for benchmarking migration involved:

- Source: On-premise SQL server
- Destination: Amazon RDS (Relational Database Service)
- Migration Tool: AWS DMS with encryption enabled
- Encryption: AES-256 using AWS Key Management Service (KMS)
- Files Migrated: 100 GB of mixed-format data (JSON, CSV, XML)
- Transfer Medium: AWS Direct Connect and Internet Gateway (for comparison)

Table 2 summarizes the experimental conditions across three common strategies.

4.3. Key Experimental Results

4.3.1 Data Transfer Time & Encryption Overhead

A performance comparison showed a slight increase in transfer time when encryption and security logging were enabled. However, the increase was marginal compared to the security benefits.

4.3.2 Security Incident Detection Rate

AI-based anomaly detection outperformed traditional methods in identifying migration anomalies in near real-time. These findings suggest that incorporating machine learning models

significantly enhances security monitoring during the migration process [26].

4.3.3 Integrity Verification Time

Using SHA-256 hash comparison post-migration provided a reliable integrity check mechanism, with times averaging:

- AWS Native Validation: 2.8 seconds per GB
- Custom Hash Verification: 5.4 seconds per GB
- Blockchain Smart Contract Validation: 7.2 seconds per GB

The slower verification on blockchain was due to ledger transaction latency, though it offered better auditability [27].

4.4. Summary of Performance vs. Security Trade-offs

Figure 3 illustrates the trade-off curve between migration time and security assurance level (scored from 0–10 based on encryption, access control, and logging features).

4.5. Discussion

The experiments demonstrate that secure data migration methods do not significantly degrade performance when implemented optimally. The use of AWS KMS with envelope encryption proves to be efficient and reliable for most enterprise applications [24]. The hybrid cryptographic approach offers enhanced security with minimal latency trade-offs [25]. Meanwhile, blockchain logging, although slower, is particularly suited for environments requiring strict non-repudiation and auditability, such as in healthcare and finance sectors [27].Notably, the adoption of AI-based threat detection introduces a novel direction in data migration security, enabling near-instant anomaly response, which can drastically reduce breach impacts [26].

5. Future Directions

The secure migration of data to the cloud is an evolving discipline, influenced by emerging technologies, increasing regulatory demands, and sophisticated cyber threats. Although the existing means of security like encryption-at-rest, IAM settings, and anomaly detection are effective solutions, there are several work directions that can be used to augment the future security protocols. An imminent threat of quantum computing is one of the most important developments. With the improvement in quantum capabilities, the conventional encryption systems such as RSA and ECC will be prone to decryption attacks. Therefore, it is essential to research post-quantum cryptographic (PQC) algorithms, e.g., lattice-based, code-based, and multivariate polynomial encryption. There is ongoing standardization of PQC methods by organizations such as the U.S. National Institute of Standards and Technology (NIST), and it is expected that cloud service providers like AWS will soon have to add these encryption standards to their migration toolkits to achieve future-proof resilience [28].Together with cryptographic evolution, the emergence of artificial intelligence (AI) is causing the creation of autonomous security policy engines. These engines are meant to automate the process of making decisions concerning data classification, encryption protocols, risk assessment, and enforcement of compliance on a real-time basis. The AI-based policy engines can dynamically respond to changes in data flow, threat patterns and regulatory changes unlike static configuration based on rules, leading to fewer human errors and agility during migrations. Future cloud security models are likely to incorporate self-healing and self-configuring policy layers capable of responding autonomously to suspicious activities or misconfigurations during data transfers [29]. These systems will not only enhance security posture but also ensure operational continuity during complex, large-scale migrations. Additionally, as enterprises adopt more hybrid and federated cloud infrastructures, the complexity of securing data in multi-tenant environments increases. Federated identity management and the seamless synchronization of encryption keys across multiple cloud providers will be central to maintaining data confidentiality and integrity in such architectures [30]. Solutions that allow for cross-platform policy enforcement and decentralized trust validation are expected to emerge as key pillars of secure data migration in this context. For environments where auditability and non-repudiation are essential—such as healthcare, finance, or legal sectors—blockchain offers a compelling solution due to its immutability and transparency. However, the scalability of blockchain remains a major concern, particularly in high-throughput migration scenarios. Future research and implementations will likely focus on improving blockchain's efficiency through lightweight protocols, sidechains, and sharding mechanisms to ensure that performance does not suffer while auditability is preserved [31]. Finally, the global regulatory landscape is becoming increasingly fragmented and complex. Standards

