ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

A Comprehensive Review of Multi-Cloud Distributed Ledger Integration for Enhancing Data Integrity and Transactional Security

Echezona Uzoma[1]; Joy Onma Enyejo[2]; Toyosi Motilola Olola[3]

[1]Information Technology Solutions & Product Development Branch,
Ministry of Public and Business Service Delivery and Procurement, Toronto, Ontario. Canada.
[2]Department of Business Administration, Nasarawa State University, Keffi. Nasarawa State. Nigeria.
[3]Department of Communications, University of North Dakota, Grand Forks, USA.

Publication Date: 2025/04/03

Abstract: The integration of distributed ledger technologies (DLTs) into multi-cloud environments presents a transformative approach to addressing data integrity and transactional security challenges in modern digital infrastructures. This review comprehensively examines the intersection of multi-cloud computing and distributed ledger systems, highlighting their potential to provide decentralized, tamper-proof, and transparent data management solutions across diverse cloud platforms. The paper explores key architectural frameworks, consensus mechanisms, interoperability protocols, and cryptographic models that enable seamless integration while ensuring scalability, reliability, and enhanced security. Furthermore, it analyzes current use cases, such as supply chain management, financial services, and healthcare, where multi-cloud DLT integration mitigates risks of single points of failure, data breaches, and unauthorized access. By identifying emerging trends, technological limitations, and research gaps, this review offers valuable insights into optimizing multi-cloud DLT deployments for robust data integrity and secure transactional processes. The study underscores the growing importance of cross-cloud blockchain interoperability and regulatory compliance in advancing secure and resilient multi-cloud ecosystems.

Keywords: *Multi-Cloud Architecture; Distributed Ledger Technology (DLT); Data Integrity; Transactional Security; Interoperability.*

How to Cite: Echezona Uzoma; Joy Onma Enyejo; Toyosi Motilola Olola. (2025). A Comprehensive Review of Multi-Cloud Distributed Ledger Integration for Enhancing Data Integrity and Transactional Security. *International Journal of Innovative Science and Research Technology*, 10(3), 1953-1970. https://doi.org/10.38124/ijisrt/25mar1970.

I. INTRODUCTION

A. Background and Motivation for Integrating Distributed Ledger Technologies (DLTs) in Multi-Cloud Environments

The rapid evolution of cloud computing has led organizations to adopt multi-cloud strategies, leveraging services from multiple providers to enhance scalability, resilience, and cost-effectiveness. However, this approach introduces complexities in data management, including challenges related to data fragmentation, latency, and security vulnerabilities. Traditional centralized databases often struggle to maintain data integrity and consistency across diverse cloud platforms, necessitating innovative solutions to address these issues. Distributed Ledger Technologies (DLTs), particularly blockchain, offer a decentralized framework for data management that inherently ensures data integrity and transparency. By recording transactions across a network of nodes, DLTs eliminate single points of failure and provide an immutable audit trail, making them well-suited for multi-cloud environments. The integration of DLTs into multi-cloud architectures can address critical challenges such as data synchronization, fault tolerance, and cross-platform interoperability. For instance, Oloruntoba (2025) explores the design of resilient multi-cloud database systems that incorporate DLTs to enhance data integrity and ensure high availability across heterogeneous cloud infrastructures. In sectors like energy derivatives trading, the convergence of cloud computing and DLTs has revolutionized traditional market structures by enhancing operational workflows and security. Marimuthu (2025) discusses how this integration addresses key challenges in trade lifecycle management, market transparency, and regulatory compliance, leading to reduced settlement times and improved risk management capabilities. These advancements highlight the potential of DLTs to transform complex, multi-party processes by providing a secure and efficient framework for data sharing and transaction execution (Ijiga, et al., 2025). The motivation for integrating DLTs into multi-cloud environments stems from the need to overcome the limitations of traditional data

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

management systems in handling the complexities of distributed, multi-provider infrastructures. By leveraging the inherent benefits of DLTs, organizations can achieve enhanced data integrity, security, and operational efficiency, paving the way for more robust and reliable multi-cloud solutions.

B. Importance of Data Integrity and Transactional Security in Distributed Systems

In distributed systems, maintaining data integrity and ensuring transactional security are paramount for the reliability and trustworthiness of the system. Data integrity guarantees that information remains accurate, consistent, and unaltered during storage, processing, and transmission. Transactional security ensures that all operations within a transaction are executed reliably and adhere to the ACID (Atomicity, Consistency, Isolation, Durability) properties, which are critical for preserving system stability and preventing anomalies such as dirty reads or lost updates (Tiamiyu, et al., 2024). The dynamic nature of distributed cloud computing environments introduces complexities in safeguarding data integrity. Data is often replicated across multiple nodes and geographic locations to enhance availability and fault tolerance. However, this replication can lead to challenges in ensuring consistency and protecting against unauthorized modifications. Ghallab et al. (2021) highlight that many integrity and security issues arise from the disparities between clients and service providers, necessitating the involvement of third-party auditors to resolve conflicts and verify data authenticity. In the context of distributed ledger technologies like IOTA, transactional security becomes even more critical. Alavizadeh et al. (2023) discuss the development of a secure algorithm for transaction confirmation in IOTA, emphasizing the need for efficient consensus mechanisms to validate transactions without compromising system performance. Their work illustrates how integrating robust security protocols within distributed systems can mitigate risks associated with transaction processing and data integrity (Ijiga, et al., 2024). Ensuring data integrity and transactional security in distributed systems is not merely a technical necessity but also a fundamental requirement for maintaining user trust and compliance with regulatory standards (Nwatuzie, et al., 2025). Implementing comprehensive security measures, including cryptographic techniques and consensus algorithms, is essential to protect against data breaches, unauthorized access, and to uphold the overall reliability of distributed architectures.

C. Scope and Objectives

The integration of Distributed Ledger Technologies (DLTs) into multi-cloud environments represents a significant advancement in enabling decentralized, secure, and transparent data management across diverse cloud platforms. This review focuses on exploring the architectural frameworks, security considerations, and interoperability challenges associated with embedding DLTs within complex multi-cloud infrastructures. The scope includes a detailed analysis of various DLT models, such as blockchain and Directed Acyclic Graphs (DAGs), assessing their suitability and performance within multi-cloud scenarios. One of the primary objectives of this review is to investigate how DLTs enhance fault tolerance, availability, and data integrity within distributed multi-cloud database systems. The review seeks to identify standardized approaches and best practices that support interoperability, ensuring seamless integration of DLTs across heterogeneous cloud platforms while maintaining robust cybersecurity. Another critical objective is to explore the development and optimization of secure algorithms for transaction confirmation within DLT frameworks operating in cloud environments. This includes analyzing consensus mechanisms and evaluating their role in ensuring transactional security, mitigating potential vulnerabilities, and supporting the integrity of distributed data across multiple cloud service providers. Ultimately, this review aims to synthesize findings from existing studies and industry applications to offer a comprehensive understanding of DLT deployment in multi-cloud environments. It seeks to outline prevailing challenges, propose technical solutions, and highlight future research directions necessary for enhancing data integrity and transactional security in distributed, cloud-based systems.

D. Structure of the Paper

This review paper is systematically structured to provide a comprehensive exploration of multi-cloud distributed ledger integration aimed at enhancing data integrity and transactional security. The paper begins with the Introduction, detailing the background, motivation, scope, and objectives, while establishing the importance of DLTs within multi-cloud architectures. The second section, Overview of Multi-Cloud Computing and Distributed Ledger Technologies, delves into the technical fundamentals, examining cloud deployment models, DLT types—including blockchain, Directed Acyclic Graphs (DAGs), and permissioned ledgers—and their respective characteristics. The third section, Architectural Frameworks and Integration Models, presents detailed multi-layered architectures, cross-platform data synchronization protocols, and interoperability standards essential for seamless DLT integration across heterogeneous cloud environments. Section four, Security, Privacy, and Data Integrity Considerations, offers a critical evaluation of encryption schemes, consensus algorithms, zero-knowledge proofs, and regulatory compliance mechanisms to mitigate cyber threats and data breaches. The fifth section, Use Cases and Application Domains, applies theoretical concepts to practical scenarios such as supply chain provenance, decentralized finance (DeFi), IoT networks, and healthcare data management. In section six, Emerging Trends, Research Challenges, and Future Directions, the paper identifies cutting-edge advancements, unresolved technical challenges, and potential pathways for future research, particularly focusing on scalability, cross-chain interoperability, and AI-driven optimization. The final section, Conclusion, synthesizes the findings, emphasizes key takeaways, and provides strategic recommendations for academia and industry.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

II. OVERVIEW OF MULTI-CLOUD COMPUTING AND DISTRIBUTED LEDGER TECHNOLOGIES

A. Definition and Key Characteristics of Multi-Cloud Architectures

Multi-cloud architecture refers to the strategic deployment of computing, storage, and networking resources across multiple public cloud service providers to optimize performance, enhance resilience, and prevent vendor lock-in. Unlike hybrid cloud models that combine private and public clouds, multi-cloud architectures rely solely on multiple public clouds to meet specific organizational needs while maximizing flexibility and minimizing operational risks (Imran et al., 2020) as represented in figure 1. The fundamental concept is to utilize best-of-breed services from different providers, enabling organizations to avoid dependency on a single cloud vendor while leveraging specialized capabilities such as machine learning, analytics, or edge computing. One of the defining characteristics of multi-cloud architecture is its ability to improve system resilience and fault tolerance. By distributing workloads across several providers, organizations mitigate the risks of service outages, data loss, and cybersecurity threats associated with single-provider reliance (Saxena et al., 2021). Additionally, multi-cloud environments support performance optimization by enabling latency-sensitive applications to run on geographically proximate data centers. Multi-cloud strategies also offer cost advantages by allowing enterprises to choose cost-effective services from various providers and negotiate favorable terms (Ijiga, et al., 2024). Furthermore, the architecture supports compliance with regional data protection laws by selecting providers based on jurisdictional requirements. However, despite these advantages, multi-cloud environments introduce complexities in interoperability, data synchronization, and unified management, requiring robust orchestration frameworks to maintain seamless operations (Imran et al., 2020; Saxena et al., 2021).

Figure 1 titled *"Multi-Cloud Architecture – Definition and Key Characteristics"* visually outlines the foundational concept and structural elements of multi-cloud environments. At its core, the architecture refers to the strategic deployment of services across multiple cloud providers to optimize flexibility, resilience, and performance. Branching from the central node, the definition highlights the use of diverse cloud platforms (public, private, or hybrid) without reliance on a single vendor. The key characteristics further elaborate on essential features: vendor diversification enables organizations to avoid lock-in and maximize service capabilities; fault tolerance and resilience are achieved by distributing workloads across providers to ensure uptime and disaster recovery; performance optimization is supported by geographically placing workloads closer to end-users; and cost efficiency arises from leveraging price variability and dynamic resource allocation. Additionally, compliance and data sovereignty are addressed by selecting cloud providers based on regulatory alignment for storing sensitive data, while integration complexity captures the orchestration and interoperability challenges that arise due to varying APIs, service models, and monitoring tools. Collectively, the diagram demonstrates how multi-cloud architectures balance operational agility with technical complexity, making them a strategic choice for modern, large-scale digital infrastructures.

