International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Reengineering Digital Trust In Cloud-Native Data Warehouses: A Security-Driven And Analytics-Enabled Framework

Submission Date: December 15, 2025, **Accepted Date:** January 12, 2026,
Published Date: January 17, 2026

Dr. Marisol Ortega
Universidad Nacional Autónoma de México, Mexico

Abstract

The accelerating migration of organizational data infrastructures toward cloud-native data warehousing platforms has profoundly transformed how enterprises generate value, manage risk, and establish digital trust with stakeholders. At the heart of this transformation lies an increasingly complex intersection between distributed systems architectures, cybersecurity governance, intelligent analytics, and socio-technical trust mechanisms. While early generations of database systems were designed primarily for performance and transactional reliability, modern cloud data warehouses such as Amazon Redshift embody a fundamentally different epistemology: they are elastic, service-oriented, algorithmically optimized, and deeply embedded in global networks of data exchange. These characteristics, although enabling unprecedented analytical power, also introduce novel vectors of vulnerability, governance ambiguity, and ethical tension. Drawing upon Worlikar, Patel, and Challa's detailed exposition of Redshift's architectural and operational paradigms, this article positions contemporary cloud data warehousing as a core substrate for digital trust in the data-driven economy (Worlikar et al., 2025).

This study integrates classical and contemporary scholarship on network security, authentication, encryption, and distributed systems governance with emerging literature on artificial intelligence, audit automation, and digital trust frameworks. By synthesizing these traditionally siloed domains, the paper argues that trust in cloud data warehouses is not merely a technical artifact but a multi-layered institutional and computational construct shaped by architecture, policy, algorithmic oversight, and user

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

perception. Historical security models such as firewalls, Kerberos authentication, and public-key cryptography are reinterpreted in light of cloud-native abstractions, while modern analytics platforms are shown to depend on machine learning-driven monitoring and governance to maintain legitimacy and reliability (Bellovin & Cheswick, 1997; Clifford et al., 1998; Adelakun et al., 2024).

Methodologically, the research adopts a critical-analytical synthesis of the provided literature, treating each reference as a conceptual node within a larger theoretical network. Rather than empirically measuring breach frequencies or algorithmic accuracy, the study interrogates how different scholarly traditions conceptualize security, risk, trust, and control in data-intensive environments. The results reveal that cloud data warehouses function simultaneously as technical infrastructures and symbolic institutions of trust, where breaches, audit failures, or ethical lapses reverberate far beyond immediate financial losses. The discussion further demonstrates that digital trust is increasingly mediated by algorithmic governance, compliance automation, and AI-driven surveillance, raising new questions about accountability, transparency, and power asymmetries between platform providers and users.

Ultimately, this article contributes a unified theoretical framework for understanding security and trust in cloud-native data warehousing. It contends that platforms like Amazon Redshift represent not only technological evolutions but also socio-economic reconfigurations of how organizations claim credibility, legitimacy, and reliability in the digital age. By bridging classic security theory with contemporary analytics and governance research, the study offers a foundation for future investigations into resilient, ethical, and trustworthy data infrastructures.

Keywords

Cloud data warehousing; digital trust; cybersecurity governance; distributed systems security; artificial intelligence in auditing; Amazon Redshift

Introduction

The emergence of cloud-native data warehousing has marked one of the most significant epistemic and infrastructural shifts in the history of information systems. Whereas earlier generations of data warehouses were conceived as relatively bounded, organization-centric repositories, contemporary platforms operate as globally distributed, service-mediated, and algorithmically optimized ecosystems that integrate data ingestion, storage, processing, and analytics into a single continuously evolving environment. This transformation has not only altered how data are technically managed but also how organizations conceptualize risk, accountability, and trust in their digital operations. The growing centrality of cloud platforms to economic, governmental, and social life means that failures in data security or

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

integrity no longer remain localized incidents but become systemic events capable of undermining public confidence in digital infrastructures as a whole (IBM Security, 2024).