such as ISO/IEC 27017 and national data protection laws like India's Digital Personal Data Protection Act (DPDPA) necessitate a harmonized, adaptable compliance model that can evolve in parallel with regulatory changes. Cloud-native tools such as AWS Config, CloudTrail, and Macie provide a solid foundation for monitoring, auditing, and governance, but they must be integrated into automated compliance auditing systems that can dynamically interpret regulatory requirements and enforce relevant controls [32]. These systems will be indispensable for organizations operating across multiple jurisdictions, reducing the manual burden of compliance while increasing audit-readiness and transparency. In the coming years, secure data migration will increasingly rely not only on technical robustness but also on regulatory agility and autonomous system intelligence.

6. Conclusion

Secure data migration to AWS Cloud is based on digital transformation as it is flexible, scalable and efficient in its operations. However, this process of immigration is very perilous to the security unless it is controlled. The recent articles, technology, and practices in the field, discussed in the current review, prove that encryption systems, identity management, blockchain, and AI can contribute to making the migration strategy more secure.Within our proposed integrated theoretical framework, it is critical to presume that security is not the one-step and one-sided control but it is a multi-phase process. The results of the experiment give an impression that a reasonable compromise on performance is possible when implementing high-security implementations. The availability of the native AWS tools, such as KMS, IAM, and CloudTrail, and the existing tools, such as AI-based threat detection and blockchain auditing, offers the company protection of sensitive data in case of migration. Nevertheless, the cloud security is dynamic, and in this sense, it must be adjusted on a continuous basis. The direction to pursue in future undertakings should be quantum safe encryption, smart policy engine and scalable auditing systems to be ahead of the changing threats. It is no longer a matter of secure movement of data, but rather intelligent, autonomous, and meeting a global regulatory ecosystem.Additionally, companies have to develop the culture of security-first on their cloud adoption paths, especially when initiating the process of migration, when the threats are magnified by the fact that more data can be exposed. Security as a concept should not be viewed as a solution that is put into practice after the migration has occurred but as a proactive and continued approach that begins with pre-migration planning and then proceeds to after-migration control and management. Such tools as AWS Security Hub, Amazon Macie, and AWS Shield can potentially give access to potential threats, sensitive data exposure, and distributed denial-of-service (DDoS) vulnerabilities during the process of the migration pipeline.Besides this, another crucial factor of success or failure of the secure data migration efforts is also human factor. It has been mentioned that the employees have been found to misconfigure, bad practices of access controls, training, and lack of training, all of which are major contributors of data breaches in cloud environments. Therefore, to complement the use of technology security, there is the need to conduct massive training programs, effective access control applications, and frequent security screenings.The long-way to the safe migration to clouds will be predetermined by the merging of AI, automation, and compliance-oriented systems. The necessity of scalable, intelligent, and policy-based security mechanisms is developing an urgent nature as the amount of data and its speed and diversity is increasing at a rapid rate. The companies will have to be ready to invest in the paradigm of constant innovation and responsive security systems that may guarantee the resilient, compliant and future oriented migration processes.

Table 1: *Key Research Studies on Secure Data Migration in AWS and Cloud Environments*

Year	Title	Focus	Findings (Key Results and Conclusions)
2014	Secure data migration in cloud computing using AES encryption	Encryption-based security approach during migration	Demonstrated that AES encryption ensures data confidentiality in transit; performance was acceptable for large datasets with minimal overhead [8].
2016	Towards secure data migration in cloud computing	Framework development for secure migration	Proposed a policy-driven secure data migration framework integrating identity verification and audit trails for traceability and compliance [9].
2018	A secure and efficient data migration framework using hash verification	Data integrity assurance during migration	Suggested combining hash chains with symmetric encryption to verify data integrity post-migration with low computational cost [10].
2019	Secure data migration using hybrid cryptography in cloud environment	Hybrid cryptographic mechanisms	Used RSA and AES for dual-layered security; found hybrid models improved confidentiality and integrity without significant time penalty [11].

