International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

EVALUATING BLOCKCHAIN AND HOMOMORPHIC ENCRYPTION FOR SECURE DATA PROCESSING IN MULTI-CLOUD HYBRID DATABASE SYSTEMS: A SYSTEMATIC LITERATURE REVIEW

Sri Rama Chandra Charan Teja Tadi
Software Developer
Raven Software Solutions Inc.
charanteja.tadi@gmail.com
West Des Moines, Iowa, USA.

Abstract

The evolving landscape of backend software development increasingly depends on multi-cloud hybrid database systems to facilitate scalability, high availability, and cost savings. Since data is spread over multiple cloud providers, it becomes difficult to deploy consistent security policies, creating data leakage, unauthorized access, and regulatory compliance issues. Homomorphic encryption (HE) is revolutionary in providing a solution by supporting mathematical operations over encrypted data so that sensitive computation never reveals plaintext values, a vital aspect for privacy-preserving analytics, machine learning models, and financial data processing. Simultaneously, blockchain technology allows an immutable audit trail; hence, unauthorized modification is averted, and auditability is facilitated with complex multi-cloud implementations. Merging HE with blockchain makes database systems clear and secure without central trust models.

An extensive and systematic literature review is undertaken to analyze such technologies' efficiency, scalability, and feasibility in software design for the cloud and backend systems. There are several existing studies that identify different methods of combining secure computation models with decentralized verification techniques, though there are still considerable challenges to overcome. Both HE-based computations and Blockchain integration come with limitations on latency, consensus protocols, and cross-cloud support, which demand dynamic solutions to facilitate high-performance and scalable hybrid cloud security paradigms. All these requirements have to be met for effective deployment in multi-cloud database systems that can support increasing needs for resilient and privacy-protecting backend architecture.

Index Terms: Multi-cloud, Homomorphic Encryption (HE), Blockchain, Hybrid database, Audit, Machine Learning, Financial data, Scalability, Latency, Privacy.

I. INTRODUCTION

A. Overview of multi-cloud hybrid database systems

Multi-cloud hybrid database systems have become popular because they enable organizations to take advantage of the best strengths of several cloud providers without sacrificing on-premises infrastructure. Organizations use this method to improve data availability, scalability, and fault tolerance by distributing loads across different cloud environments. Hybrid cloud platforms allow

businesses the ability to make tactical trade-offs between efficiency savings, performance, and compliance demands and balance the management of on-premises assets with the public cloud's dynamism [13]. The solutions also bring some security issues, such as data fragmentation, cross-cloud communications vulnerabilities, and disparate security policies.

One of the major issues with multi-cloud hybrid architecture is maintaining the confidentiality and integrity of data while data is processed and stored across various environments. Third-party cloud providers make the data more susceptible to data breaches, misuse, and non-compliance. The application of standard encryption schemes provides a level of security but can subject sensitive data to attacks before it is decrypted for computation. Homomorphic encryption addresses this limitation by allowing computations to be executed on encrypted data, while blockchain enhances data provenance, integrity, and access control through a decentralized, tamper-proof ledger [1].

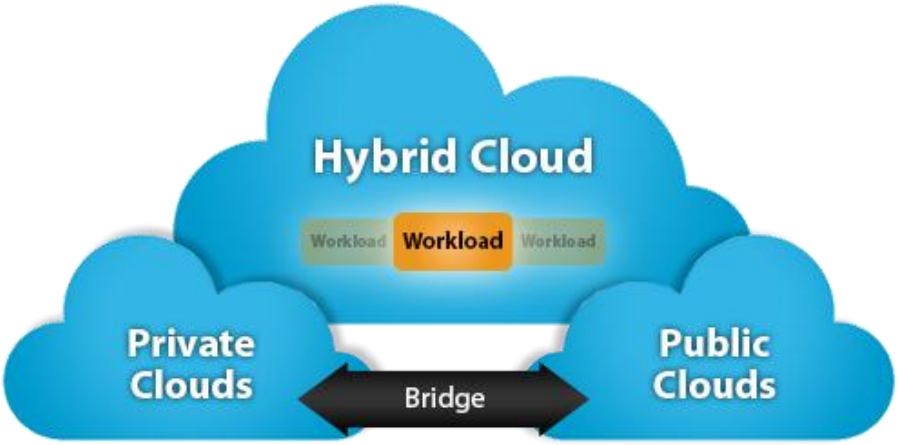

Figure 1: Illustration of a hybrid cloud architecture [14]

B. Overview of blockchain and homomorphic encryption

Blockchain technology is a distributed and decentralized ledger technology that has been developed to provide transparency, security, and immutability in digital transactions. It eliminates the need for centralized authorities. As such, it is best to secure multi-cloud hybrid database systems where data integrity and trust between stakeholders are of utmost importance. The immutability of blockchain blocks unauthorized alteration and provides an auditable history of data modification. Smart contracts, as part of blockchain, facilitate automatic, secure, and verifiable data processing with less reliance on third-party intermediaries [1].

Homomorphic encryption (HE) is a cryptographic method that allows mathematical computation on encrypted data without decryption. Unlike conventional encryption schemes, HE supports privacy-preserving computation, maintaining the confidentiality of data even in untrusted environments. Nevertheless, computational overhead and performance bottlenecks are still the main challenges in practical deployment [1].

Together, homomorphic encryption and blockchain create a robust model for secure computation in hybrid databases in a multi-cloud environment. Blockchain provides transparency, tamper resistance, and trust, while data privacy is ensured through homomorphic encryption during computation. In combination, these technologies render solutions to problems such as unauthorized access, data protection regulations, and secure inter-cloud transactions, making it a robust security model for database systems in the cloud.