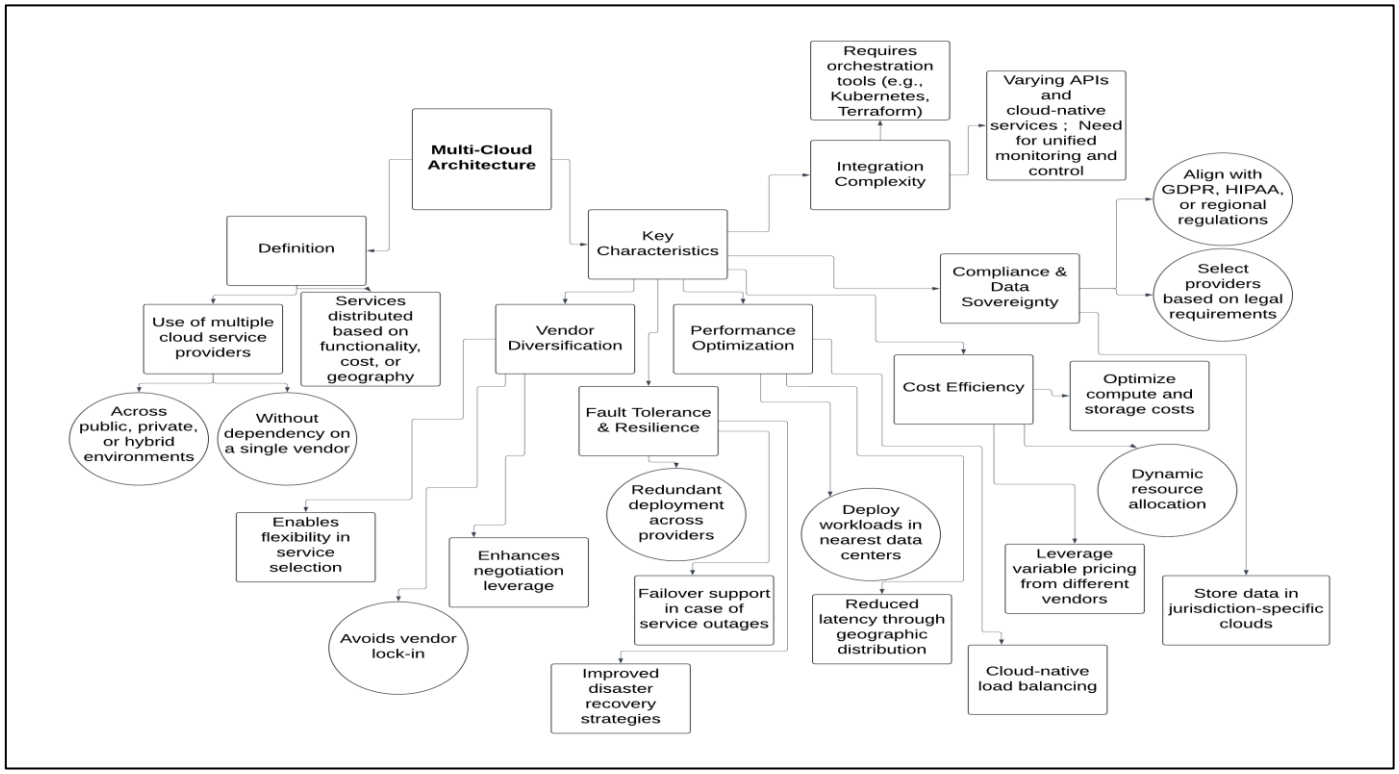

Fig 1: Diagram Illustrating a Hierarchical Overview of Multi-Cloud Architecture Showing the Definition and Core Characteristics Driving Flexibility, Resilience and Strategic Cloud Deployment

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

B. Core Principles of Distributed Ledger Technologies (Blockchain, DAGs, Consortium Ledgers)

Distributed Ledger Technologies (DLTs) underpin decentralized systems by ensuring transparent, secure, and immutable transaction records across a network. Among the prominent DLT structures are Blockchain, Directed Acyclic Graphs (DAGs), and Consortium Ledgers, each with distinct principles and operational frameworks. Blockchain operates on a linear sequence of blocks, where each block contains a batch of transactions. These blocks are cryptographically linked, ensuring that once data is recorded, it cannot be altered without modifying all subsequent blocks—a feat rendered impractical by the network's consensus mechanisms. This structure guarantees data immutability and fosters trust among participants (Benčić & Podnar Žarko, 2018). Directed Acyclic Graphs (DAGs) represent an evolution in DLTs, addressing some limitations inherent in traditional blockchains, such as scalability. In DAG-based ledgers, transactions are structured as vertices in a graph, with each transaction confirming one or more previous transactions. This parallel processing capability enhances transaction throughput and reduces confirmation times. Unlike the linear nature of blockchains, DAGs allow for a more dynamic and scalable approach to data recording (Benčić & Podnar Žarko, 2018). Consortium Ledgers blend elements of public and private blockchains. In this model, a pre-selected group of organizations collaboratively governs the ledger, balancing decentralization with operational efficiency. Access permissions are tiered, allowing consortium members to validate transactions while restricting broader network participation. This structure is particularly advantageous for industries requiring both transparency and confidentiality, such as finance and supply chain management (Dib et al., 2018). Understanding these core principles is essential for integrating DLTs into multi-cloud environments, as each structure presents unique considerations for scalability, security, and interoperability.

C. Benefits and Challenges of DLTs in Multi-Cloud Contexts

The integration of DLTs into multi-cloud environments presents significant benefits in enhancing data integrity, operational resilience, and transparency. By decentralizing data storage and transaction validation across multiple cloud service providers, DLTs reduce reliance on any single vendor, effectively mitigating risks associated with service outages and system failures (Nerella, 2023) as presented in table 1. This architecture improves fault tolerance and ensures that critical operations continue uninterrupted even when a specific cloud platform experiences performance degradation or cyberattacks. Furthermore, the immutability of distributed ledgers guarantees that once data is recorded, it remains tamper-proof, fostering trust among stakeholders and supporting compliance with audit and regulatory requirements (Ijiga, et al., 2024). However, DLT deployment in multi-cloud ecosystems also introduces technical and operational challenges. The lack of standardized interoperability protocols across cloud providers complicates the synchronization of distributed ledgers and consensus mechanisms, increasing the risk of latency and inconsistent data states (Kathiravelu et al., 2018). Managing complex network topologies, varying security models, and regulatory requirements across multiple jurisdictions adds further difficulty. Additionally, the consensus process inherent in DLTs can exacerbate latency in multi-cloud contexts, reducing transaction throughput and system efficiency (Igba, et al., 2024). These challenges underscore the need for robust cross-cloud orchestration frameworks, optimized consensus protocols, and unified security governance to maximize the potential of DLTs in multi-cloud deployments.

Table 1: Summary of Benefits and Challenges of DLTs in Multi-Cloud Contexts

Aspect	Benefits	Challenges	Example/Application
Resilience & Availability	Enhanced fault tolerance through data distribution across multiple clouds	Complex orchestration needed to manage distributed ledger replicas	Multi-cloud blockchain nodes maintaining redundancy in financial networks
Data Integrity & Trust	Immutable and transparent ledger increases data credibility	Latency and synchronization issues across heterogeneous platforms	Tamper-proof medical records synchronized between hospitals using different cloud services
Cost Optimization	Flexibility to choose cost-effective services across vendors	Varying pricing models and lack of unified governance increase management complexity	Dynamically shifting blockchain workloads to lower-cost cloud regions
Security & Compliance	Enhanced auditability and cryptographic protection of transactions	Inconsistent security standards and regulatory frameworks across cloud providers	Healthcare data shared across AWS and Azure requiring unified compliance enforcement

III. ARCHITECTURAL FRAMEWORKS AND INTEGRATION MODELS

A. Design Patterns for Multi-Cloud DLT Integration

DLTs into multi-cloud environments necessitates the adoption of robust design patterns to ensure seamless interoperability, scalability, and security. A prevalent pattern is the partitioned multi-cloud architecture, where distinct components of a DLT application are deployed across multiple cloud providers. This approach allows organizations to leverage specific strengths of each provider, such as computational power or storage capabilities, optimizing overall system performance and resilience (Ghosh, 2023). Another critical design pattern involves the use of interoperability frameworks to facilitate communication between disparate DLT networks operating across various cloud platforms. The Hyperledger Weaver project exemplifies this by providing a set of protocols and tools that enable cross-ledger interactions, ensuring consistent data synchronization and transaction validation across different

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

DLT systems (Belchior, et al., 2023). Implementing these design patterns requires meticulous attention to network topology, data governance policies, and security protocols to mitigate risks associated with data breaches and ensure compliance with regulatory standards (Idoko, et al., 2024).. By strategically deploying DLT components and employing interoperability frameworks, organizations can achieve a cohesive multi-cloud DLT integration that enhances operational efficiency and trustworthiness.

B. Interoperability Layers and Cross-Cloud Communication Protocols

DLTs across multiple cloud platforms necessitates robust interoperability layers and cross-cloud communication protocols to ensure seamless data exchange and transaction processing. Interoperability in this context refers to the ability of diverse DLT systems to interact and share information effectively, despite differences in their underlying architectures and consensus mechanisms as represented in figure 2. A critical component of achieving interoperability is the implementation of standardized communication protocols that facilitate cross-chain interactions. These protocols enable transactions and data to be securely transmitted between disparate DLT networks operating on various cloud infrastructures. For instance, cross-chain messaging protocols have been developed to address the challenges posed by heterogeneity in consensus mechanisms, smart contracts, and token systems, allowing decentralized applications to access data and interact with smart contracts on different chains (Belchior et al., 2022). Furthermore, the network layer plays a pivotal role in the communication infrastructure required to facilitate transactions and data sharing between nodes in a DLT network. This layer encompasses the distributed networking mechanism, communication protocols, and data verification processes essential for maintaining the integrity and consistency of the ledger across multiple cloud environments (Zhang & Lee, 2020). Implementing these interoperability layers and communication protocols requires meticulous attention to security, latency, and compliance considerations (Ibokette, et al., 2024). Ensuring that cross-cloud communications are encrypted and that consensus mechanisms are robust enough to prevent unauthorized transactions is paramount. Additionally, addressing potential latency issues that may arise from cross-cloud interactions is crucial to maintain the performance and reliability of the DLT system.