Within this broader context, Amazon Redshift occupies a particularly influential position as one of the most widely adopted cloud-native data warehousing platforms in the world. As described in Worlikar, Patel, and Challa's comprehensive technical exposition, Redshift embodies a hybrid architectural philosophy that blends massively parallel processing, columnar storage, elastic scalability, and automated optimization to deliver high-performance analytics at scale (Worlikar et al., 2025). Yet the very features that make Redshift attractive to enterprises—multi-tenancy, elastic resource pooling, deep integration with other cloud services, and automated management—also complicate traditional models of security and governance. In a cloud-native warehouse, the boundaries between organizational control and platform provider authority are blurred, creating new forms of dependency and vulnerability that cannot be adequately addressed by legacy security paradigms.

Historically, the study of computer and network security emerged in response to relatively well-defined threats to relatively well-bounded systems. Early theoretical frameworks, such as those articulated by Amoroso, focused on the protection of computational assets through access control, authentication, and cryptographic safeguards in environments where the physical and logical perimeters of a system were largely congruent (Amoroso, 1994). Similarly, early network security research emphasized the role of firewalls, intrusion detection, and protocol-level protections as means of maintaining the integrity of local area networks and client-server architectures (Appelton & Elain, 1997; Bellovin & Cheswick, 1997). These models assumed a relatively clear distinction between trusted internal users and untrusted external actors, a distinction that becomes increasingly tenuous in cloud-native ecosystems where data, computation, and control are distributed across multiple administrative domains.

The problem of authentication illustrates this shift with particular clarity. The development of Kerberos as a network authentication service was predicated on the need to establish trust relationships in open but still relatively structured network environments (Clifford et al., 1998). Kerberos introduced the idea of a trusted third party that could mediate identity verification without exposing sensitive credentials, a conceptual innovation that remains foundational to modern cloud identity and access management. However, in platforms such as Redshift, authentication is embedded within a broader fabric of federated identities, role-based access controls, and automated policy enforcement that operates at scales and speeds unimaginable in the era of early distributed systems (Worlikar et al., 2025). This raises new questions about how trust is constructed, delegated, and audited in environments where both users and machines interact through layers of abstraction.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

Encryption technologies likewise illustrate the evolving nature of security in data-intensive systems. The promotion of public-key cryptography and tools such as Pretty Good Privacy reflected a growing recognition that data needed to be protected not only at rest but also in transit across insecure networks (Elliot, 1998). In cloud data warehouses, encryption has become a baseline expectation rather than an optional enhancement, yet its implementation is deeply intertwined with platform-level key management services and automated lifecycle controls. This dependence on provider-managed cryptographic infrastructures introduces a paradox: while encryption enhances confidentiality, it also centralizes control over the mechanisms that enable decryption, thereby relocating trust from the organization to the cloud provider (Worlikar et al., 2025).

Beyond technical safeguards, the notion of digital trust has gained prominence as organizations increasingly rely on data-driven systems to mediate relationships with customers, regulators, and the public. Reports from Deloitte and McKinsey emphasize that trust in digital systems is not solely a function of technical reliability but also of perceived ethical conduct, transparency, and accountability (Albinson et al., 2022; Boehm et al., 2022). In this sense, a data breach is not merely a failure of security controls but a rupture in the social contract between organizations and their stakeholders. The IBM Cost of a Data Breach Report further underscores this point by demonstrating how the financial and reputational consequences of breaches continue to escalate as data becomes more central to organizational value creation (IBM Security, 2024).

Cloud data warehouses sit at the nexus of these technical and social dimensions of trust. On one hand, they provide the analytical foundations for everything from financial reporting and regulatory compliance to personalized marketing and predictive risk modeling. On the other hand, they concentrate vast amounts of sensitive information within infrastructures that are, by design, shared and remotely managed. This concentration amplifies both the potential benefits and the potential harms of data-driven decision-making. In financial and accounting domains, for example, the integration of artificial intelligence into audit and fraud detection processes promises greater efficiency and accuracy but also introduces new ethical and governance challenges related to algorithmic bias, opacity, and accountability (Adelakun et al., 2024a; Adelakun et al., 2024b).