C. Research objectives and scope

The primary objective of this study is to analyze and compare using blockchain and homomorphic encryption for improving multi-cloud hybrid database system security. This research has the following objectives:

- To evaluate security issues in place in multi-cloud hybrid setups.
- To study data provenance, access, and integrity protection capabilities of blockchain.
- To study privacy-preserving computation facilitation due to homomorphic encryption.
- To identify integration hurdles between blockchain and homomorphic encryption.
- Discuss potential improvements to meet performance and scalability limitations.

Various research has been carried out on blockchain's application in the security of data transactions and cloud storage. Studies have shown that blockchain-based provenance can be used to deter unauthorized modification and avoid central points of failure [3]. Various studies have explored homomorphic encryption, with its application highlighted in secure cloud computation and privacy protection [4].

There is a gap, however, in converging these two technologies to deliver an end-to-end security solution for multi-cloud hybrid databases. A comparison of the current methodologies reveals that today's security measures are highly dependent on trust-based access control and centralized trust models [7].

This review recognizes that homomorphic encryption and blockchain are both potent on their own but have yet to be deployed together to their maximum potential. The study intends to bridge the gap by considering actual use cases, performance compromises, and implementation methods, advancing the development of secure multi-cloud hybrid database systems.

II. BLOCKCHAIN IN MULTI-CLOUD HYBRID DATABASE SYSTEMS

A. Architecture and implementation

Blockchain technology integration in multi-cloud hybrid database environments is on the rise because it is decentralized and tamper-proof. Conventional multi-cloud infrastructure uses centralized control frameworks to deal with data over one cloud provider, and therefore, there are security issues and distrust. Blockchain has a built-in distributed ledger technology where transactional history, access logs, and security policies can be decentralized across various clouds.

The architecture of a typical blockchain-multi-cloud hybrid database includes the following key components:

- Decentralized Ledger
  The decentralized ledger is the underpinning of blockchain security in the form of an immutable, tamper-evident ledger of all transactions. In contrast to conventional databases based on central control, this layer shares trust across multiple cloud providers and nodes such that data remains intact, transparent, and secure against cyber attacks. With the removal of single points of failure, it offers safe, verifiable, and auditable multi-cloud operation.
- Interoperability Layer
  This layer facilitates interoperable communication and data exchange between various cloud infrastructures (AWS, Azure, Google Cloud, on-premise). It utilizes API gateways, middleware, and cross-cloud authentication mechanisms for effective, secure inter-cloud

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

collaboration. By providing standardized data exchange and access interfaces, it reduces compatibility problems and provides real-time data synchronization in distributed systems.

- Data Encryption & Anonymization Layer
  Security in the multi-cloud environment means protecting data at every stage, and this layer achieves that through tokenization and zero-knowledge proofs (ZKP). Other privacy improvement mechanisms like attribute-based encryption (ABE) and differential privacy also enhance data security without compromising usability.
- Blockchain Ledger
  The blockchain ledger ensures that all data changes, access logs, and security breaches are recorded forever in an infallible, cryptographically secure ledger. Each transaction is checked by a distributed agreement protocol (e.g., Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT)), meaning that unauthorized alteration is impossible [2]. This layer provides complete traceability, accountability, and international data security regulations compliance (GDPR, HIPAA, CCPA).
- Smart Contracts
  Smart contracts enforce security automatically, access, and compliance verification without intervention. They are used to authorize policy-based permission for access that guarantees that only authorized bodies can engage with sensitive information. Smart contracts limit human intervention in order to boost cloud efficiency, regulation, as well as anti-fraud mechanisms.
- Hybrid Database System
  The last safe storage and processing layer, the hybrid database system, combines blockchain with regular cloud databases to provide high-performance, scalable data processing. The layer also enables blockchain-secured encrypted queries so that cloud applications can perform secure computation in a safe way without undermining data integrity. It achieves security, performance, and cost-effectiveness using on-chain verification and off-chain storage optimization.