Figure 2 illustrates the architectural and protocol-based components required for seamless integration across distributed ledger platforms operating within multi-cloud environments. At the core lies Multi-Cloud DLT Interoperability, which branches into two primary domains: Interoperability Layers and Cross-Cloud Communication Protocols. The Interoperability Layers consist of the Protocol Layer, responsible for establishing foundational messaging frameworks and consensus signaling mechanisms that allow blockchain networks to exchange data securely and consistently, and the Application Layer, which facilitates the execution of cross-chain smart contracts and the coordination of decentralized applications (dApps) over heterogeneous cloud infrastructures. On the other side, Cross-Cloud Communication Protocols encompass components such as API Gateways and Service Meshes, which manage service discovery, traffic control, and secure communication across cloud platforms, ensuring that ledger nodes and services remain discoverable and resilient. Additionally, Middleware and Translation Bridges play a crucial role in harmonizing different cloud-native interfaces and data schemas (e.g., RESTful APIs, gRPC, and proprietary blockchain interfaces), enabling interoperability between public, private, and consortium blockchain networks. This diagram emphasizes the importance of modular design, standardized communication stacks, and semantic translation to build resilient, scalable, and interoperable multi-cloud DLT ecosystems.

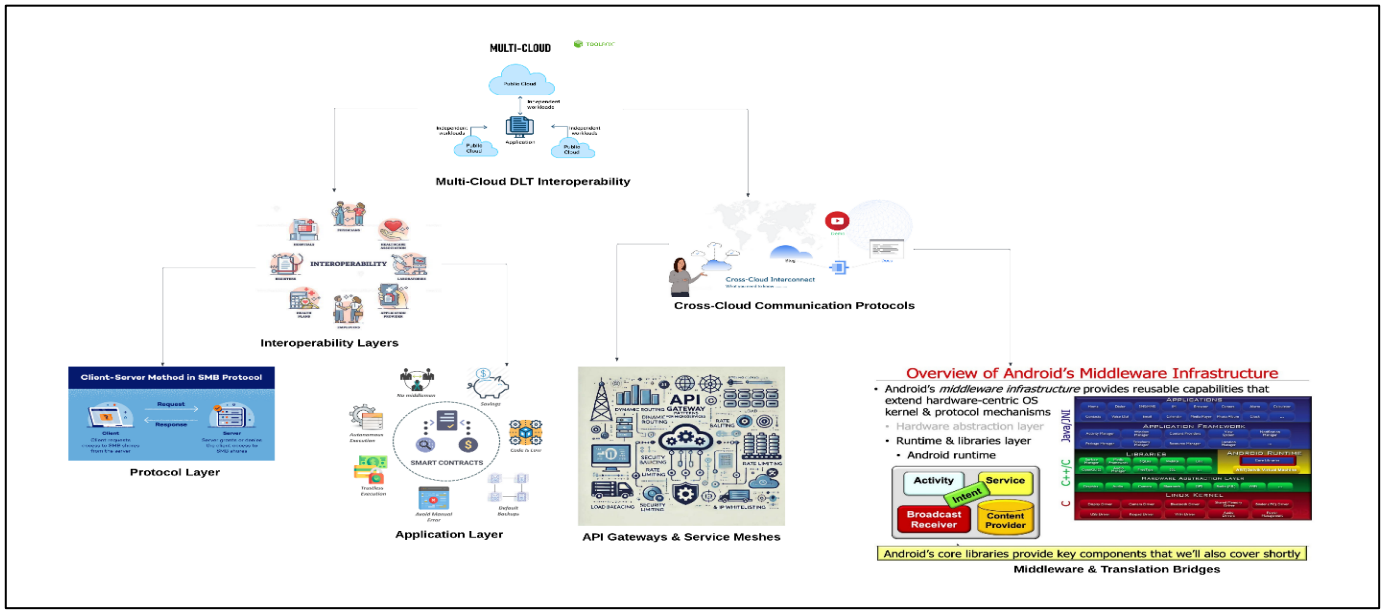

Fig 2: Diagram Illustration of Key Interoperability Layers and Cross-Cloud Communication Protocols Enabling Seamless Integration in Multi-Cloud Distributed Ledger Systems

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

C. *Consensus Algorithms and Their Implications for Multi-Cloud Deployments*

Consensus algorithms are fundamental to DLTs, ensuring agreement among distributed nodes on the state of the ledger. In multi-cloud deployments, where DLT nodes operate across diverse cloud platforms, the choice of consensus mechanism significantly impacts performance, security, and scalability as presented in table 2. Traditional consensus protocols like Paxos and Raft are designed for consistency in distributed systems. However, their applicability in multi-cloud environments presents challenges due to factors such as network latency and partitioning inherent in cross-cloud communications. Li, et al., (2022) highlights that while these protocols maintain data consistency, their performance can degrade in multi-cloud contexts, necessitating adaptations to address inter-cloud latency and fault tolerance. In blockchain-based DLTs, consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) have distinct implications for multi-cloud deployments. PoW, known for its intensive computational requirements, may lead to increased costs and energy consumption when nodes are distributed across multiple cloud providers (Ezeh, et al., 2024).. Conversely, PoS offers a more energy-efficient alternative but requires robust security measures to prevent attacks like long-range attacks, which can be exacerbated in a multi-cloud setup. Emerging consensus algorithms tailored for specific applications, such as the CBCIoT algorithm proposed by Uddin et al. (2021), aim to enhance scalability and efficiency in Internet of Things (IoT) contexts. While designed for IoT, the principles of CBCIoT, which focus on reducing validation and verification times, could inform the development of consensus mechanisms optimized for the complexities of multi-cloud environments.

In summary, selecting an appropriate consensus algorithm for DLTs in multi-cloud deployments requires careful consideration of the unique challenges posed by operating across multiple cloud platforms. Factors such as network latency, security vulnerabilities, and resource availability must be balanced to achieve optimal performance and maintain the integrity of the distributed ledger.

Table 2: Summary of Consensus Algorithms and Their Implications for Multi-Cloud Deployments

Consensus Algorithm	Key Characteristics	Implications for Multi-Cloud Deployments	Example/Application
Paxos / Raft	Ensure strong consistency in distributed systems	Suffer from high latency and reduced performance in multi-cloud setups	Used in traditional distributed databases; not ideal for geographically dispersed nodes
Proof of Work (PoW)	High security through computational effort	Resource-intensive and costly across multi-cloud nodes	Bitcoin-style mining not suitable for cloud resource optimization
Proof of Stake (PoS)	Consensus based on stake held by validators	More energy-efficient; needs secure validator selection across clouds	Ethereum 2.0 model can be adapted for federated cloud DLTs
Byzantine Fault Tolerant (BFT)	Fast finality and high fault tolerance for smaller networks	Challenges in scaling across cloud zones; requires low-latency links	Suitable for consortium blockchains across trusted cloud environments

D. *Smart Contract Deployment Across Heterogeneous Cloud Services*

Deploying smart contracts across heterogeneous cloud services presents unique challenges and opportunities, particularly in achieving interoperability and maintaining security. One significant challenge is the lack of standardized platforms and languages among different cloud providers, which complicates the seamless migration and execution of smart contracts. To address this issue, tools like Osprey have been developed to facilitate the translation of smart contracts between different blockchain platforms, such as converting Solidity-based contracts from Ethereum to Hyperledger Fabric's chaincode. This translation ensures that the functional integrity of the contract is preserved across diverse environments (Belchior, 2024). In addition to migration tools, innovative frameworks have been proposed to enhance the deployment of smart contracts in multi-cloud settings. For instance, the Nubo Virtual Services Marketplace utilizes a decentralized application built on the J.P. Morgan Quorum blockchain to manage tenant and service accounts through static smart contracts written in Solidity. This approach enables multiple cloud and service providers to collaborate in delivering resources to tenants securely and transparently, leveraging the tamper-evident and tamper-resistant properties of blockchain technology (Kempf et al., 2019). Implementing such solutions requires careful consideration of interoperability protocols, security measures, and performance optimization to ensure that smart contracts function effectively across heterogeneous cloud services (Enyejo, et al., 2024). By adopting these strategies, organizations can leverage the benefits of decentralized applications while navigating the complexities inherent in diverse cloud infrastructures.

IV. SECURITY, PRIVACY, AND DATA INTEGRITY CONSIDERATIONS

A. *Threats, Vulnerabilities, and Attack Surfaces in Multi-Cloud DLT Systems*

The integration of DLTs into multi-cloud environments introduces a complex security landscape characterized by diverse threats, inherent vulnerabilities, and expanded attack surfaces. Understanding these challenges is crucial for developing robust security frameworks tailored to such intricate systems as represented in figure 3. A prominent threat in multi-cloud DLT systems is the Sybil attack, where an adversary creates numerous pseudonymous identities to gain disproportionate influence over the network. This can

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

compromise consensus mechanisms and disrupt the integrity of the ledger. Baninemeh et al. (2024) highlight the susceptibility of DLT applications to such attacks, emphasizing the need for stringent identity verification and trust establishment protocols. Another critical vulnerability arises from interoperability issues among heterogeneous cloud platforms. Variations in security policies, authentication mechanisms, and data formats can create inconsistencies that adversaries might exploit. Reece et al. (2023) discuss how these disparities can lead to misconfigurations and unauthorized access, highlighting the importance of standardized security protocols across cloud providers. The expanded attack surface in multi-cloud DLT deployments also includes potential weaknesses in Application Programming Interfaces (APIs), which serve as conduits for cross-cloud communication. Poorly secured APIs can be targeted for data breaches and service disruptions (Ebenibo, et al., 2024). Implementing robust API security measures, such as stringent authentication, authorization, and encryption, is imperative to mitigate these risks. Additionally, the distributed nature of these systems can lead to data fragmentation, where sensitive information is dispersed across multiple jurisdictions, each with its own regulatory landscape. This fragmentation complicates compliance efforts and can inadvertently expose data to unauthorized entities (Enyejo, et al., 2024). Developing comprehensive data governance strategies that account for regional regulations and ensure consistent security practices is essential to address this challenge.

In summary, securing multi-cloud DLT systems requires a holistic approach that addresses identity management, standardizes interoperability protocols, fortifies APIs, and implements cohesive data governance. By proactively identifying and mitigating these threats and vulnerabilities, organizations can enhance the resilience and trustworthiness of their multi-cloud DLT deployments.

Fig 3: Picture of Visualizing Cyber Threats Targeting Multi-Cloud DLT Ecosystems and the Expanding Attack Surfaces in Decentralized Infrastructure (Eze, E. 2024).