The literature on distributed systems security has long recognized that technical controls alone are insufficient to guarantee trustworthy outcomes. White's analysis of distributed systems security highlights the importance of governance structures, organizational policies, and human factors in shaping the effectiveness of technical safeguards (White, 1999). Similarly, O'Mahony's work on network management environments emphasizes that security must be understood as an ongoing process of negotiation and adaptation rather than a static configuration (O'Mahony, 1998). These insights are particularly salient in the context of cloud data warehousing, where

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

continuous updates, elastic scaling, and automated optimization mean that the system is perpetually in flux.

Despite the richness of existing scholarship, a significant gap remains in our theoretical understanding of how security and trust are co-constructed in cloud-native data warehousing ecosystems. Much of the classical literature focuses either on low-level technical mechanisms or on organizational governance, while much of the contemporary literature on digital trust and AI-driven analytics treats the underlying data infrastructure as a black box. Worlikar et al.'s detailed account of Redshift provides a crucial bridge between these perspectives by revealing how architectural choices, operational practices, and security controls are intertwined in a modern cloud warehouse (Worlikar et al., 2025). Yet this technical insight has not been fully integrated into broader theoretical debates about trust, risk, and governance in the digital economy.

The present study seeks to address this gap by developing an integrative theoretical framework that situates cloud data warehousing within the broader ecology of digital trust and security. By synthesizing classical security theory, distributed systems research, and contemporary analyses of AI-driven governance, the article argues that trust in cloud data warehouses emerges from the dynamic interaction between technological architecture, institutional norms, and algorithmic oversight. This perspective moves beyond simplistic dichotomies between technical and social factors, instead emphasizing their mutual constitution in shaping the reliability and legitimacy of data-driven systems (Worlikar et al., 2025; Bellovin & Cheswick, 1997).

In pursuing this aim, the article also engages with the growing body of literature on business intelligence, predictive analytics, and supply chain resilience, which underscores the strategic importance of trustworthy data infrastructures for organizational competitiveness (Adewusi et al., 2024a; Adewusi et al., 2024b). These studies implicitly assume the availability of reliable, secure, and well-governed data warehouses, yet they rarely interrogate the conditions under which such assumptions hold. By foregrounding the infrastructural and governance dimensions of cloud data warehousing, this research contributes a critical layer of analysis to debates about digital transformation and organizational performance.

The remainder of this article unfolds as a sustained theoretical and analytical exploration of these issues. The methodology section elaborates the interpretive synthesis approach used to integrate the diverse bodies of literature provided. The results section presents a descriptive and conceptual mapping of how security and trust are articulated across different scholarly traditions in relation to cloud-native data warehousing. The discussion section offers a deep theoretical interpretation of these findings, situating them within broader debates about digital trust, algorithmic governance, and socio-technical systems. Finally, the conclusion reflects on the implications of this integrative framework for future research and practice in the design and governance of cloud-based data infrastructures.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

ISSN-2750-1396

METHODOLOGY

The methodological orientation of this study is grounded in interpretive analytical synthesis, a form of qualitative research that does not attempt to generate empirical measurements but instead seeks to construct theoretically coherent explanations from heterogeneous bodies of scholarly and professional literature. This approach is particularly appropriate for investigating cloud-native data warehousing and digital trust, because the phenomena under examination are not reducible to discrete technical variables. Rather, they emerge from the complex interaction between architecture, governance, security controls, institutional norms, and algorithmic decision-making, all of which are deeply embedded in both historical and contemporary discourses on information systems security and organizational legitimacy (White, 1999; O'Mahony, 1998).