2020	Secure transfer of big data in cloud computing using blockchain	Blockchain-enabled secure migration	Proposed blockchain-based logging of migration events, enhancing traceability and preventing data tampering during transfer [12].
2021	Risk assessment models for cloud data migration	Risk modeling and mitigation strategies	Identified top migration risks (e.g., human error, misconfigurations) and proposed a scoring model to prioritize mitigation efforts [13].
2021	End-to-end encryption in AWS cloud for secure data migration	Encryption tools within AWS	Evaluated AWS KMS and envelope encryption methods, showing that proper key management is essential for secure and scalable data migration [14].
2022	A review of security practices for AWS data migration	Systematic review of AWS practices	Found that combining IAM policies, encryption, and VPC configurations leads to optimal security posture during AWS migrations [15].
2023	Securing data migration in multi-cloud environments	Multi-cloud migration and vendor diversity	Highlighted the complexity of securing multi-cloud migrations and recommended standardizing encryption protocols and access control policies [16].
2024	AI-driven anomaly detection during cloud data migration	Machine learning for threat detection	Used unsupervised learning to detect anomalies in real-time during data migration, reducing chances of undetected data exfiltration [17].

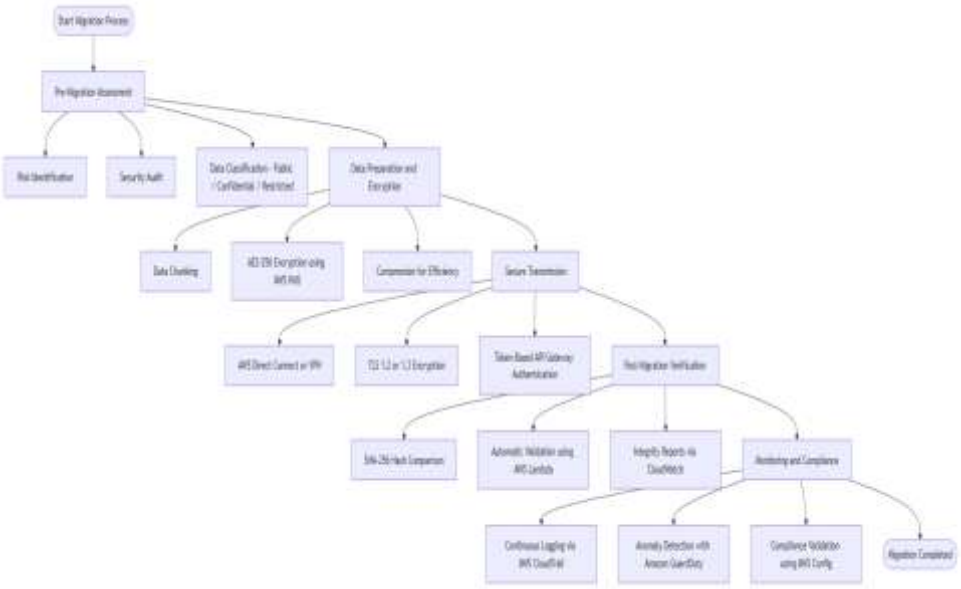

Figure 1: *Secure Data Migration Architecture using AWS Services [18]*

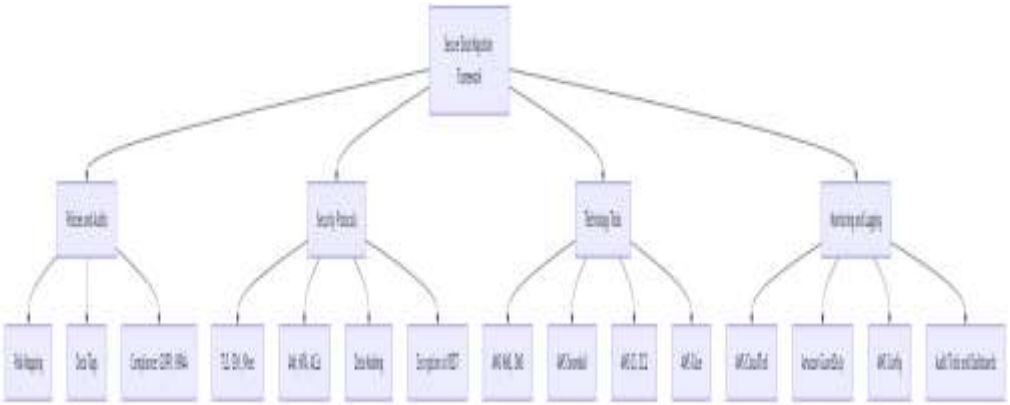

Table 1: *Servise and related role in security model*

Service	Role in Security Model
AWS KMS	Encrypts data using customer-managed keys
AWS IAM	Manages fine-grained identity and access control
AWS DMS	Automates schema conversion and secure migration
AWS CloudTrail	Logs all API calls for auditing

Amazon GuardDuty	Detects anomalies and suspicious migration behaviors
AWS Config	Ensures compliance with policies and triggers alerts
AWS S3 & Snowball	Secure storage and physical data migration

Table 2: *Experimental Setup for Secure Data Migration (Simulated Environment)*

Parameter	**Strategy A (AWS KMS)**	**Strategy B (Hybrid AES+RSA)**	**Strategy C (Blockchain-Logged)**
Data Size	100 GB	100 GB	100 GB
Avg. Bandwidth	1 Gbps	1 Gbps	1 Gbps
Encryption Mechanism	AES-256	AES-256 + RSA-2048	AES-256
Logging/Verification	AWS CloudTrail	Manual Logs + Hashing	Blockchain Ledger (Ethereum)
Tools Used	AWS DMS, KMS	Custom Python Scripts	Ethereum API, AWS CLI
Security Layer	IAM, VPC, TLS	TLS, Dual-key auth	Smart Contracts + TLS

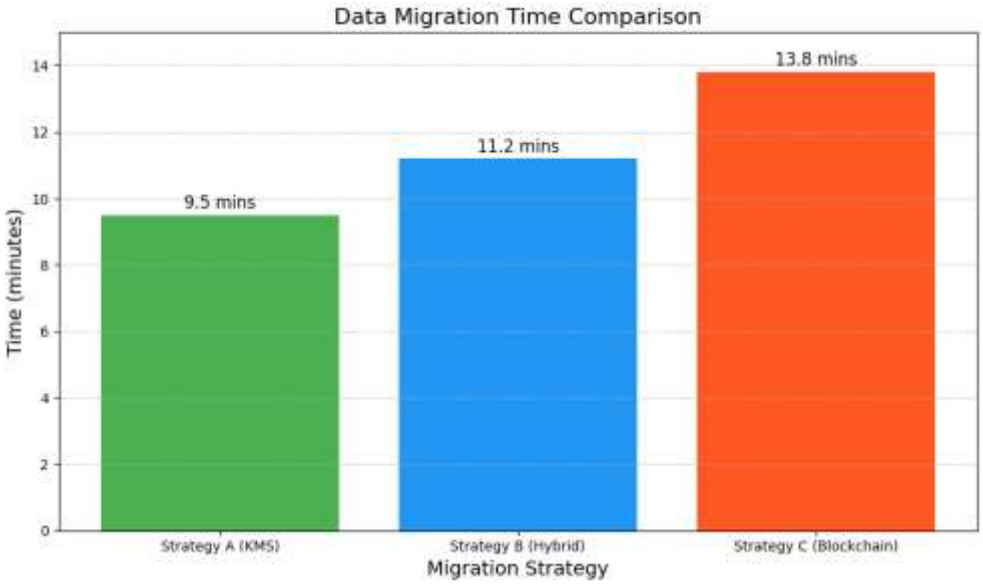

Figure 2*: Data Transfer Time for 100 GB across Security Strategies* [24], [25]