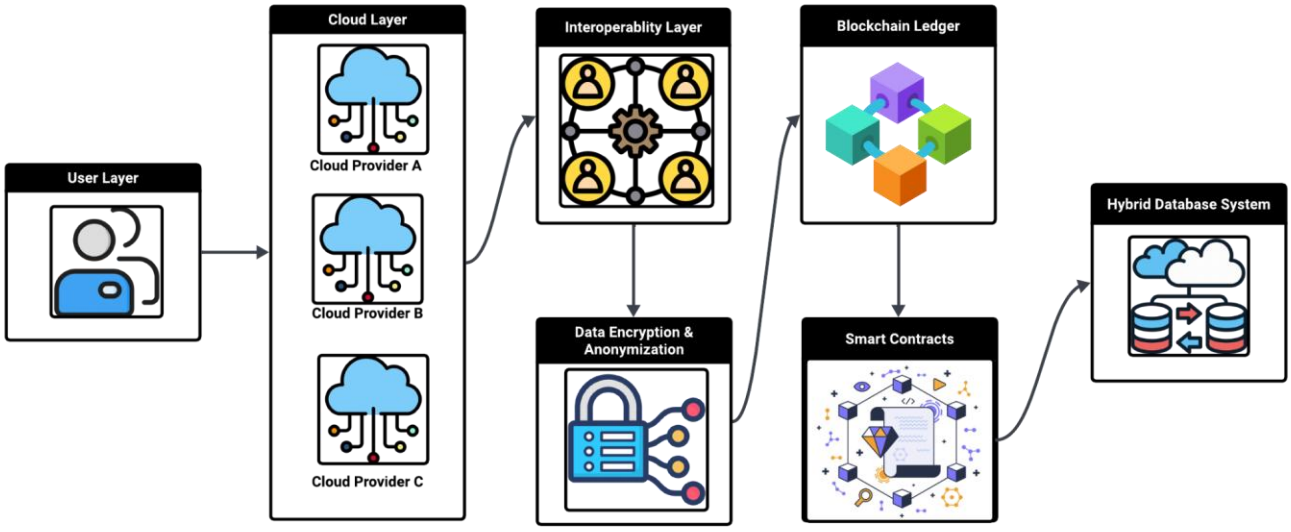

Figure 2: Blockchain-based multi-cloud hybrid database architecture

B. Security benefits and challenges

1. Security Advantages

Implementation of blockchain technology across multi-cloud hybrid database environments is accompanied by a chain of security advantages, mainly in terms of data integrity, decentralization of trust, and improved authentication processes. The advantages provide remedies for most challenges encountered by security when working with data across multiple cloud sources and on-premises setups.

- Data Integrity and Source:

Centralized control tends to be implemented in typical cloud-based databases for the sake of ensuring consistency and integrity of data. This makes it vulnerable to unauthorized modification, insider threats, and accidental data corruption. In hybrid multi-cloud database environments, blockchain's immutable ledger ensures data provenance by logging all transactions in an auditable format, with cryptographic chaining that does not allow data forgery [3]. This enables organizations to monitor changes, verify authenticity, and meet regulatory frameworks like GDPR and HIPAA.

- Decentralized Access Control:

In hybrid multi-cloud environments, it is hard to enforce the same access control in various cloud environments. Security models based on conventional approaches rely on centralized identity management systems and create a threat of single points of failure. Blockchain technology promotes decentralized access control by integrating self-sovereign identities (SSI), role-based blockchain authentication (RBBA), and smart contracts. These mechanisms facilitate the access and modification of given datasets by authorized users and processes alone, precluding privilege escalation attacks and credential theft.

- Improved Authentication Mechanisms:

The use of blockchain-based identity verification fortifies authentication procedures with the implementation of multi-factor authentication (MFA), zero-knowledge proofs (ZKP), and decentralized public-key infrastructure (DPKI). The methods remove password-username-based authentication, which is substituted with phishing attacks, credential exposure, and brute force attack-resistant cryptographic authentication techniques [8]. Blockchain's decentralized structure also guarantees identity verification and authentication records are verifiable worldwide but privacy-preserving, thereby strengthening data security in a hybrid cloud.

2. Security Issues

While it has its benefits, the integration of blockchain into multi-cloud hybrid database systems presents a chain of security issues that need to be resolved for real-world applications.

- Latency and Performance Bottlenecks

Blockchain transactions entail cryptographic verification and consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT) [2]. Verification incurs latency on real-time database transactions, rendering blockchain inappropriate for applications where instant access and data alteration are necessary. Although private blockchains (e.g., Hyperledger Fabric, Corda) are less latency-susceptible than public blockchains (e.g., Ethereum, Bitcoin), they do have some latency when processing transactions. Techniques such as off-chain storage, layer-2 scaling, and blockchain sharding are currently being developed to speed up transactions and minimize computational expense.

- Data Storage Overhead

Blockchain's need to hold a full, unalterable record of transactions is accompanied by enormous data storage overhead. In contrast to conventional cloud storage, where pruning of data and compression can be done, blockchain nodes must retain history data forever for integrity and consensus-proof purposes. This is even more intimidating in high-volume multi-cloud hybrid setups where database transactions create terabytes of logs every day. Solutions like Merkle tree optimization, pruning algorithms, and off-chain decentralized storage solutions (i.e., InterPlanetary File System (IPFS)) mitigate this problem, although more work must be done to attain blockchain storage scalability.

- Interoperability Problems

Multi-cloud hybrid architecture is constructed using a collection of database management systems (DBMS), cloud vendors (AWS, Azure, Google Cloud), and business applications. The inclusion of blockchain in these heterogeneous stacks involves middleware solutions, API gateways, and interoperability frameworks that need to be custom-tailored. Insufficient hybrid cloud security standard blockchain protocols hamper data exchange interoperability, homogeneous security policy imposition, and ensuring cross-platform compatibility [13]. Projects like Cross-Cloud Blockchain Interoperability (CCBI) and Decentralized Identity Foundation (DIF) try to mitigate these issues, but industrial-scale adoption remains an issue.

C. Performance considerations

The effect of blockchain on multi-cloud hybrid database system performance relies on a number of factors, such as consensus mechanism, network scalability, and storage efficiency. Public blockchains like Bitcoin and Ethereum are computationally intensive and slow with proof-of-work (PoW) consensus and are not feasible for enterprise cloud environments. The performance considerations of paramount importance are:

- Transaction Throughput: Legacy cloud databases handle transactions in milliseconds, and blockchain verification adds delays of seconds to minutes based on the consensus model.
- Storage and Computational Burden: It is computationally costly to store full blockchain ledgers in a cloud platform.
- Scalability Trade-offs: Scalability solutions on layer 2 (e.g., state channels and sharding) may improve blockchain efficiency with lower latency and fees [2].

D. Blockchain vs. Traditional Security Models

The transition from security models of the past to blockchain-based security in hybrid multi-cloud database systems represents a fundamental shift, and it affects trust, data governance, threat management, and abstraction techniques. Classical security models, though time-tested, have a bias toward centralized control points and are vulnerable to single points of failure, insider threats, and large-scale cyberattacks. Blockchain security, on the other hand, relies on a decentralized network so that no one entity has complete control over the system.