Figure 3 shows a hooded individual at a multi-monitor workstation, symbolizing a cybersecurity threat actor targeting sophisticated digital infrastructures, such as multi-cloud Distributed Ledger Technology (DLT) systems. It visually encapsulates the core issues highlighted in *Section 4.1: Threats, Vulnerabilities, and Attack Surfaces in Multi-Cloud DLT Systems*, where adversaries exploit expanded attack surfaces, misconfigured APIs, and inconsistent cloud security protocols. The presence of multiple screens with digital schematics and biometric data reflects the complexity and heterogeneity of cloud environments where decentralized nodes interact across various platforms. This setting illustrates how threats such as Sybil attacks, DDoS campaigns, and data exfiltration are amplified in multi-cloud contexts due to disparate authentication mechanisms and jurisdictional data fragmentation. The interconnected icons, such as padlocks and identity symbols overlaid across the image, signify data sovereignty risks and access control vulnerabilities that arise from inconsistent policy enforcement between cloud providers. The anonymity of the attacker further emphasizes the challenges in attribution and real-time response, stressing the urgent need for standardized security frameworks, cryptographic access controls, and continuous threat monitoring in DLT-enabled cloud ecosystems. This scene encapsulates the fragile balance between decentralized innovation and security resilience in modern blockchain-based infrastructures.

B. Cryptographic Techniques and Data Validation Models

In multi-cloud DLT systems, robust cryptographic techniques and data validation models are essential to ensure data integrity, confidentiality, and authenticity across diverse cloud platforms. One prominent approach involves the integration of homomorphic encryption and blockchain technology. Homomorphic encryption allows computations on encrypted data without revealing the underlying information, thereby preserving privacy during data processing. When combined with blockchain's immutable ledger, this technique facilitates secure computations in hybrid databases within multi-cloud environments, addressing challenges related to unauthorized access and data protection regulations (Oloruntoba, 2025). Another critical cryptographic method is the application of zero-knowledge proofs (ZKPs), which enable one party to prove to another that a statement is true without revealing any information beyond the validity of the statement itself. In the context of DLTs, ZKPs enhance privacy by allowing data verification without exposing the actual data, thus maintaining

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

confidentiality while ensuring integrity (Mohankumar, 2025). This is particularly beneficial in multi-cloud scenarios where data traverses various platforms with differing security protocols. Implementing these cryptographic techniques necessitates addressing challenges such as computational overhead and integration complexity. Homomorphic encryption, while preserving data privacy, can introduce significant performance bottlenecks due to its intensive computational requirements. Similarly, the deployment of ZKPs requires careful consideration of the trade-offs between security and efficiency, as complex proofs can lead to increased latency. Therefore, optimizing these cryptographic methods for practical deployment in multi-cloud DLT systems is an ongoing area of research.

In summary, the convergence of advanced cryptographic techniques like homomorphic encryption and zero-knowledge proofs with DLTs offers promising avenues for enhancing data security and validation in multi-cloud environments. However, balancing the robustness of these methods with operational efficiency remains a critical consideration for their widespread adoption.

C. Privacy-Preserving Mechanisms (Zero-Knowledge Proofs, Homomorphic Encryption)

In the realm of multi-cloud DLT systems, safeguarding data privacy is paramount. Two pivotal cryptographic techniques—Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption (HE)—offer robust solutions to this challenge. Zero-Knowledge Proofs enable a prover to convince a verifier of the truth of a statement without revealing any underlying information as represented in figure 4. This mechanism is instrumental in authentication processes where user credentials must be validated without exposing sensitive data. Fouda, (2024) emphasizes that ZKPs facilitate secure data exchanges, allowing entities to confirm possession of specific information without disclosure, thereby mitigating potential data breaches. For instance, in a multi-cloud environment, ZKPs can authenticate users across different platforms without transmitting actual credentials, enhancing both security and user privacy. Homomorphic Encryption permits computations to be performed directly on encrypted data, yielding encrypted results that, when decrypted, match the outcome of operations performed on the plaintext. Dhokrat et al. (2024) discuss a framework integrating HE with ZKPs to bolster data privacy in cloud-based multiparty computations. This integration allows collaborative data processing across various cloud services without decrypting the data, ensuring confidentiality throughout the computational process. For example, in a scenario where multiple healthcare providers collaborate on patient data analysis across different cloud platforms, HE enables the execution of aggregate computations on encrypted datasets without exposing individual patient records. Implementing these privacy-preserving mechanisms in multi-cloud DLT systems necessitates addressing challenges such as computational overhead and integration complexity. While HE ensures data remains confidential during processing, it can introduce performance bottlenecks due to its intensive computational requirements. Similarly, deploying ZKPs requires careful consideration of trade-offs between security and efficiency, as complex proofs can lead to increased latency. Therefore, optimizing these cryptographic methods for practical deployment in multi-cloud DLT systems is an ongoing area of research.

In summary, the strategic application of Zero-Knowledge Proofs and Homomorphic Encryption significantly enhances privacy preservation in multi-cloud DLT environments. By enabling secure computations and verifications without exposing sensitive information, these techniques address critical privacy concerns inherent in distributed systems spanning multiple cloud platforms.

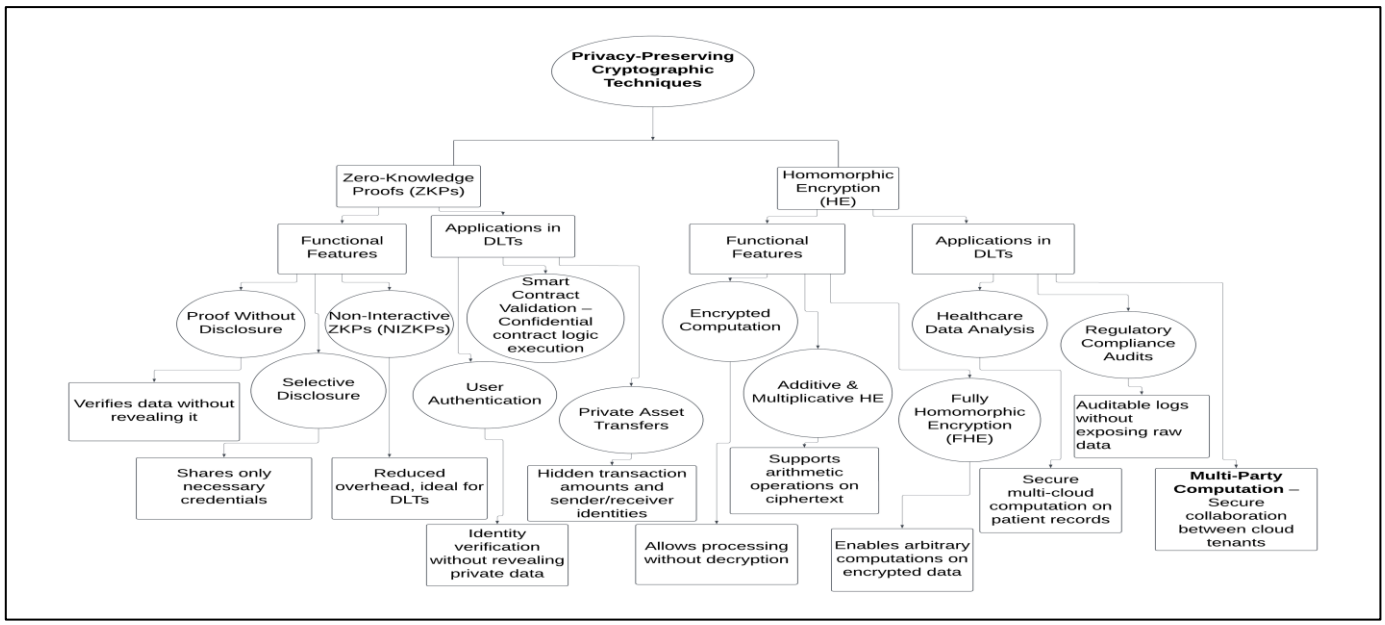

Fig 4: Diagram Illustrating Privacy-Preserving Cryptographic Techniques for Secure Data Processing in Multi-Cloud DLT Systems

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

Figure 4 titled visually delineates two critical cryptographic pillars—Zero-Knowledge Proofs (ZKPs) and Homomorphic Encryption (HE)—used to safeguard data confidentiality in distributed ledger environments deployed across multiple cloud platforms. From the central node representing privacy-preserving techniques, the first branch explores ZKPs, which allow one party to prove possession of information without revealing the data itself. Sub-branches detail its core functions, such as proof without disclosure, selective credential sharing, and non-interactive formats optimized for low-latency DLT operations. It also outlines applications like privacy-respecting user authentication, confidential smart contract execution, and anonymous asset transfers, all critical in systems requiring trustless validation. The second branch covers Homomorphic Encryption, enabling computations on encrypted data without the need for decryption, thus preserving confidentiality during processing. Functional sub-branches illustrate additive and multiplicative schemes, along with the more advanced Fully Homomorphic Encryption (FHE), which supports arbitrary operations. The application sub-branches demonstrate use cases in secure multi-cloud healthcare analytics, regulatory audits that maintain data secrecy, and multi-party computations where cloud tenants collaborate on encrypted datasets. The diagram emphasizes how these technologies jointly form the backbone of secure, regulation-compliant, and privacy-focused multi-cloud DLT infrastructures, without sacrificing utility or computational capabilities.

D. Regulatory and Compliance Challenges (GDPR, HIPAA, etc.)

Integrating DLTs within multi-cloud environments introduces complex regulatory and compliance challenges, particularly concerning frameworks like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA)as presented in table 3. The decentralized and immutable nature of DLTs often conflicts with these regulations, necessitating nuanced approaches to ensure compliance.

➢ *Data Sovereignty and Jurisdictional Conflicts*

In multi-cloud deployments, data may reside across various jurisdictions, each with distinct legal requirements. This dispersion complicates adherence to data sovereignty laws, as organizations must navigate a web of regional regulations governing data storage and transfer. Nair, et al., (2024) highlights that the lack of standardized compliance frameworks across cloud providers exacerbates this issue, making it challenging to maintain consistent regulatory adherence.

➢ *Immutability vs. Right to Erasure*

The GDPR's "right to be forgotten" mandates that individuals can request the deletion of their personal data. However, the inherent immutability of blockchain—a core component of many DLTs—contradicts this requirement, as data, once recorded, cannot be altered or deleted. Augusto, et al, (2024) discusses this conflict, noting that blockchain's design does not readily accommodate data modification or removal, posing significant compliance challenges.

➢ *Transparency vs. Data Minimization*

DLTs promote transparency by allowing all participants access to the ledger's contents. While this fosters trust, it may conflict with data minimization principles, which advocate for limiting the collection and exposure of personal data. Ensuring that only necessary data is processed and that access is appropriately restricted becomes complex in transparent DLT systems. Implementing robust access controls and data encryption techniques is essential to mitigate unauthorized data exposure.