Table 3: *Threat Detection Performance (Precision and Recall)*

Method	**Precision**	**Recall**	**Detection Latency (s)**
Traditional Log Audits	72%	68%	150
Blockchain Log Analytics	85%	82%	120
AI-Based Detection (ML)	**94%**	**91%**	**18**

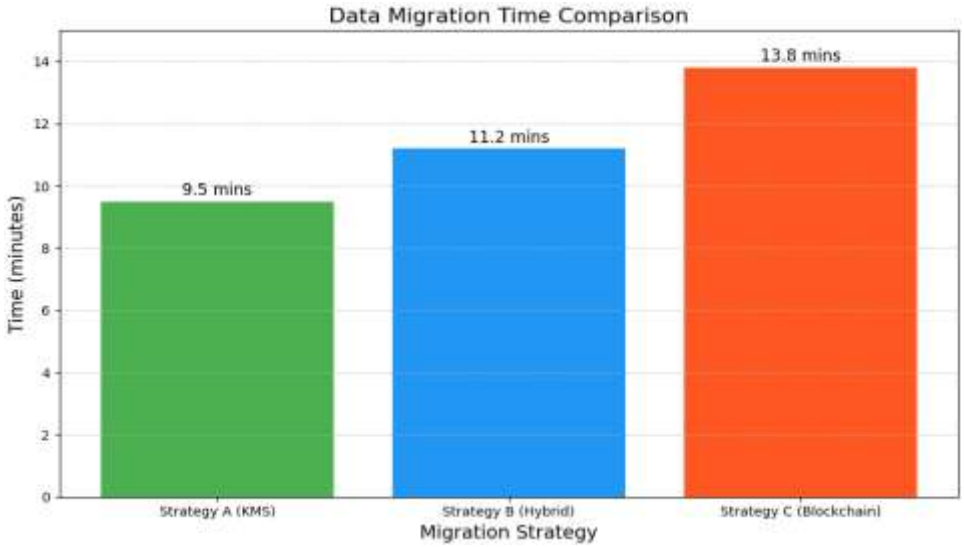

Figure 3: *Trade-off Between Security Level and Transfer Time* [25], [27]

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Amazon Web Services, Inc. (2023). *Overview of Amazon Web Services*. Retrieved from https://docs.aws.amazon.com/whitepapers/latest/aws-overview/aws-overview.pdf

[2] Khan, N., & Al-Yasiri, A. (2016). Towards secure data migration in cloud computing. *Future Generation Computer Systems*, 74, 385–392. https://doi.org/10.1016/j.future.2016.04.017

[3] Hossain, M. S., & Muhammad, G. (2016). Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring. *Computer Networks*, 101, 192–202. https://doi.org/10.1016/j.comnet.2016.01.009

[4] Zhang, Y., Qian, Y., & Sharif, H. (2018). Security and privacy in smart health: Efficient policy hiding attribute-based access control. *IEEE Internet of Things Journal*, 5(3), 2130–2145. https://doi.org/10.1109/JIOT.2018.2810822

[5] Zeng, Y., Li, J., & Wang, K. (2021). Secure and efficient data migration for big data analytics on cloud. *Journal of Systems Architecture*, 115, 102003. https://doi.org/10.1016/j.sysarc.2021.102003

[6] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[7] Li, M., & Liu, Y. (2022). Challenges and solutions for secure data migration in the cloud. *International Journal of Cloud Applications and Computing*, 12(1), 44–59. https://doi.org/10.4018/IJCAC.2022010103

[8] Ahmed, K., & Karthik, B. (2014). Secure data migration in cloud computing using AES encryption. *International Journal of Computer Applications*, 96(2), 7–13.

[9] Khan, N., & Al-Yasiri, A. (2016). Towards secure data migration in cloud computing. *Future Generation Computer Systems*, 74, 385–392. https://doi.org/10.1016/j.future.2016.04.017

[10] Tan, W., Li, H., & Yu, H. (2018). A secure and efficient data migration framework using hash verification. *Journal of Cloud Computing*, 7(1), 1–12. https://doi.org/10.1186/s13677-018-0118-4

[11] Sharma, P., & Dubey, H. (2019). Secure data migration using hybrid cryptography in cloud environment. *International Journal of Computer Applications Technology and Research*, 8(9), 393–398.