III. HOMOMORPHIC ENCRYPTION FOR SECURE DATA PROCESSING

Homomorphic encryption (HE) is a groundbreaking cryptographic technique that enables computations on data at rest without decrypting it. This feature is especially useful for multi-cloud hybrid database environments, where data must be kept private and secure with different cloud

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

vendors. Unlike conventional encryption, HE provides end-to-end data confidentiality, even within untrusted clouds.

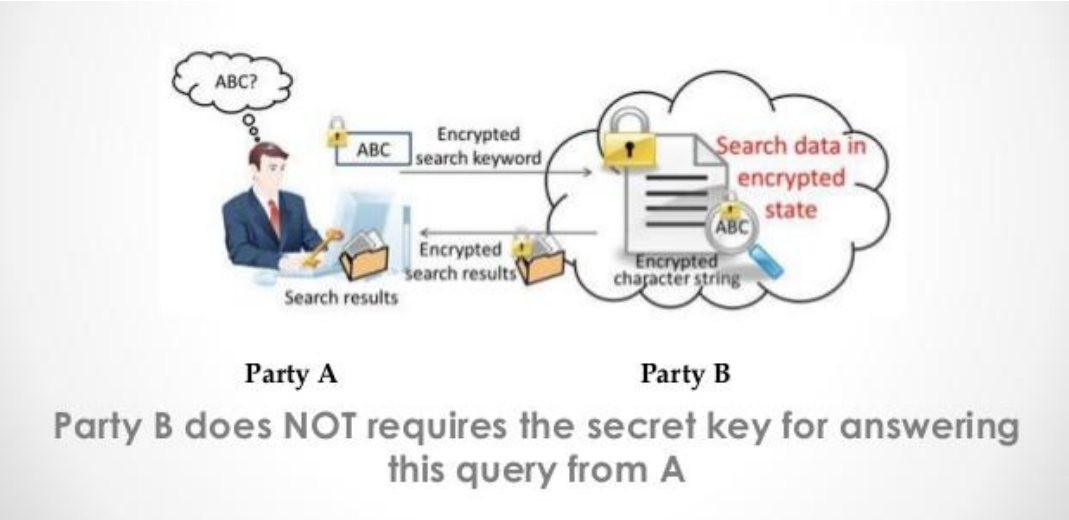

Figure 3: Homomorphic Encryption [15]

A. Types of homomorphic encryption schemes

Homomorphic encryption schemes are classified depending on whether they can perform arithmetic computation over ciphertexts. The three fundamental classes are:

- Partially Homomorphic Encryption (PHE): Can do only one type of operation, either addition or multiplication. Examples are RSA (Rivest–Shamir–Adleman) encryption, which can multiply, and ElGamal encryption, which can perform multiplicative homomorphism [9]. PHE is lightweight and efficient for trivial computations and hence suitable for verifiable encryption in authentication systems.
- Somewhat Homomorphic Encryption (SHE): Facilitates a small number of additions and multiplications prior to noise building up to render decryption risky. Though more lenient than PHE, SHE also faces computation boundaries that reduce its applicability in sophisticated cloud-based applications [5].
- Fully Homomorphic Encryption (FHE): The strongest type, with unlimited additions and multiplications over encrypted information. Originally proposed by Craig Gentry, FHE can perform any arbitrary function on encrypted data. It is, therefore, best suited for privacy-preserving cloud computing, machine learning over encrypted information, and secure multi-party computation. Substantial computational overhead, however, remains an issue in real-world implementations [5].

In homomorphic multi-cloud databases, the selection of the homomorphic encryption scheme depends on the degree of computational complexity, security needs, and performance.

B. Applications in cloud database systems

Homomorphic encryption is increasingly used in cloud databases for managing data to enable safe, privacy-aware data computation. The primary use cases are:

- Privacy-Preserving Database Queries: Decryption before query operation is required for regular cloud databases, exposing the data to a potential attack. HE enables secure search

and calculation on the ciphertext records, ensuring sensitive information is still safe even from the cloud provider [9].

- Secure Data Sharing & Multi-Cloud Storage: Organisations exchanging sensitive data between a group of different cloud providers can utilize HE to benefit from fine-grained access control without revealing plain text data to any particular cloud entity. Financial transactions, medical records, and government data storage use this feature greatly [5].
- Regulatory Compliance & Secure Auditing: GDPR and HIPAA guidelines specify stringent data security and audibility. HE allows auditors to verify compliance without decrypting information, lessening legal liability and increasing confidence in cloud computing.

Although the examples show how HE can secure cloud databases, the performance limitation must be removed in order to enable mass use.

C. Computational overhead and optimization techniques

Despite its security advantages, homomorphic encryption is costly to calculate, causing latency and expensive processing in cloud computing. The following methods are researched to enhance its efficiency:

- Noise Reduction & Bootstrapping: FHE operations introduce noise that reduces decryption quality. Bootstrapping, an operation introduced by Gentry's original FHE scheme, updates ciphertexts so that decryption would not fail. It is computationally costly, though, and needs more optimizations [5].
- Batching (SIMD Operations): Single Instruction Multiple Data (SIMD) permits several calculations to be performed simultaneously over encrypted data to enhance throughput. This especially benefits financial computations and encrypted database queries.
- Hybrid Cryptographic Models: Most cloud vendors use hybrid models where HE is blended with symmetric encryption or multi-party computation (MPC) to restrict overhead while maintaining privacy. This ensures maximum security and efficiency in real-time cloud applications [8].
- GPU & Hardware Acceleration: HE acceleration research on hardware like FPGAs and GPUs is focused on enhancing processing rates for big data-encrypted computations. This is necessary to enable HE for big data analysis in the cloud.