➢ *Compliance Strategies*

To address these challenges, organizations can adopt several strategies:

- *Hybrid Architectures:* Combining on-chain and off-chain storage allows sensitive data to be stored off-chain, with only essential references on-chain, facilitating compliance with data deletion requests.
- *Advanced Cryptographic Techniques:* Employing methods such as zero-knowledge proofs can enable data validation without revealing the data itself, aligning with privacy regulations.
- *Regulatory Collaboration:* Engaging with regulators to develop DLT-specific compliance guidelines can help bridge the gap between innovative technologies and existing legal frameworks.

In conclusion, while DLTs offer transformative potential for multi-cloud environments, aligning their deployment with regulatory requirements like GDPR and HIPAA demands careful architectural planning and proactive compliance strategies.

Table 3: Summary of Regulatory and Compliance Challenges in Multi-Cloud DLT Systems (GDPR, HIPAA, etc.)

Challenge Area	Description	Impact on Multi-Cloud DLTs	Examples/ Application
Data Sovereignty	Data stored across jurisdictions with conflicting regulations	Complicates compliance with regional data protection laws	Health records stored in different countries must align with local GDPR and HIPAA laws
Immutability vs. Erasure	Blockchain immutability conflicts with the right to be forgotten (e.g., GDPR)	Prevents deletion of personal data upon user request	Personal data on-chain cannot be erased when a patient exercises their GDPR rights

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

Transparency vs. Minimization	Ledger openness may violate data minimization principles	Risks overexposure of personal data across participants	Public access to transaction logs in open blockchains revealing patient or user IDs
Lack of Standardized Frameworks	No unified compliance standards across cloud providers and jurisdictions	Inconsistent security and governance practices in DLT applications	Enterprises face difficulties aligning smart contract policies across cloud services

V. USE CASES AND APPLICATION DOMAINS

A. Financial Services and Cross-Border Payments

The integration of DLTs in financial services has significantly transformed cross-border payment systems by enhancing efficiency, reducing costs, and promoting financial inclusion. Traditional cross-border transactions often involve multiple intermediaries, leading to delays and increased expenses. DLTs, such as blockchain, offer decentralized networks that facilitate direct peer-to-peer transactions, thereby streamlining the payment process and minimizing reliance on intermediaries. A notable example is the Stellar network, which employs blockchain technology to enable rapid and cost-effective cross-border payments. Zhuo et al. (2023) highlight Stellar's consensus protocol and payment mechanisms, emphasizing its advantages over conventional systems, particularly in enhancing financial inclusion in regions like Africa. By allowing the issuance and transfer of digital representations of various currencies, Stellar provides a platform for seamless currency exchange and remittance services, addressing challenges faced by underbanked populations. Moreover, DLTs contribute to the efficiency of securities clearing and settlement processes. Priem (2020) discusses the potential of DLT to revolutionize these processes by reducing counterparty risks and settlement times. The immutable and transparent nature of blockchain ensures that all parties have access to a single source of truth, thereby enhancing trust and reducing the need for reconciliations. This is particularly beneficial in cross-border transactions, where differences in time zones and regulatory frameworks can complicate settlements (Ayoola, et al., 2024). However, the adoption of DLTs in cross-border payments is not without challenges. Regulatory uncertainties, interoperability issues between different blockchain platforms, and concerns regarding scalability and energy consumption are significant hurdles that need to be addressed. Collaborative efforts among financial institutions, technology providers, and regulators are essential to establish standardized protocols and frameworks that ensure the secure and efficient implementation of DLT-based payment systems.

In summary, the application of DLTs in financial services, particularly in cross-border payments, offers substantial benefits in terms of speed, cost reduction, and financial inclusion. While challenges remain, ongoing advancements and collaborative initiatives continue to pave the way for more efficient and inclusive global financial systems.

B. Supply Chain Management and Provenance Tracking

DLTs have emerged as transformative tools in supply chain management, offering real-time visibility, enhanced traceability, and immutable provenance records. Traditional supply chains often suffer from information silos, fraud, and a lack of transparency, making it difficult to trace the origin and movement of goods. Blockchain and other DLTs address these challenges by creating decentralized, tamper-proof records of every transaction and asset movement across the supply chain (Kamble et al., 2019) as represented in figure 5. Blockchain enables all stakeholders—including manufacturers, logistics providers, and retailers—to access a shared ledger that captures data points such as production details, shipment updates, and environmental conditions. Kamble et al. (2019) argue that this transparency builds trust and accountability, particularly in sectors like food, pharmaceuticals, and luxury goods where provenance and authenticity are critical. Tijan et al. (2021) emphasize blockchain's application in logistics operations, noting that smart contracts can automate compliance checks, trigger payments, and manage inventory with greater accuracy (Awotiwon, et al., 2024). For example, a smart contract can automatically release payment when goods arrive at a destination verified through IoT-enabled GPS tracking. This eliminates manual processing delays and ensures tamper-evident verification (Enyejo, et al., 2024). By integrating DLTs in a multi-cloud environment, organizations can decentralize data storage while maintaining synchronized provenance records across geographically dispersed systems. This significantly enhances resilience and data integrity in global supply chains, positioning DLTs as a cornerstone of modern logistics infrastructure.

Fig 5: Picture of Enhancing Global Supply Chain Transparency and Real-Time Tracking Through the Integration of IoT Sensors and Blockchain Technology (Enyejo, et al., 2024)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

Figure 5 powerfully illustrates the convergence of IoT sensors and blockchain in enhancing end-to-end visibility within global supply chains, directly reflecting the core insights of *Section 5.2: Supply Chain Management and Provenance Tracking*. On the left, the bold caption underscores the technological theme, while the right side depicts a digitized global logistics network, with interconnected trucks, warehouses, ports, and cargo containers visualized as part of a cyber-physical infrastructure. The glowing world map surrounded by digital icons represents the integration of IoT devices that continuously transmit real-time data—such as temperature, location, and handling conditions—across the supply chain. Blockchain acts as the immutable backbone, validating and securely recording each transaction and status update, thereby enabling traceability, authenticity, and auditability of goods from origin to destination. The visual flow of data suggests how smart contracts automate critical events like customs clearance, payment settlements, and inventory reordering. This integration ensures that all stakeholders, from manufacturers to retailers, have synchronized and tamper-proof access to shared data, eliminating information silos and fraud. The image encapsulates how blockchain and IoT-driven provenance tracking can transform traditional supply chains into transparent, responsive, and intelligent multi-cloud ecosystems tailored for modern global commerce.

Table 4: Summary of Healthcare Data Sharing and Integrity in Multi-Cloud DLT Systems

Focus Area	Key Insights	Benefits	Example/Application
DLT-Based Data Sharing	DLTs enable decentralized and tamper-proof health record management	Improves data traceability and patient safety	Immutable patient records accessible across hospitals and insurers
Smart Contracts	Automate consent management and enforce access policies	Enhances patient control and reduces administrative overhead	Patients granting or revoking access to medical records in real time
Privacy & Compliance	Leverages cryptographic tools to secure data and meet HIPAA/GDPR requirements	Ensures regulatory compliance and data confidentiality	Encrypted health data transactions with full access logging
Multi-Cloud Integration	DLTs synchronize data across multiple cloud platforms	Promotes interoperability and availability across institutions	Cross-provider electronic health record sharing in multi-cloud healthcare networks

C. Healthcare Data Sharing and Integrity

In healthcare, the protection of sensitive patient information and the assurance of data integrity are paramount. DLTs provide a decentralized framework that ensures tamper-proof, traceable, and transparent healthcare data sharing across multi-cloud environments. By eliminating centralized points of failure, DLTs mitigate the risks of data breaches and unauthorized modifications, which are prevalent in conventional cloud-based health systems (Agbo et al., 2019) as presented in table 4. Healthcare data is frequently exchanged among hospitals, insurers, laboratories, and governmental agencies. However, data fragmentation and inconsistencies often result in duplication, medical errors, and inefficiencies. Blockchain technology enables a unified, immutable health record that can be securely accessed and validated by authorized stakeholders. Agbo et al. (2019) emphasize that this ensures accurate patient history tracking, clinical decision support, and improved continuity of care. Esposito et al. (2018) highlight the role of smart contracts in enforcing data-sharing policies and consent management. Patients can grant and revoke access to their health records in real-time, enhancing transparency and user control. Additionally, blockchain's cryptographic mechanisms strengthen authentication and access logging, ensuring data privacy while complying with regulations such as HIPAA and GDPR (Ajayi, et al., 2024). By deploying DLTs over a multi-cloud architecture, healthcare providers can ensure cross-institutional data availability and integrity, ultimately supporting patient-centric, secure, and interoperable health ecosystems.

D. IoT, Edge Computing, and Real-Time Transactional Systems

The convergence of Internet of Things (IoT), edge computing, and real-time transactional systems introduces a paradigm where vast amounts of data are generated, processed, and acted upon at high velocity. DLTs within this architecture enhances data authenticity, trust, and automation across decentralized devices and nodes. With billions of connected devices transmitting sensitive data across distributed networks, blockchain ensures a tamper-evident audit trail and decentralized consensus for real-time transactions (Novo, 2018). In traditional IoT architectures, data is typically aggregated at centralized servers, making the system vulnerable to bottlenecks, latency, and single points of failure. Edge computing shifts computation closer to the data source, but without strong integrity guarantees (Akindote, et al., 2024). By combining blockchain with edge devices, secure peer-to-peer communication and transaction verification can occur at the network edge, enabling trusted autonomous operations such as smart manufacturing, energy grids, and supply logistics (Novo, 2018). Xu et al. (2019) emphasize that smart contracts deployed in edge-enabled blockchain systems facilitate real-time enforcement of device-level policies, enabling adaptive responses to sensor data. For instance, in a smart grid, smart contracts can autonomously adjust energy distribution based on real-time consumption data (Novo, 2018). These DLT-based frameworks support low-latency, decentralized decision-making critical for resilient and scalable edge-IoT ecosystems operating across multi-cloud infrastructures.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

VI. EMERGING TRENDS, RESEARCH CHALLENGES, AND FUTURE DIRECTIONS

A. Advancements in Cross-Chain Interoperability and Multi-Cloud Orchestration

As organizations adopt DLTs across diverse blockchain platforms and multi-cloud environments, cross-chain interoperability and orchestration mechanisms have emerged as critical enablers of system scalability, resilience, and functional integration as represented in figure 6. Interoperability ensures that independent blockchain systems can communicate and transact with each other without compromising security or decentralization, which is essential in a multi-cloud context where applications may span private, consortium, and public ledgers (Belchior et al., 2021). Recent developments in interoperability protocols such as Interledger, Polkadot, Cosmos, and Hyperledger Cactus enable atomic cross-chain transactions, shared state synchronization, and consensus layering across heterogeneous blockchains. These frameworks abstract protocol-level differences, supporting secure data transfers and smart contract execution across chains—key for orchestrating distributed workflows in complex cloud ecosystems (Akindote, et al., 2024). For example, Cosmos's Inter-Blockchain Communication (IBC) protocol enables independent blockchain networks to interoperate without relying on centralized intermediaries (Belchior et al., 2021). In parallel, orchestration tools like Kubernetes, Terraform, and multi-cloud service meshes are evolving to coordinate containerized DLT nodes across hybrid cloud environments. Hardjono and Pentland (2019) emphasize the importance of trust registries, decentralized identity models, and cryptographic anchors to unify access control and governance in federated blockchain systems. These advancements collectively support secure and scalable multi-cloud orchestration, positioning blockchain as a foundational layer for cross-domain, trustless collaboration.