The core rationale for selecting an interpretive synthesis methodology is that cloud data warehouses such as Amazon Redshift are socio-technical systems. They do not merely process data; they shape how organizations understand risk, how regulators evaluate compliance, and how users perceive the reliability of digital services. Worlikar, Patel, and Challa's detailed articulation of Redshift's architectural and operational mechanisms provides a crucial anchor for this analysis, because it translates abstract notions of elasticity, scalability, and security into concrete design principles and operational practices that can be interrogated through the lens of digital trust (Worlikar et al., 2025). By positioning this technical reference alongside classical works on network security and emerging studies on AI-driven auditing and governance, the methodology enables a multi-layered interpretation of how trust is constructed and maintained in cloud-native environments.

The primary data for this study consist exclusively of the provided references, which span more than three decades of research and professional analysis. These sources were treated not as isolated factual repositories but as discursive artifacts that reflect evolving assumptions about security, control, and reliability in distributed information systems. Early works on firewalls, authentication, and cryptography were analyzed to identify foundational concepts of trust and threat, while more recent publications on digital trust, artificial intelligence, and cloud-native architectures were examined to trace how these concepts have been rearticulated in response to technological and organizational change (Bellovin & Cheswick, 1997; Adelakun et al., 2024a).

The analytical process unfolded through iterative thematic coding and theoretical triangulation. First, each reference was read with a focus on how it conceptualized security, risk, or trust in relation to information systems. For example, Amoroso's treatment of computer security emphasizes technical control and policy enforcement as mechanisms for preserving system integrity, whereas Deloitte's digital trust report foregrounds stakeholder perception and ethical governance as equally important

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

ISSN-2750-1396

dimensions (Amoroso, 1994; Albinson et al., 2022). These conceptual differences were not treated as contradictions but as complementary perspectives that illuminate different layers of the same phenomenon.

Second, these thematic insights were mapped onto the architectural and operational features of Amazon Redshift as described by Worlikar et al. (2025). This mapping exercise allowed the study to explore how abstract security principles manifest in specific cloud-native mechanisms such as role-based access control, encryption at rest and in transit, automated scaling, and integration with identity management services. The objective was not to evaluate the technical efficacy of these mechanisms but to interpret their significance within broader narratives of digital trust and organizational accountability.

Third, the analysis incorporated insights from the literature on artificial intelligence and analytics-driven governance. Studies on AI in auditing, fraud detection, and ethical accounting were used to examine how automated decision-making and monitoring reshape the meaning of trust in data-intensive environments (Adelakun et al., 2024b; Adelakun et al., 2024c). These works suggest that as organizations increasingly rely on algorithmic systems to detect anomalies, ensure compliance, and optimize performance, trust becomes distributed across human and machine actors in ways that challenge traditional notions of responsibility and oversight.

A key methodological principle in this study is reflexive contextualization. Rather than treating each reference as an objective statement of fact, the analysis situates each work within its historical and institutional context. For instance, the emphasis on perimeter security in 1990s network security literature reflects an era in which systems were primarily localized and organizationally bounded, whereas the emphasis on digital trust and AI-driven governance in contemporary reports reflects the globalization and platformization of data infrastructures (Appelton & Elain, 1997; Boehm et al., 2022). This contextual sensitivity allows the study to trace how shifting technological paradigms necessitate new conceptualizations of trust and security.

The limitations of this methodology must also be acknowledged. Because the study relies exclusively on secondary sources, it cannot provide empirical validation of specific security controls or breach probabilities. The IBM Cost of a Data Breach Report offers quantitative insights into the financial impact of breaches, but these data are interpreted here as indicators of the broader socio-economic stakes of digital trust rather than as precise measures of system performance (IBM Security, 2024). Similarly, the absence of primary case studies means that the analysis cannot account for organization-specific variations in governance or implementation. Nevertheless, by integrating diverse scholarly and professional perspectives, the methodology offers a robust theoretical foundation for understanding cloud-native data warehousing as a locus of digital trust.