Optimizations enhance performance, yet actual deployment of fully homomorphic encryption in cloud databases still depends on prudent resource management and optimized architectures.

D. Homomorphic Encryption vs. Other Methods

Homomorphic encryption offers an exclusive set of benefits over conventional encryption as well as other encryption protocols utilized within securing cloud databases. Unlike traditional encryption, which needs to be decrypted before processing, HE enables secure data processing without losing confidentiality. The main barrier to HE adoption remains its computational overhead, but ongoing advances in efficiency and hybrid security models are making it a viable solution for next-generation cloud security architectures.

IV. INTEGRATION OF BLOCKCHAIN AND HOMOMORPHIC ENCRYPTION

The combination of homomorphic encryption (HE) and blockchain is a paradigm shift in secure multi-cloud hybrid database systems, solving the most critical issues of data integrity, confidentiality, and access control. Blockchain provides decentralized trust, data immutability, and

verifiable transactions, while homomorphic encryption provides secure computation on encrypted data, avoiding unauthorized usage even in untrusted environments.
Although they share interrelated capacities, their integration comes with computational and architectural challenges that must be overcome for large-scale adoption. This section explains how blockchain and homomorphic encryption complement each other, the pitfalls in their implementation, and the real-world applications of their integration.

A. Interrelated Elements and Potential Benefits
The combination of blockchain and homomorphic encryption leads to an assured security model that improves confidentiality, integrity, and auditability for cloud database systems.
1. Interrelated Key Features

- Data Security & Privacy:
  - Blockchain facilitates tamper-evident transaction logs but is not directly concerned with data confidentiality.
  - Homomorphic encryption provides data privacy by supporting computation on ciphertexts without decryption [5].
- Trust & Decentralization:
  - Blockchain eliminates centralized data authorities, providing transparent access records and verifiable transactions.
  - Homomorphic encryption keeps unauthorized data exposure at bay, maintaining data confidentiality even in decentralized storage systems.
- Regulatory Compliance & Data Protection:
  - Blockchain offers automated regulatory compliance via immutable audit trails.
  - HE offers data sovereignty compliance (e.g., GDPR, HIPAA, and CCPA) by providing protection against sensitive data exposure, even in computation.
- Decentralized Access Control:
  - Blockchain identity management substitutes conventional authentication systems with self-sovereign identities (SSI).
  - HE-secured credentials facilitate privacy-preserving user authentication without exposing personal information.

These interrelated capabilities render blockchain and homomorphic encryption a powerful couple for multi-cloud hybrid database protection, supporting privacy-preserving analysis, secure collaboration in the cloud, and cloud-resistant fraud-proof transactions.

B. Case studies and proof-of-concept implementations
Various research studies and business ventures have experimented with blockchain-based homomorphic encryption to protect multi-cloud hybrid environments.

1. Case Study 1: Privacy-Preserving Sharing of Healthcare Data
A HE and blockchain were employed by a multi-hospital research network to share patient data securely among cloud providers.
Implementation:
Encrypted patient record hashes were stored in the blockchain ledger to facilitate tamper-proof auditing.

Homomorphic encryption supported remote AI-based diagnosis on encrypted data without loss of privacy.
Outcome:
Data integrity and patient privacy were increased while medical research was GDPR compliant.

2. Case Study 2: Private Multi-Cloud Financial Transactions
A set of global banks deployed a blockchain-secured financial transaction system using homomorphic encryption for private computation.
Implementation:
HE was applied to conduct risk analysis on encrypted transactions without divulging account information.
Blockchain provided open, tamper-evident transaction history to avoid fraud.
Outcome:
Improved customer data secrecy and compliance with regulations in cross-border banking.

These initial deployments show how blockchain and homomorphic encryption may lock down cloud infrastructures, especially in healthcare, finance, and artificial intelligence-driven analytics.

Table 1: A comparison of features of Blockchain and Homomorphic Encryption Integration

Feature	Blockchain	Homomorphic Encryption (HE)	Blockchain + HE Integration
Data Confidentiality	Public ledger, data is transparent but pseudonymous	Ensures encrypted data remains private during computation	Combines HE's privacy with blockchain's integrity
Data Integrity	Ensures immutability through cryptographic hashing	Encryption alone does not verify the integrity	Immutable encrypted records for tamper-proof security
Trust Model	Decentralized, eliminates single points of failure	No inherent decentralization relies on encryption keys	Decentralized encrypted data processing
Computation on Encrypted Data	Not supported (data must be decrypted for processing)	Fully supports secure encrypted computations	Allows privacy-preserving computations on the blockchain
Scalability	Limited due to high storage and processing demands	Computationally expensive, especially for FHE	Requires optimization for real-time multi-cloud use
Regulatory Compliance	Provides audibility but lacks data privacy	Meets GDPR, HIPAA, and CCPA by preventing exposure	Supports regulatory compliance while ensuring transparency

Storage Overhead	Requires full ledger replication across nodes	Encrypted data is larger than plaintext	Hybrid storage (off-chain encrypted data, on-chain hashes)
Latency	High due to consensus mechanisms	High due to complex encryption computations	Optimization needed to reduce processing overhead
Interoperability in Multi-Cloud	Standardized APIs and frameworks exist	Limited cloud support, requires specialized middleware	Requires blockchain-aware encryption frameworks
Security Threats	Susceptible to quantum computing attacks	Computationally secure, but key management is crucial	Strong security model, but requires efficient key handling

V. PRIVACY AND SECURITY INSIGHTS

With multi-cloud hybrid database systems currently in vogue, security and privacy are the topmost issues. Organizations operating distributed cloud-based infrastructures need to guarantee data confidentiality, integrity, and strict access controls to avoid issues like unauthorized access, insider attacks, and data breaches. A multi-layered security framework with the implementation of blockchain and HE is an option, but issues of improving efficiency, authentication frameworks, and compliance persist.