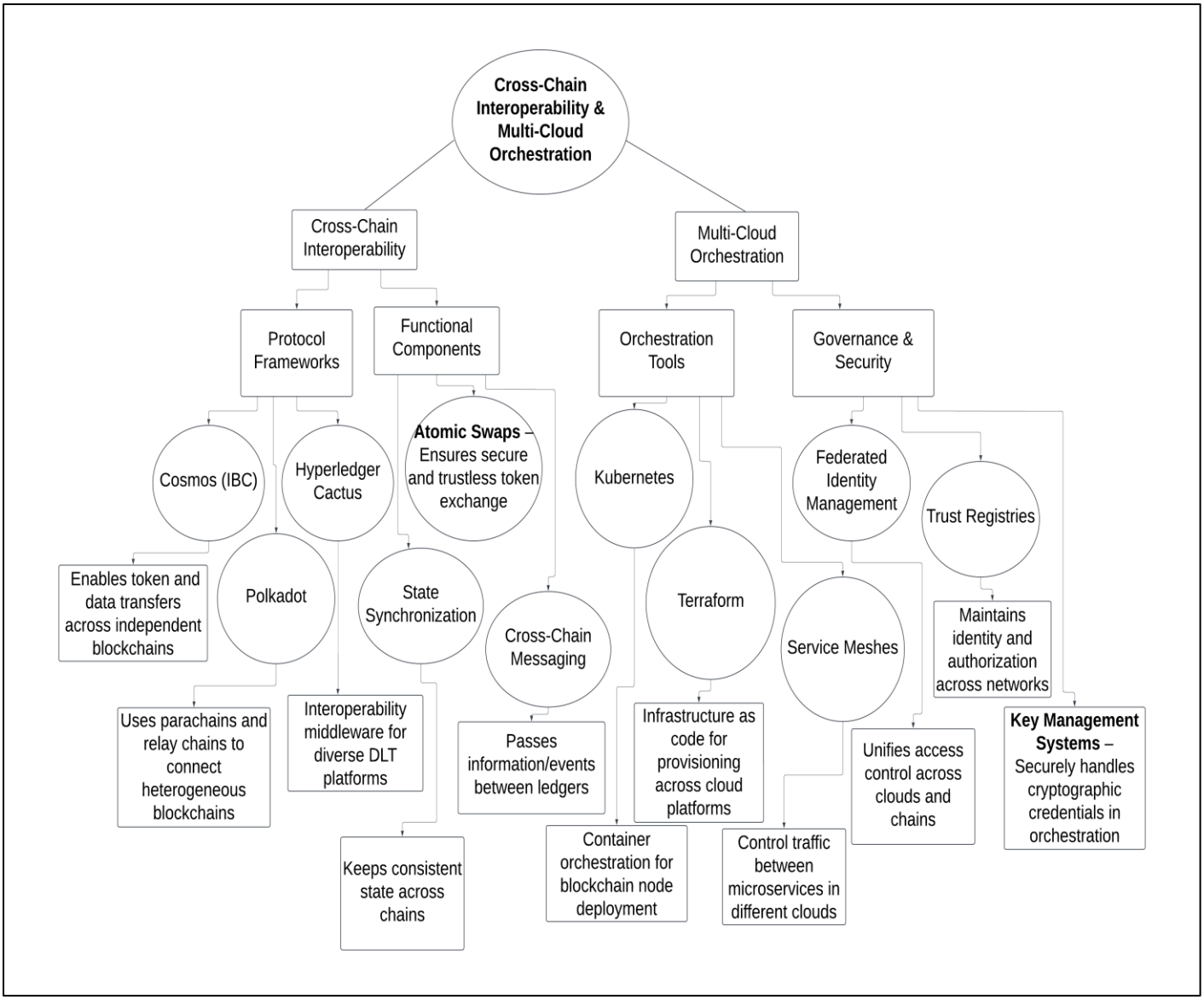

Fig 6: Diagram Illustrating Cross-Chain Interoperability and Multi-Cloud Orchestration in DLT Systems

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

Figure 6 provides a comprehensive visual representation of the evolving technologies and frameworks enabling seamless interaction between distributed ledger networks and cloud platforms. At the core is the concept of Cross-Chain Interoperability and Multi-Cloud Orchestration, branching into two primary areas. The Cross-Chain Interoperability section highlights protocol frameworks such as Cosmos (IBC), Polkadot, and Hyperledger Cactus, which facilitate asset and data exchange across independent blockchain networks. Supporting components like state synchronization, atomic swaps, and cross-chain messaging ensure real-time consistency and trustless communication across ledgers. The second major branch, Multi-Cloud Orchestration, focuses on the tools and governance models that manage distributed ledger deployments across diverse cloud environments. This includes orchestration tools like Kubernetes for container management, Terraform for infrastructure provisioning, and service meshes for managing microservice communication. Under governance and security, elements such as federated identity management, trust registries, and key management systems enable secure access control, identity validation, and cryptographic credential handling across federated blockchain-cloud ecosystems. The diagram emphasizes the modular, layered architecture required to achieve scalable, interoperable, and secure multi-cloud DLT operations, laying the foundation for next-generation decentralized infrastructure.

B. Scalability and Performance Optimization Techniques

Scalability remains a central concern in DLTs, particularly in multi-cloud deployments where network latency, transaction volume, and resource heterogeneity can severely degrade system performance. To address these limitations, various performance optimization techniques have been proposed, focusing on consensus efficiency, parallel processing, and layered architectures (Wang et al., 2019). One of the key strategies for improving blockchain scalability is the implementation of sharding, which partitions the ledger into multiple shards capable of processing transactions in parallel. This reduces the load on individual nodes and improves throughput significantly. Additionally, layer-2 protocols such as state channels and sidechains enable off-chain transaction processing while anchoring final results to the main blockchain, preserving security and integrity without burdening the base layer (Wang et al., 2019). Zheng et al. (2018) highlight delegated proof-of-stake (DPoS) and Byzantine fault-tolerant (BFT) consensus algorithms as alternatives to traditional proof-of-work (PoW) to reduce latency and energy consumption. These approaches are particularly advantageous in multi-cloud systems, where trust boundaries vary and low-latency coordination across clouds is essential. Furthermore, the use of hardware acceleration through trusted execution environments (TEEs) and field-programmable gate arrays (FPGAs) has demonstrated promise in enhancing cryptographic processing and reducing bottlenecks (Zheng et al., 2018). Together, these optimization techniques aim to ensure that DLTs remain viable and efficient as their adoption scales across global, multi-cloud infrastructures.

C. AI-Driven Analytics and Predictive Security in Multi-Cloud DLTs

Artificial Intelligence (AI) plays a critical role in augmenting DLTs deployed across multi-cloud infrastructures, particularly in the realms of analytics and predictive security. As decentralized systems generate vast volumes of transactional and telemetry data, AI algorithms can extract actionable insights to improve decision-making, monitor network health, and detect anomalies in real time (Kouicem et al., 2018). AI-driven anomaly detection models, such as federated learning and unsupervised clustering, enhance the security of multi-cloud DLTs by identifying irregular transaction patterns and network behaviors. These models enable preemptive responses to security breaches, including Sybil attacks, double-spending, or unauthorized data access. Kouicem et al. (2018) demonstrate that federated learning, when applied in decentralized IoT ecosystems, maintains data privacy while supporting collaborative threat detection across heterogeneous nodes—an approach that aligns well with multi-cloud DLT networks. Chang et al. (2021) emphasize the synergy between AI and blockchain in edge-enabled health systems, where predictive analytics improve reliability and reduce downtime. In a similar vein, multi-cloud DLTs can incorporate machine learning to dynamically optimize load balancing, consensus throughput, and resource allocation based on real-time system metrics. These adaptive models improve both performance and resilience, making AI an indispensable asset in securing and scaling DLT-based multi-cloud infrastructures.

Table 5: Summary of Recommendations for Future Research and Practical Adoption

Focus Area	Recommendation	Purpose	Example/Application
Consensus Mechanisms	Develop lightweight, adaptive consensus algorithms	Enhance fault tolerance and performance in multi-cloud environments	Algorithms optimized for latency-aware multi-cloud deployments
Interoperability Protocols	Advance cross-chain and cross-cloud communication frameworks	Support decentralized identity, asset transfer, and smart contracts	Protocols like IBC or custom APIs enabling DLT and cloud integration
Hybrid Deployment Models	Use off-chain storage with on-chain data anchoring	Achieve regulatory compliance and optimize storage	Store medical records off-chain and reference hashes on-chain for auditability
Pilot Testing & Tooling	Conduct pilot projects with orchestration and monitoring tools	Validate architecture and inform real-world adoption	Deploy DLTs in healthcare or finance with Kubernetes-based orchestration and auditing

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

D. Open Research Challenges and Potential Future Developments

Despite the growing adoption of DLTs in multi-cloud environments, several unresolved challenges hinder their widespread deployment and scalability. A fundamental concern lies in the scalability of consensus mechanisms under heterogeneous network conditions. Traditional algorithms such as Proof of Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) suffer from limitations in energy efficiency, latency, and fault tolerance, especially in geographically dispersed multi-cloud infrastructures (Nguyen & Kim, 2018) as presented in table 5. As applications scale, the trade-off between decentralization, security, and performance becomes increasingly complex, demanding novel consensus protocols that are lightweight, adaptive, and cross-cloud compatible. Another persistent challenge involves the integration of DLTs with legacy systems and regulatory frameworks. Ensuring backward compatibility while maintaining cryptographic security standards across platforms is a non-trivial task, particularly when data sovereignty and jurisdictional constraints intersect with immutable ledgers (Xie et al., 2019). Furthermore, the absence of standardized interoperability frameworks continues to hinder the seamless orchestration of services across multi-cloud DLT ecosystems. Future developments may include blockchain-aware orchestration layers embedded with AI for predictive system scaling and dynamic governance models tailored for federated networks. Additionally, advances in quantum-resistant cryptography, zero-knowledge interoperability proofs, and ethical AI-driven blockchain regulation are expected to redefine how DLTs evolve within complex cloud-native environments. These innovations represent promising avenues for ensuring sustainable and secure multi-cloud DLT deployments.