Results

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

The interpretive synthesis of the provided literature reveals a coherent yet multifaceted picture of how security and trust are articulated within cloud-native data warehousing ecosystems. One of the most striking findings is that trust in such systems is no longer anchored primarily in physical or organizational boundaries but in layers of abstraction, automation, and institutionalized control. Worlikar et al. (2025) describe Amazon Redshift as an environment in which compute and storage are decoupled, resources are dynamically allocated, and management tasks are increasingly automated. This architectural flexibility, while enabling unprecedented scalability and efficiency, also means that users must trust not only the platform's technical robustness but also the integrity of its automated governance mechanisms.

From the perspective of classical security theory, this represents a profound shift. Early network security models assumed that threats could be mitigated by controlling access to a clearly defined perimeter, as reflected in the emphasis on firewalls and network segmentation in works by Bellovin and Cheswick (1997) and Neuman (1998). In a cloud-native data warehouse, however, the perimeter is virtualized and fluid, making it impractical to rely on static boundary defenses. Instead, trust is distributed across identity management systems, encryption protocols, and continuous monitoring tools that operate within the platform's internal fabric (Worlikar et al., 2025).

Another key result concerns the role of authentication and identity in establishing trust. The Kerberos model introduced the idea of a centralized authority that could vouch for the identity of users in a distributed environment (Clifford et al., 1998). In Redshift and similar platforms, this model is extended through federated identity systems that integrate organizational directories, multi-factor authentication, and role-based access controls. The literature suggests that these mechanisms do more than prevent unauthorized access; they symbolically encode organizational hierarchies and responsibilities into the technical fabric of the data warehouse, thereby shaping how accountability and trust are operationalized (White, 1999; Worlikar et al., 2025).

The integration of artificial intelligence into auditing and fraud detection further transforms the trust landscape. Studies by Adelakun and colleagues demonstrate that machine learning algorithms can identify anomalous transactions and compliance risks more efficiently than traditional manual processes, thereby enhancing the reliability of financial reporting (Adelakun et al., 2024b; Adelakun et al., 2024c). When such algorithms are deployed within cloud data warehouses, they rely on the integrity and security of the underlying data infrastructure to function effectively. This creates a recursive relationship: the trustworthiness of AI-driven governance depends on the trustworthiness of the data warehouse, while the perceived trustworthiness of the data warehouse is

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

reinforced by the effectiveness of AI-driven controls.

The literature on digital trust emphasizes that stakeholder perception is a critical dimension of this recursive relationship. Deloitte and McKinsey both argue that organizations must demonstrate not only technical competence but also ethical responsibility and transparency to earn the confidence of customers, regulators, and partners (Albinson et al., 2022; Boehm et al., 2022). In the context of cloud data warehousing, this means that security certifications, compliance audits, and public disclosures become performative acts of trust-building that complement technical safeguards. Worlikar et al. (2025) note that Redshift's integration with compliance frameworks and logging services allows organizations to produce evidence of control and accountability, thereby translating technical operations into institutional legitimacy.

The IBM report on data breaches provides a sobering backdrop to these findings by illustrating the escalating costs of trust failures in a data-driven economy (IBM Security, 2024). The financial, legal, and reputational consequences of breaches underscore that trust in cloud data warehouses is not an abstract ideal but a tangible economic asset. This aligns with earlier observations by Burleson and Guynes et al. that security in distributed database environments is as much about protecting organizational value as it is about safeguarding technical assets (Burleson, 1998; Guynes et al., 2000).

Collectively, these results suggest that cloud-native data warehousing has transformed the very meaning of security and trust. Rather than being static properties of a system, they are dynamic, continuously negotiated outcomes of interactions between architecture, governance, and algorithmic oversight. Amazon Redshift, as portrayed by Worlikar et al. (2025), exemplifies this transformation by embedding security and compliance into the operational logic of the platform itself, thereby making trust an emergent property of everyday data processing.