This section discusses key security and privacy issues that include data confidentiality, integrity, access control, and authentication mechanisms within multi-cloud environments.

A. Data confidentiality and integrity

1. Ensuring Data Confidentiality

Confidentiality of data is important in cloud settings where sensitive information is stored, processed, and transmitted between various cloud providers. The following methods supplement data privacy for multi-cloud hybrid database systems:

- Homomorphic Encryption for Privacy-Preserving Computation:
  - Traditional encryption protects data in transit and at rest but must be decrypted before it can be processed, exposing sensitive data to attack.
  - Homomorphic encryption allows mathematic operations to be performed on an encrypted piece of data without revealing its secrecy and without decrypting it in the process [4].
  - Example: A bank processing encrypted customer transactions between cloud providers can perform risk calculations securely without revealing raw information.
- Blockchain for Immutable and Confidential Data Logging:
  - While blockchain provides data provenance and integrity, its public nature can violate confidentiality.

- To avoid this, hybrid architectures place only cryptographic hashes on-chain, with encrypted data stored off-chain in a secure cloud database.
- Example: A health system handling patient data can use blockchain for access logs and HE for privacy, being HIPAA compliant [5].

- Access-Based Data Partitioning:
  - Sensitive information can be partitioned across several cloud providers such that no single party has complete access to unencrypted information.
  - Attribute-Based Encryption (ABE) also enhances role-based data access, enabling users to download only approved parts of encrypted data sets [6].
  - Collectively, these controls supporting confidentiality create a strong security mechanism for cloud databases, protecting against data exposure attacks while supporting successful, privacy-augmented operations.

2. Ensuring Data Integrity

Data integrity guarantees that stored and processed information is not manipulated and is verifiable, avoiding tampering, unintended corruption, and insider attacks. The following mechanisms guarantee data integrity in multi-cloud environments:

- Blockchain for Tamper-Proof Data Auditing:
  - Blockchain provides tamper-proof data provenance in multi-cloud hybrid database platforms by cryptographically chaining all the transactions within a distributed ledger such that unauthorized data rollback and modification are practically impossible [3].
  - Example: In a supply chain management use case, blockchain can confirm logistics records to catch real-time unauthorized modifications.
- Merkle Trees for Integrity Verification:
  - Cloud-stored data sets can make use of Merkle tree-based cryptographic proofs in order to confirm the authenticity of data in an efficient manner without revealing raw data.
  - Example: Secure votes can be saved through a cloud-voting system using Merkle trees and blockchain-based validation for providing tamper-evidence elections [3].
- Secure Multi-Party Computation (SMPC) for Cross-Cloud Data Processing:
  - SMPC allows secure computation over distributed data in cloud providers without revealing raw data.
  - It prevents data tampering during collaborative multi-cloud computations and provides accuracy and security in financial or healthcare applications.

B. Access control and authentication

1. Challenges with Traditional Access Control Models

Hybrid multi-cloud database systems have sophisticated authentication and access control issues, such as:

- Various authentication models from cloud providers hinder the consistent implementation of security.
- Centralized models of access control introduce single points of failure, leaving data vulnerable to insider threats and credential theft.
- Role-based access control (RBAC) is static and does not support dynamic enforcement of policy, and hence it is inefficient for current cloud applications.

To combat these problems, new blockchain-based and cryptographic authentication systems are under investigation.

2. Blockchain-Based Decentralized Access Control
Blockchain facilitates access control using self-sovereign identities (SSI), smart contract-based authorization, and decentralized authentication models:

- Self-Sovereign Identity (SSI):
  - Authenticity using traditional methods is based on centralized parties (OAuth, Active Directory, etc.), which is a security risk.
  - Blockchain-based SSI enables users to hold their own encrypted identity credentials without central reliance.
  - Example: A cloud-based healthcare database can utilize SSI to authenticate patients for privacy-compliant access control.
- Dynamic Role-Based Access Control (RBAC) with Smart Contracts:
  - Smart contracts dynamically grant and revoke access without overprivileged access.
  - Example: An enterprise cloud database can utilize smart contracts to limit employee access depending on project assignments to reduce exposure to unauthorized data.
- Blockchain-based Multi-Factor Authentication (MFA):
  - Blockchain MFA clarifies dependence on conventional password-based security, thus minimizing credential theft and phishing attacks.
  - Example: Banks can use blockchain-authenticated biometric authentication, allowing fraud-free identification [7].

These methods offer decentralized, flexible access control, safeguarding against identity attacks in multi-clouds.

3. Homomorphic Encryption for Secure Authentication
While blockchain protects identity management and authorizations, homomorphic encryption enhances the security of authentication by making it private:

- Zero-Knowledge Proof (ZKP) Authentication
  - ZKPs enable individuals to verify identities without exposing confidential credentials.
  - Example: A government cloud infrastructure can verify user identities without plain text storage of credentials, protecting against identity theft.
- Homomorphic Token-Based Authentication:
  - Homomorphic authentication tokens can be used in cloud applications to provide secure login authentication without decrypting stored credentials.
  - Example: A cloud bank application could conduct homomorphic authentication tokens to facilitate secure, privacy-protecting transactions.

By combining blockchain's decentralized identity management with authentication mechanisms powered by HE, scalable, privacy-preserved access control is given to cloud infrastructure, and credential-based attacks are minimized.