VII. CONCLUSION

A. Summary of Key Findings

This review has systematically examined the integration of DLTs in multi-cloud environments, highlighting their transformative impact on data integrity, transactional security, and system decentralization. Key findings reveal that DLTs, including blockchain, Directed Acyclic Graphs (DAGs), and consortium ledgers, offer robust mechanisms for immutable data recording, consensus validation, and trustless interactions across heterogeneous cloud platforms. Design patterns such as partitioned architectures and cross-cloud interoperability protocols facilitate seamless integration and orchestration across providers. Smart contracts enhance automation and governance, while advanced cryptographic techniques like zero-knowledge proofs and homomorphic encryption ensure data privacy and regulatory compliance. Use cases in financial services, supply chain management, healthcare, and IoT illustrate the practical benefits of DLTs in reducing intermediaries, enhancing traceability, and securing real-time transactions. Moreover, emerging trends such as AI-driven analytics, cross-chain communication frameworks, and performance optimization techniques—including sharding and layer-2 protocols—demonstrate the evolving sophistication of multi-cloud DLT ecosystems. However, unresolved challenges persist in achieving full scalability, interoperability, and regulatory alignment, particularly in the context of decentralized data sovereignty and trust federation. Overall, this study affirms that the convergence of DLTs and multi-cloud computing presents a viable path toward secure, efficient, and scalable distributed systems capable of supporting the next generation of global digital infrastructure.

B. Implications for Industry and Academia

The integration of DLTs within multi-cloud infrastructures presents profound implications for both industry and academia. For industry stakeholders, this convergence offers a blueprint for creating decentralized, resilient, and secure systems capable of supporting critical applications in finance, healthcare, supply chains, and IoT ecosystems. Enterprises can leverage smart contracts and real-time transactional integrity to automate processes such as cross-border settlements, inventory verification, and medical record sharing, thereby reducing operational costs, eliminating fraud, and enhancing compliance. The ability to orchestrate distributed nodes across multiple cloud providers enables scalability without sacrificing availability or performance, a crucial factor in supporting global operations. From an academic perspective, this study opens new avenues for research into consensus algorithms, cryptographic models, privacy-preserving mechanisms, and cross-chain communication protocols tailored for heterogeneous cloud environments. Interdisciplinary efforts combining distributed computing, information security, AI, and regulatory policy are necessary to address ongoing challenges in scalability, interoperability, and governance. Furthermore, the development of testbeds and simulation platforms for evaluating multi-cloud DLT configurations will be essential for validating theoretical models in real-world scenarios. Academia can also contribute to standardization efforts, providing foundational frameworks that inform both industry practices and international regulatory compliance. Collectively, these implications underscore the strategic value of DLT-driven multi-cloud architectures in shaping the future of digital infrastructure.

C. Recommendations for Future Research and Practical Adoption

Future research should prioritize the development of lightweight, adaptive consensus algorithms that can maintain fault tolerance and throughput in dynamic multi-cloud settings, especially where latency and resource availability vary across cloud providers. Special attention should be given to scalable cross-chain interoperability protocols capable of supporting decentralized identity, asset transfer, and smart contract execution across diverse ledger technologies. Researchers should explore the integration of federated learning with DLTs to enable collaborative anomaly detection, secure data analytics, and privacy-preserving AI in distributed cloud systems. From a practical standpoint, organizations adopting DLTs in multi-cloud architectures should begin with hybrid deployments that use off-chain storage for sensitive data and anchor hashes on-chain to ensure compliance with regulations like GDPR. Implementation frameworks must include multi-cloud orchestration tools that provide unified monitoring, fault

isolation, and automatic scaling of distributed ledger nodes. Industry practitioners are encouraged to adopt standardized APIs and interoperability frameworks to minimize vendor lock-in and ensure seamless integration between legacy systems and emerging blockchain networks. Furthermore, pilot projects in regulated sectors such as finance and healthcare should be used to validate security models, data governance strategies, and compliance workflows. These implementations will provide actionable insights, helping bridge the gap between academic theory and enterprise-scale DLT adoption across complex, multi-cloud infrastructures.

REFERENCES

[1]. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, 7(2), 56. https://doi.org/10.3390/healthcare7020056

[2]. Ajayi, A. A., Igba, E., Soyele, A. D., & Enyejo, J. O. (2024). Enhancing Digital Identity and Financial Security in Decentralized Finance (Defi) through Zero-Knowledge Proofs (ZKPs) and Blockchain Solutions for Regulatory Compliance and Privacy. OCT 2024 |*IRE Journals* | Volume 8 Issue 4 | ISSN: 2456-8880

[3]. Akindote, O., Enyejo, J. O., Awotiwon, B. O. & Ajayi, A. A. (2024). Integrating Blockchain and Homomorphic Encryption to Enhance Security and Privacy in Project Management and Combat Counterfeit Goods in Global Supply Chain Operations. *International Journal of Innovative Science and Research Technology* Volume 9, Issue 11, NOV. 2024, ISSN No:-2456-2165. https://doi.org/10.38124/ijisrt/IJISRT24NOV149.

[4]. Akindote, O., Igba E., Awotiwon, B. O., & Otakwu, A (2024). Blockchain Integration in Critical Systems Enhancing Transparency, Efficiency, and Real-Time Data Security in Agile Project Management, Decentralized Finance (DeFi), and Cold Chain Management. *International Journal of Scientific Research and Modern Technology (IJSRMT)* Volume 3, Issue 11, 2024. DOI: 10.38124/ijsrmt.v3i11.107.

[5]. Alavizadeh, A. S., Erfani, S. H., Mirabi, M., & Sahafi, A. (2023). An Efficient Distributed and Secure Algorithm for Transaction Confirmation in IOTA Using Cloud Computing. *The Journal of Supercomputing*, 80(3), 1491–1521. https://doi.org/10.1007/s11227-023-05525-4

[6]. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024, May). Sok: Security and privacy of blockchain interoperability. In *2024 IEEE Symposium on Security and Privacy (SP)* (pp. 3840-3865). IEEE.

[7]. Awotiwon, B. O., Enyejo, J. O., Owolabi, F. R. A., Babalola, I. N. O., & Olola, T. M. (2024). Addressing Supply Chain Inefficiencies to Enhance Competitive Advantage in Low-Cost Carriers (LCCs) through Risk Identification and Benchmarking Applied to Air Australasia's Operational Model. *World Journal of Advanced Research and Reviews, 2024, 23(03), 355–370.* https://wjarr.com/content/addressing-supply-chain-inefficiencies-enhance-competitive-advantage-low-cost-carriers-lccs

[8]. Ayoola, V. B., Ugoaghalam, U. J., Idoko P. I, Ijiga, O. M & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances,* 2024, 20(03), 094–117. https://gjeta.com/content/effectiveness-social-engineering-awareness-training-mitigating-spear-phishing-risks

[9]. Baninemeh, E., Slikker, M., Labunets, K., & Jansen, S. (2024). A Security Risk Assessment Method for Distributed Ledger Technology (DLT) based Applications: Three Industry Case Studies. *arXiv preprint arXiv:2401.12358*. https://arxiv.org/abs/2401.12358

[10]. Belchior, R., Riley, L., Hardjono, T., Vasconcelos, A., & Correia, M. (2023). Do you need a distributed ledger technology interoperability solution? *Distributed Ledger Technologies: Research and Practice*, *2*(1), 1-37.

[11]. Belchior, R., Süßenguth, J., Feng, Q., Hardjono, T., Vasconcelos, A., & Correia, M. (2024). A brief history of blockchain interoperability. *Communications of the ACM*, *67*(10), 62-69.

[12]. Belchior, R., Vasconcelos, A., Correia, M., & Almeida, H. (2022). Do You Need a Distributed Ledger Technology Interoperability Solution? *ACM Computing Surveys*, 55(8), 1–37. https://doi.org/10.1145/3564532

[13]. Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys*, 54(8), 1–41. https://doi.org/10.1145/3452266

[14]. Benčić, F. M., & Podnar Žarko, I. (2018). Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph. *arXiv preprint arXiv:1804.10013*. https://arxiv.org/abs/1804.10013

[15]. Chang, Z., Liu, S., Xiong, X., Cai, Z., & Tu, G. (2021). A survey of recent advances in edge-computing-powered artificial intelligence of things. *IEEE Internet of Things Journal*, *8*(18), 13849-13875.

[16]. Dhokrat, J., Pulgam, N., Maktum, T., & Mane, V. (2024). A Framework for Privacy-Preserving Multiparty Computation with Homomorphic Encryption and Zero-Knowledge Proofs. *Informatica*, 48, 1–14. https://doi.org/10.31449/inf.v48i21.6562

[17]. Dib, O., Brousmiche, K. L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium Blockchains: Overview, Applications and Challenges. *International Journal on Advances in Telecommunications*, 11(1 & 2), 51–64. https://personales.upv.es/thinkmind/dl/journals/tele/tele_v11_n12_2018/tele_v11_n12_2018_5.pdf

[18]. Ebenibo, L., Enyejo, J. O., Addo, G., & Olola, T. M. (2024). Evaluating the Sufficiency of the data protection act 2023 in the age of Artificial Intelligence (AI): A comparative case study of Nigeria and the USA. *International Journal of Scholarly Research*

and Reviews, 2024, 05(01), 088–107. https://srrjournals.com/ijsrr/content/evaluating-sufficiency-data-protection-act-2023-age-artificial-intelligence-ai-comparative

[19]. Enyejo, J. O., Adeyemi, A. F., Olola, T. M., Igba, E & Obani, O. Q. (2024). Resilience in supply chains: How technology is helping USA companies navigate disruptions. *Magna Scientia Advanced Research and Reviews,* 2024, 11(02), 261–277. https://doi.org/10.30574/msarr.2024.11.2.0129

[20]. Enyejo, J. O., Babalola, I. N. O., Owolabi, F. R. A. Adeyemi, A. F., Osam-Nunoo, G., & Ogwuche, A. O. (2024). Data-driven digital marketing and battery supply chain optimization in the battery powered aircraft industry through case studies of Rolls-Royce's ACCEL and Airbus's E-Fan X Projects. *International Journal of Scholarly Research and Reviews, 2024, 05(02), 001–020.* https://doi.org/10.56781/ijsrr.2024.5.2.0045

[21]. Enyejo, J. O., Fajana, O. P., Jok, I. S., Ihejirika, C. J., Awotiwon, B. O., & Olola, T. M. (2024). Digital Twin Technology, Predictive Analytics, and Sustainable Project Management in Global Supply Chains for Risk Mitigation, Optimization, and Carbon Footprint Reduction through Green Initiatives. *International Journal of Innovative Science and Research Technology,* Volume 9, Issue 11, November–2024. ISSN No:-2456-2165. https://doi.org/10.38124/ijisrt/IJISRT24NOV1344

[22]. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, 5(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

[23]. Eze, E. (2024). Nigeria Now Faces 4,718 Cyber Attacks Weekly – Report. https://arbiterz.com/nigerians-now-face-4718-cyber-attacks-weekly-report/

[24]. Ezeh, N. V., Batur, S. D., Oluhaiyero, Shade. Y., Abiodun, K., Nwobi, C. C., Ali, O. E., & Igba, E. (2024). Blockchain Driven Cold Chain Logistics and Decentralized Inventory Systems for Managing Post-Harvest Losses and Improving Financial Sustainability in Regional Food Hubs. *International Journal of Scientific Research and Modern Technology (IJSRMT)*. Volume 3, Issue 9, 2024. DOI: https://doi.org/10.5281/zenodo.14874303

[25]. Fouda, M. M., Fadlullah, Z. M., Ibrahem, M. I., & Kato, N. (2024). Privacy-Preserving Data-Driven Learning Models for Emerging Communication Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*.