Discussion

The findings of this study invite a deeper theoretical interrogation of what it means to trust a cloud-native data warehouse in the contemporary digital economy. Traditional security theory, rooted in notions of control, boundary, and enforcement, provides only a partial account of the trust dynamics that unfold within platforms such as Amazon Redshift. As Bellovin and Cheswick (1997) observed in the context of early firewalls, security mechanisms both reflect and shape organizational assumptions about threat and authority. In a cloud-native environment, these assumptions are reconfigured by the platform's architectural and institutional characteristics, which relocate significant aspects of control from individual organizations to the service provider (Worlikar et al., 2025).

One of the most profound implications of this relocation is the emergence of what might be

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

termed infrastructural trust. Unlike interpersonal or organizational trust, which is grounded in social relationships and contractual obligations, infrastructural trust is vested in the reliability and integrity of a technological substrate that operates largely beyond the direct visibility of its users. When an organization deploys its data warehouse on Redshift, it implicitly trusts Amazon's ability to manage physical security, network isolation, software patching, and disaster recovery. This trust is not blind, but it is mediated through certifications, service-level agreements, and reputational signals rather than through direct oversight (IBM Security, 2024; Worlikar et al., 2025).

The literature on digital trust underscores that such mediation is both necessary and precarious. Deloitte's analysis emphasizes that trust in digital platforms is built through consistent, transparent, and ethical behavior over time, yet it can be rapidly eroded by high-profile failures or scandals (Albinson et al., 2022). In cloud data warehousing, where multiple organizations share the same underlying infrastructure, a breach affecting one tenant can cast doubt on the entire platform, illustrating the collective nature of infrastructural trust. This collective dimension complicates traditional risk management approaches that treat security as an organization- specific responsibility.

Artificial intelligence further complicates this landscape by introducing new forms of algorithmic authority into the governance of data warehouses. As Adelakun et al. (2024b) argue, AI-driven audit and fraud detection systems can enhance accuracy and efficiency, but they also obscure the decision-making process behind complex models. When such systems are embedded in cloud data warehouses, their outputs are only as trustworthy as the data and infrastructure on which they rely. This creates a layered trust relationship in which users must trust the platform, the algorithms, and the governance frameworks that regulate their interaction.

From a distributed systems perspective, this layered trust can be understood as a form of delegated control. White (1999) observed that distributed systems inherently involve the delegation of authority across multiple nodes and administrative domains. Cloud data warehousing extends this delegation to an unprecedented degree by centralizing infrastructure management while decentralizing data ownership and use. Worlikar et al. (2025) describe how Redshift automates many aspects of performance tuning, scaling, and maintenance, thereby reducing the burden on users but also diminishing their direct control over the system. This trade-off between convenience and autonomy lies at the heart of contemporary debates about cloud governance.

The ethical and legal dimensions of this trade-off are particularly salient in regulated industries such as finance and accounting. Studies on legal frameworks and tax compliance in the digital economy highlight the challenges of ensuring accountability when data and computation are dispersed across cloud platforms (Adelakun et al., 2024d). In such contexts, the data warehouse

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

becomes not merely a technical tool but a juridical space in which regulatory requirements are interpreted and enforced through code. The ability of platforms like Redshift to provide detailed logging, audit trails, and compliance reports thus becomes a crucial component of organizational legitimacy (Worlikar et al., 2025).

At the same time, the concentration of data and computational power in cloud platforms raises concerns about power asymmetries and dependency. Business intelligence and predictive analytics literature often celebrates the strategic advantages conferred by big data and advanced analytics, yet these advantages are contingent on access to reliable and secure data infrastructures (Adewusi et al., 2024a; Adewusi et al., 2024b). When such infrastructures are controlled by a small number of global providers, organizations may find themselves locked into relationships that limit their ability to negotiate terms or exit unfavorable arrangements. This structural dependency introduces a new dimension of risk that is not captured by traditional security metrics.