VI. PERFORMANCE EVALUATION

The combination of homomorphic encryption (HE) with blockchain within multi-cloud hybrid database systems brings a suite of security benefits that also carry the price of performance trade-

offs in areas such as scalability, latency, and throughput. Since multi-cloud environments demand effective real-time processing and secure access control, it is crucial to analyze the performance of the integration of blockchain-HE so that it can be verified for real-world viability.
This section discusses scalability issues, latency issues, and throughput bottlenecks and compares blockchain-HE integration to conventional security techniques to emphasize performance trade-offs.

A. Scalability in multi-cloud environments

1. Scalability Challenges in Scaling Blockchain and HE in Multi-Cloud Deployments

Scalability is a key challenge for blockchain and HE-based systems because:

- Blockchain's replication process, in which every transaction needs to be stored and validated by multiple nodes, leading to data redundancy and network load.
- Homomorphic encryption's computational cost, slowing down real-time query computation on encrypted data [9].
- Multi-cloud interoperability challenges, where each cloud provider has different storage, networking, and compute boundaries impacting scale consistency [10].

2. Scalability Optimization Techniques

To enhance scalability, the following techniques are being investigated:

- Off-Chain and Layer-2 Scalability Solutions for Blockchain:
  - State channels and sidechains off-load on-chain transactional load to enhance processing efficiency for multi-cloud hybrid deployments.
  - Sharding techniques split blockchain records into multiple partitions to support parallel transaction verification.
- Batch Processing and Noise Cancellation for HE:
  - Batching methods execute numerous encrypted operations concurrently, lowering HE computation overhead.
  - Optimized HE libraries (e.g., PALISADE, Microsoft SEAL) support more efficient execution of encrypted queries.
- Cross-Cloud Load Balancing for Distributed Processing:
  - Decentralized cloud orchestration facilitates agile workload distribution in an effort to maximize storage scalability, computational effectiveness, and trustworthy blockchain verification and thus guarantee improved data management and privacy breach protection in mobile cloud computing [11].

3. Real-World Multi-Cloud Scalability Benchmarking

- Case Study: A homomorphically encrypted AI model based on the cloud with privacy-preserving training over multi-clouds had scalability bottlenecks as ciphertext sizes increased. Distributed GPU acceleration and encryption key optimization enhanced the scalability significantly.

B. Latency and throughput analysis

1. Factors Influencing Latency in Blockchain-HE Architectures

International Journal of Core Engineering & Management
Volume-6, Issue-06, 2019 ISSN No: 2348-9510

The integration of blockchain and homomorphic encryption introduces massive latency issues, especially for real-time data processing and encrypted database queries.

- Blockchain Transaction Verification Latencies:
  - Public blockchains incur extremely high times to validate transactions because of consensus protocols (e.g., Proof of Work - PoW, Practical Byzantine Fault Tolerance - PBFT) [2].
  - Private blockchain implementations (e.g., Hyperledger Fabric, Quorum) minimize latency but need trusted authority nodes.
- Homomorphic Encryption Processing Latencies:
  - Encrypted computations add processing time over plaintext operations, especially in the case of Fully Homomorphic Encryption (FHE) schemes.
  - Noise build-up during encryption necessitates bootstrapping at frequent intervals, which introduces considerable processing time [7].

2. Bottlenecks in Throughput in Blockchain and HE Systems

Throughput refers to the number of operations executed per unit of time and is an essential metric for multi-cloud systems with large amounts of encrypted transactions.

Table 2: Latency and Throughput analysis of various security models

Security Model	Average Transaction Latency	Throughput (Transactions per Second - TPS)
Traditional Security (TLS, AES Encryption)	Milliseconds (low overhead)	High (~10,000 TPS in cloud DBs)
Blockchain (Ethereum PoW)	~15 seconds per block	Low (~15 TPS, increases with Layer-2 scaling)
Homomorphic Encryption (FHE-based query execution)	~3-10x slower than plaintext processing	Limited (~100-200 queries per second in optimized settings)
Blockchain + HE Integration	Higher due to consensus + encryption overhead	Varies (~10-200 TPS, dependent on architecture & optimizations)

3. Optimization Methods to Enhance Performance

- Employing Proof-of-Stake (PoS) or Proof-of-Authority (PoA) for Blockchain Consensus:

Reduces delay in transaction validation by eliminating Proof-of-Work (PoW) computational waste [2].

- Parallel Computation for HE:

Distributed and GPU-accelerated homomorphic encryption enhances the throughput efficiency of HE in the cloud.

- Edge Computing and Fog Computing for Reducing Latency:

Homomorphic encryption offloading in the edge layer minimizes the latency in transferring data across cloud providers.

4. Real-World Case Study of Enhancing Latency

- Case Study Example with a Financial Institution:

- A blockchain-secured banking transaction system with FHE integration was plagued by query latency.
- A shift to Somewhat Homomorphic Encryption (SHE) and hybrid blockchain consensus model usage resulted in a greater boost in transaction rate [7].

VII. FUTURE RESEARCH DIRECTIONS

The unification of homomorphic encryption (HE) and blockchain in multi-cloud hybrid database systems has developed a strong paradigm for decentralized, privacy-assured, and secure computing systems. Nonetheless, some future trends, open issues, and research directions have to be met with a view to providing scalability, efficiency, and interoperability to the security models. Future research directions are discussed in this section, with a particular focus on emerging technologies, open issues, and their implications on cloud security, enterprise applications, and research studies.

A. Emerging trends and technologies

A number of breakthroughs in cryptography, distributed computing, and secure data processing are driving the future of blockchain-HE convergence in the cloud.