[26]. Ghallab, A., Saif, M. H., & Mohsen, A. (2021). Data Integrity and Security in Distributed Cloud Computing—A Review. *International Journal of Computer Applications*, 174(30), 1–9. https://doi.org/10.5120/ijca2021921512

[27]. Hardjono, T., & Pentland, A. (2019). Towards a Design Philosophy for Interoperable Blockchain Systems. *Communications of the ACM*, 62(12), 36–39. https://doi.org/10.1145/3363577

[28]. Ibokette., A. I. Ogundare, T. O., Danquah, E. O., Anyebe, A. P., Agaba, J. A., & Olola, T. M. (2024). The impacts of emotional intelligence and IOT on operational efficiency in manufacturing: A cross-cultural analysis of Nigeria and the US. *Computer Science & IT Research Journal P-ISSN: 2709-0043, E-ISSN: 2709-0051.* DOI: 10.51594/csitrj.v5i8.1464

[29]. Idoko, I. P., Ijiga, O. M., Enyejo, L. A., Akoh, O., & Isenyo, G. (2024). Integrating superhumans and synthetic humans into the Internet of Things (IoT) and ubiquitous computing: Emerging AI applications and their relevance in the US context. **Global Journal of Engineering and Technology Advances**, 19(01), 006-036.

[30]. Igba E., Ihimoyan, M. K., Awotinwo, B., & Apampa, A. K. (2024). Integrating BERT, GPT, Prophet Algorithm, and Finance Investment Strategies for Enhanced Predictive Modeling and Trend Analysis in Blockchain Technology. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.,* November-December-2024, 10 (6) : 1620-1645.https://doi.org/10.32628/CSEIT241061214

[31]. Ijiga, A. C., Igbede, M. A., Ukaegbu, C., Olatunde, T. I., Olajide, F. I. & Enyejo, L. A. (2024). Precision healthcare analytics: Integrating ML for automated image interpretation, disease detection, and prognosis prediction. *World Journal of Biology Pharmacy and Health Sciences,* 2024, 18(01), 336–354. https://wjbphs.com/sites/default/files/WJBPHS-2024-0214.pdf

[32]. Ijiga, A. C., Olola, T. M., Enyejo, L. A., Akpa, F. A., Olatunde, T. I., & Olajide, F. I. (2024). Advanced surveillance and detection systems using deep learning to combat human trafficking. *Magna Scientia Advanced Research and Reviews*, 2024, 11(01), 267–286. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0091.pdf.

[33]. Ijiga, M. O., Olarinoye, H. S., Yeboah, F. A. B. & Okolo, J. N. (2025). Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches. *International Journal of Scientific Research and Modern Technology*, *4*(3), 1–15. https://doi.org/10.38124/ijsrmt.v4i3.376

[34]. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *Open Access Research Journals.* Volume 13, Issue. https://doi.org/10.53022/oarjst.2024.11.1.0060

[35]. Imran, H. A., Latif, U., Ikram, A., & Wazir, S. (2020). Multi-Cloud: A Comprehensive Review. *International Journal of Advanced Computer Science and Applications*, 11(10), 370–379. https://doi.org/10.14569/IJACSA.2020.0111048

[36]. Jamshidi, P., Pahl, C., & Mendonça, N. C. (2017). Pattern-based multi-cloud architecture migration. *Software: Practice and Experience*, *47*(9), 1159-1184.

[37]. Kamble, S. S., Gunasekaran, A., & Arha, H. (2019). Understanding the influence of blockchain technology on supply chain management: A review of current literature and future research agenda. *Supply Chain Management: An International Journal*, 24(4), 62–84. https://doi.org/10.1108/SCM-03-2018-0148

[38]. Kathiravelu, P., Chiesa, M., Marcos, P., Canini, M., & Veiga, L. (2018, May). Moving bits with a fleet of shared virtual routers. In *2018 IFIP Networking Conference (IFIP Networking) and Workshops* (pp. 1-9). IEEE.

[39]. Kempf, J., Nayak, S., Robert, R., Feng, J., Deshmukh, K. R., Shukla, A., Obeso Duque, A., Narendra, N., & Sjöberg, J. (2019). The Nubo Virtual Services Marketplace. *arXiv preprint arXiv:1909.04934*. https://arxiv.org/abs/1909.04934

[40]. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of Things Security: A Topology-Aware Federated Learning Model for Detecting Anomalies. *Future Generation Computer Systems*, 87, 501–516. https://doi.org/10.1016/j.future.2018.05.020

[41]. Li, Q., Yang, Z., Qin, X., Tao, D., Pan, H., & Huang, Y. (2022). CBFF: A cloud–blockchain fusion framework ensuring data accountability for multi-cloud environments. *Journal of Systems Architecture*, *124*, 102436.

[42]. Marimuthu, G. (2025). The Role of Cloud Computing and Distributed Ledger Technology in Energy Derivatives Trading. *International Journal of Research in Computer Applications and Information Technology*, 8(1), 2804–2819. https://doi.org/10.34218/IJRCAIT_08_01_202

[43]. Mohankumar, R. (2025). Enhancing Blockchain, Internet of Things, and Cloud Security Through Advanced Cryptographic Techniques and Threat Mitigation Strategies. *International Journal of Advanced Research in Cyber Security*, 6(2), 7–14.

[44]. Nair, R. R., Sreevidya, D., Mohan, C. R., Banerjee, J., & Chouhan, K. (2024, September). Comprehensive Approaches to Securing Multi-Cloud Architectures: Best Practices and Emerging Solutions. In *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 7, pp. 1631-1636). IEEE.

[45]. Nerella, H. (2023). Navigating the Multi-Cloud Maze: Benefits, Challenges, and Future Trends. *ResearchGate*. https://www.researchgate.net/publication/381304851_Navigating_the_Multi-Cloud_Maze_Benefits_Challenges_and_Future_Trends

[46]. Nguyen, G. T., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems*, 14(1), 101–128. https://doi.org/10.3745/JIPS.03.0099

[47]. Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

[48]. Nwatuzie, G. A., Ijiga, O. M., Idoko, I. P., Enyejo, L. A. & Ali, E. O. (2025). Design and Evaluation of a User-Centric Cryptographic Model Leveraging Hybrid Algorithms for Secure Cloud Storage and Data Integrity. *American Journal of Innovation in Science and Engineering (AJISE).* Volume 4 Issue 1, ISSN: 2158-7205 https://journals.e-palli.com/home/index.php/ajise DOI: https://doi.org/10.54536/ajise.v4i1.4482

[49]. Oloruntoba, O. (2025). Architecting Resilient Multi-Cloud Database Systems: Distributed Ledger Technology, Fault Tolerance, and Cross-Platform Synchronization. *International Journal of Research Publication and Reviews*, 6(2), 2358–2376. https://doi.org/10.55248/gengpi.6.0225.0918

[50]. Priem, R. (2020). Distributed Ledger Technology for Securities Clearing and Settlement: Benefits, Risks, and Regulatory Implications. *Financial Innovation*, 6(1), 11. https://doi.org/10.1186/s40854-019-0169-6 SpringerOpen

[51]. Reece, M., Lander Jr., T. E., Stoffolano, M., Sampson, A., Dykstra, J., Mittal, S., & Rastogi, N. (2023). Systemic Risk and Vulnerability Analysis of Multi-cloud Environments. *arXiv preprint arXiv:2306.01862*. https://arxiv.org/abs/2306.01862

[52]. Saxena, D., Gupta, R., & Singh, A. K. (2021). A Survey and Comparative Study on Multi-Cloud Architectures: Emerging Issues and Challenges for Cloud Federation. *arXiv preprint arXiv:2108.12831*. https://arxiv.org/abs/2108.12831

[53]. Tiamiyu, D., Aremu, S. O., Igba, E., Ihejirika, C. J., Adewoye, M. B. & Ajayi, A. A. (2024). Interpretable Data Analytics in Blockchain Networks Using Variational Autoencoders and Model-Agnostic Explanation Techniques for Enhanced Anomaly Detection. *International Journal of Scientific Research in Science and Technology.* Volume 11, Issue 6 November-December-2024. 152-183. https://doi.org/10.32628/IJSRST24116170

[54]. Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2021). Blockchain Technology Implementation in Logistics. *Sustainability*, 13(4), 2241. https://doi.org/10.3390/su13042241

[55]. Uddin, M., Muzammal, M., Hameed, M. K., Javed, I. T., Alamri, B., & Crespi, N. (2021). CBCIoT: A Consensus Algorithm for Blockchain-Based IoT Applications. *Applied Sciences*, 11(22), 11011. https://doi.org/10.3390/app112211011

[56]. Wang, W., Hoang, D. T., Xie, L., Hu, P., & Niyato, D. (2019). Performance Evaluation of Blockchain Systems: A Systematic Survey. *IEEE Access*, 7, 150327–150339. https://doi.org/10.1109/ACCESS.2019.2949514

[57]. Xie, J., Tang, H., Huang, Y., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, 21(3), 2794–2830. https://doi.org/10.1109/COMST.2019.2899617

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1970

[58]. Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. In *Architecture for Blockchain Applications* (pp. 55–72). Springer. https://doi.org/10.1007/978-3-030-03035-3_4

[59]. Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, 6(2), 93–97. https://doi.org/10.1016/j.icte.2019.08.001

[60]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *IEEE International Congress on Big Data*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[61]. Zhuo, X., Irresberger, F., & Bostandzic, D. (2023). Blockchain for Cross-border Payments and Financial Inclusion: The Case of Stellar Network. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4550837 ResearchGate+1SSRN+1.