Counterarguments to these concerns emphasize the robustness and professionalism of major cloud providers. Proponents argue that platforms like Redshift benefit from economies of scale that allow them to invest far more in security, monitoring, and resilience than any individual organization could (Worlikar et al., 2025; IBM Security, 2024). From this perspective, infrastructural trust is justified by empirical evidence of superior performance and reliability. However, this argument presupposes that technical excellence is sufficient to guarantee trust, overlooking the social and political dimensions of digital governance highlighted by Deloitte and McKinsey (Albinson et al., 2022; Boehm et al., 2022).

A more nuanced view recognizes that trust in cloud data warehousing is inherently provisional and contingent. It is continually renegotiated through incidents, audits, regulatory changes, and technological innovation. O'Mahony's observation that security in network management environments is an ongoing process rather than a static state is especially relevant here (O'Mahony, 1998). In a cloud-native warehouse, software updates, configuration changes, and new service integrations constantly reshape the system's security posture, requiring continuous vigilance and adaptation.

This dynamic perspective also opens up new avenues for future research. As AI-driven governance becomes more pervasive, scholars must examine how algorithmic systems interact with human decision-makers in shaping perceptions of trust and responsibility. The integration of machine learning into audit and fraud detection, for example, raises questions about who is accountable when an algorithm fails to detect wrongdoing or produces false positives (Adelakun et al., 2024b; Adelakun et al., 2024c). In cloud data warehouses, where these algorithms operate on shared infrastructure, such questions become even more complex.

Moreover, the globalization of cloud platforms invites comparative studies of how different legal

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

and cultural contexts shape digital trust. While this study draws on a diverse set of references, it remains primarily conceptual. Future work could build on this foundation by examining how organizations in different jurisdictions negotiate their relationships with cloud providers, regulators, and stakeholders in the context of data warehousing (Akinsulire et al., 2024; Adelakun et al., 2024d). Such research would further illuminate the interplay between infrastructure, governance, and trust in the digital age.

Conclusion

This article has advanced a comprehensive theoretical framework for understanding security and digital trust in cloud-native data warehousing ecosystems. By integrating classical security theory, distributed systems research, contemporary analyses of artificial intelligence, and detailed architectural insights from Amazon Redshift, the study has shown that trust in modern data infrastructures is neither purely technical nor purely social. It is an emergent property of socio-technical systems in which architecture, governance, and algorithmic oversight are deeply intertwined (Worlikar et al., 2025; White, 1999).

Cloud data warehouses have redefined the locus of control, relocating critical aspects of security and governance from individual organizations to global platform providers. This relocation creates both opportunities for enhanced resilience and risks of dependency and opacity. The literature reviewed here demonstrates that while advanced security mechanisms and AI-driven governance can strengthen trust, they also introduce new ethical, legal, and institutional challenges that demand ongoing scholarly and practical attention (Adelakun et al., 2024b; Albinson et al., 2022).

Ultimately, the future of digital trust in cloud-native data warehousing will depend on the ability of organizations, platform providers, and regulators to align technical innovation with transparent, accountable, and ethically grounded governance frameworks. By situating Amazon Redshift within this broader theoretical landscape, this study contributes a foundational perspective for understanding how data-driven societies can build and sustain trust in the infrastructures that increasingly mediate their economic and social lives.

References

1. Amoroso, E. (1994). Fundamentals of Computer Security Technology. Prentice-Hall, Englewood Cliffs, NJ.
2. Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, O. D., & Obi, C. O. (2024). A USA Review: Artificial Intelligence in Cybersecurity: Protecting National Infrastructure. World Journal of Advanced Research and Reviews, 21(01), 2263–2275.
3. Worlikar, S., Patel, H., & Challa, A. (2025). Amazon Redshift Cookbook: Recipes for building modern data warehousing solutions. Packt Publishing Ltd.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