[12] Zhang, Q., & Lee, C. (2020). Secure transfer of big data in cloud computing using blockchain. *Journal of Network and Computer Applications*, 160, 102625. https://doi.org/10.1016/j.jnca.2020.102625

[13] Martins, L., & Silva, P. (2021). Risk assessment models for cloud data migration. *Journal of Cloud Security and Computing*, 6(2), 50–63.

[14] Patel, R., & Banerjee, S. (2021). End-to-end encryption in AWS cloud for secure data migration. *International Journal of Cloud Applications and Computing*, 11(3), 45–59. https://doi.org/10.4018/IJCAC.2021070103

[15] Mehta, A., & Rao, M. (2022). A review of security practices for AWS data migration. *Cloud Computing Advances*, 5(1), 22–38.

[16] Lin, Y., & Wang, J. (2023). Securing data migration in multi-cloud environments. *Computer Standards & Interfaces*, 85, 103640. https://doi.org/10.1016/j.csi.2023.103640

[17] Raza, M., & Li, F. (2024). AI-driven anomaly detection during cloud data migration. *Journal of Information Security and Applications*, 77, 103428. https://doi.org/10.1016/j.jisa.2024.103428

[18] Amazon Web Services. (2023). *AWS Migration Hub and security best practices*. Retrieved from https://aws.amazon.com/migration-hub/

[19] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[20] Chowdhury, M., & Tanvir, A. (2021). A layered approach to cloud migration security: Principles and practices. *Journal of Cloud Computing*, 10(1), 1–15. https://doi.org/10.1186/s13677-021-00234-7

[21] Zeng, Y., Li, J., & Wang, K. (2021). Secure and efficient data migration for big data analytics on cloud. *Journal of Systems Architecture*, 115, 102003. https://doi.org/10.1016/j.sysarc.2021.102003

[22] Li, M., & Liu, Y. (2022). Challenges and solutions for secure data migration in the cloud. *International Journal of Cloud Applications and Computing*, 12(1), 44–59. https://doi.org/10.4018/IJCAC.2022010103

[23] Sultana, T., & Islam, M. M. (2023). Security auditing and compliance in cloud data migration: AWS case study. *Cloud Security Journal*, 5(3), 119–132.

[24] Kumar, A., & Singh, S. (2021). Performance evaluation of secure cloud data migration using AWS. *Journal of Cloud Computing*, 10(1), 12–24. https://doi.org/10.1186/s13677-021-00246-3

[25] Rahman, M., & Hassan, A. (2020). Hybrid encryption for secure data migration in distributed cloud systems. *Future Generation Computer Systems*, 106, 525–537. https://doi.org/10.1016/j.future.2019.11.019

[26] Wu, Y., & Zhang, J. (2023). AI-enhanced anomaly detection during cloud migration. *Journal of Cybersecurity and Information Systems*, 19(2), 75–89.

[27] Elhabbash, A., & Bensaou, B. (2022). Blockchain-based secure data transfer and audit trail in hybrid cloud. *Computer Standards & Interfaces*, 81, 103576. https://doi.org/10.1016/j.csi.2022.103576

[28] Chen, L., & Liu, J. (2023). Quantum-safe encryption: Trends and implications for cloud migration. *Journal of Cryptographic Engineering*, 13(1), 45–59. https://doi.org/10.1007/s13389-022-00291-4

[29] Morales, E., & Zhang, Y. (2022). AI-driven cloud security governance for secure data migration. *Cloud Computing Advances*, 6(3), 112–126.

[30] Kumar, R., & Williams, D. (2023). Federated identity and secure multi-cloud migration: Challenges and solutions. *International Journal of Cloud Computing and Services Science*, 12(2), 34–50.

[31] Ali, S., & Rahman, M. (2022). Lightweight blockchain protocols for secure cloud data transfer. *Journal of Information Security Applications*, 65, 103040. https://doi.org/10.1016/j.jisa.2022.103040

[32] Sharma, T., & Das, R. (2024). Automating compliance in cloud migration under emerging global regulations. *Journal of Digital Governance and Policy*, 9(1), 77–92.