4. Albinson, N., Balaji, S., & Chu, Y. (2022). Building Digital Trust: Technology can lead the way. Deloitte Digital Trust Report.
5. Bellovin, S., & Cheswick, W. (1997). Network Firewalls. IEEE Communications Magazine, September, 65–70.
6. Adelakun, B. O., Nembe, J. K., Oguejiofor, B. B., Akpuokwe, C. U., & Bakare, S. S. (2024). Legal frameworks and tax compliance in the digital economy: a finance perspective. Engineering Science & Technology Journal, 5(3), 844–853.
7. IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Security Research Report.
8. Appelton, K., & Elain, L. (1997). Network Security: Is Your LAN Safe? DATAMATION, 39, 45–49.
9. Adewusi, A. O., Komolafe, A. M., Ejairu, E., Aderotoye, I. A., Abiona, O. O., & Oyeniran, O. C. (2024). The Role of Predictive Analytics in Optimizing Supply Chain Resilience. International Journal of Management & Entrepreneurship Research, 6(3), 815–837.
10. Clifford, R., Neuman, B., & Ts'o, T. (1998). Kerberos: An Authentication Service for Computer Networks. IEEE Communications Magazine, September.
11. Adelakun, B. O., Fatogun, D. T., Majekodunmi, T. G., & Adediran, G. A. (2024). Integrating machine learning algorithms into audit processes: Benefits and challenges. Finance & Accounting Research Journal, 6(6), 1000–1016.
12. Guynes, C., Golladay, R., & Huff, R. (2000). Database security in a client/server environment. SIGSAC Review, 14, 9–12.
13. Boehm, J., Grennan, L., Singla, A., & Smaje, K. (2022). Why Digital Trust Truly Matters. Digital/McKinsey Insights.
14. O'Mahony, D. (1998). Security Considerations in a Network Management Environment. IEEE Network, May/June.
15. Burleson, D. (1998). Managing security in a distributed database environment. DBMS, 8, 72–77.
16. Adewusi, A. O., Okoli, U. I., Adaga, E., Olorunsogo, T., Asuzu, O. F., & Daraojimba, O. D. (2024). Business Intelligence in the Era of Big Data. Computer Science & IT Research Journal, 5(2), 415–431.
17. White, D. (1999). Distributed systems security. DBMS, 10, 44–48.
18. Adelakun, B. O., Majekodunmi, T. G., & Akintoye, O. S. (2024). AI and ethical accounting: Navigating challenges and opportunities. International Journal of Advanced Economics, 6(6), 224–241.
19. Neuman, D. (1998). Firewall Follow-Up. Data Communications, March.
20. Elliot, P. (1998). Pretty Good Privacy (PGP). Electronic Frontiers Houston.
21. Akinsulire, A. A., Idemudia, C., Okwandu, A. C., & Iwuanyanwu, O. (2024). Dynamic financial modeling and feasibility studies for affordable housing policies. International Journal of Advanced Economics, 6(7), 288–305.
22. Akinsulire, A. A. (2012). Sustaining competitive advantage in a small-sized animation & movie studio in a developing economy like Nigeria. The University of Manchester, Manchester.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 01 Pages: 48-61
OCLC – 1368736135

23. Adewusi, A. O., Asuzu, O. F., Olorunsogo, T., Iwuanyanwu, C., Adaga, E., & Daraojimba, D. O. (2024). AI in Precision Agriculture. World Journal of Advanced Research and Reviews, 21(1), 2276–2285.

24. Adewusi, A. O., Asuzu, O. F., Olorunsogo, T., Iwuanyanwu, C., Adaga, E., & Daraojimba, O. D. (2024). Technologies for Sustainable Farming Practices. World Journal of Advanced Research and Reviews, 21(01), 2276–2895.

25. Akagha, O. V., Coker, J. O., Uzougbo, N. S., & Bakare, S. S. (2023). Company secretarial and administrative services in modern Irish corporations. International Journal of Management & Entrepreneurship Research, 5(10), 793–813.

26. Adelakun, B. O., Onwubuariri, E. R., Adeniran, G. A., & Ntiakoh, A. (2024). Enhancing fraud detection in accounting through AI. Finance & Accounting Research Journal, 6(6), 978–999.