- Quantum-Safe Cryptography for Post-Quantum Security
  - Quantum computing poses a serious threat to current public-key encryption and blockchain security models.
  - Lattice-based cryptography and quantum-resistant HE algorithms are being considered as possible countermeasures [5].
  - Hybrid cryptographic designs, mixing legacy HE with post-quantum cryptography, will be required to provide long-term security for cloud infrastructure.
- Decentralized Identity Management (DID) and Privacy-Preserving Authentication
  - Self-sovereign identity (SSI) protocols are gaining traction, allowing users to own identity credentials without central control.
  - Homomorphic token-based authentication will be required for privacy-preserving multi-cloud access control.
  - Combining blockchain-based identity management with HE-secured authentication techniques can avoid credential stealing, unauthorized data access, and insider attacks [7].
- Cross-Cloud Blockchain Interoperability Solutions
  - The absence of a single scheme to implement blockchain across multi-cloud infrastructures is the greatest challenge, stopping seamless integration, security support, and efficient management of blockchain networks [12].
  - Interoperability frameworks like Cross-Cloud Blockchain Interoperability (CCBI) are being researched to facilitate end-to-end communication between cloud-based blockchains.

These solutions will provide secure, cross-cloud transactions and decentralized governance models, minimizing dependency on centralized intermediaries.

B. Open challenges

Despite recent progress, blockchain and HE integration also have several technical and practical issues to address with continued research and optimization.

1. Computational Overhead and Processing Efficiency
   Homomorphic Encryption (HE) is still computationally costly, contributing significantly to processing time and storage needs [6].
2. Scalability and Blockchain Transaction Speed
   Blockchain transaction validation is associated with latency and scalability problems, and it is not feasible for cloud applications with high throughput.
3. Multi-Cloud Key Management Security
   Homomorphic encryption is based on sophisticated key management systems, and storage quotas in blockchain ledgers make further safe key deployment difficult.
4. Data Protection Compliance
   Cloud data processing and storage must comply with strict privacy laws (GDPR, HIPAA, CCPA), and blockchain's immutability contradicts the erasure rights of data.

By addressing such open challenges, blockchain-HE integration has the potential to be a powerful solution for multi-cloud protection with high performance and regulatory compliance.

C. Implications for practice and research

The innovations in blockchain and HE security models will have major effects on industry usage, cloud security regulation, and research.

1. Consequences for Industry and Enterprise Deployment

- Companies will have to deploy hybrid encryption plans that balance out HE's computation security with the blockchain's integrity promise.
- Government bodies, healthcare companies, and banking institutions will pioneer the use of blockchain-based privacy-preserving cloud structures.
- Quantum-proof cryptography solutions will be ever more necessary as cloud computing environments are ready to cope with post-quantum security issues.

2. Cloud Security Governance Implications

- Businesses using multi-cloud systems will need standardized security models to be transformed into shapes that harmonize blockchain and privacy-enhancing encryption models [12].
- Decentralized identity management (authentication based on DIDs) will be one of the primary multi-cloud access management and compliance building blocks.
- Government and regulatory authorities might recommend compliance models specially engineered for blockchain-based cloud security.

3. Implications for Future Research

- Further optimization of HE algorithms will be needed to enhance latency, efficiency, and scalability for massive cloud applications.
- Quantum-resistant HE models will be researched to ensure long-term cloud security.
- The intersection of edge computing, HE, and blockchain is an area still to be researched, particularly for low-latency, privacy-enhancing IoT and 5G use cases.

These research directions will set the course for the decade ahead of cloud security innovation, ensuring that privacy-enhancing computing remains in the game in the era of decentralized cloud architecture.

REFERENCES

1. L. Zhou, L. Wang, T. Ai, and Y. Sun, "Beekeeper 2.0: Confidential blockchain-enabled IoT system with fully homomorphic computation," *Sensors*, vol. 18, no. 11, p. 3785, 2018.
2. L. Feng, H. Zhang, Y. Chen, and L. Lou, "Scalable dynamic multi-agent practical Byzantine fault-tolerant consensus in permissioned blockchain," *Applied Sciences*, vol. 8, no. 10, p. 1919, 2018.
3. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid, Spain, 2017.
4. A. Wainakh, "Homomorphic Encryption for Data Security in Cloud Computing," *ResearchGate Preprint*, 2018.
5. A. El-Yahyaoui and M. D. Ech-Cherif El Kettani, "A Verifiable Fully Homomorphic Encryption Scheme for Cloud Computing Security," *Technologies*, 2019.
6. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 9, pp. 2546-2559, 2016.
7. Y. Gahi, M. Guennoun, Z. Guennoun, and K. El-khatib, "On the Use of Homomorphic Encryption to Secure Cloud Computing, Services, and Routing Protocols," *arXiv Preprint*, 2015.
8. M. Li, C. Qin, and P. P. C. Lee, "CDStore: Toward Reliable, Secure, and Cost-Efficient Cloud Storage via Convergent Dispersal," *arXiv Preprint*, 2015.
9. Q. Wang, D. Zhou, and Y. Li, "Secure Outsourced Calculations with Homomorphic Encryption," *arXiv Preprint*, 2018.
10. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222-233, 2014.
11. H. Li, D. Liu, Y. Dai, T. H. Luan, and X. Shen, "Enabling Efficient Multi-Keyword Ranked Search over Encrypted Mobile Cloud Data through Blind Storage," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 127-138, 2015.
12. K. Rajasekhar, N. Rohith, G. Mohan, D. Divya, and C. Bharathi, "Enhancement of blockchain security using re-authentication of digital signatures," *International Journal of Engineering & Technology*, vol. 7, no. 1.1, p. 667, 2017.
13. "Key Strategies for Securing the Hybrid Cloud," *Trend Micro*, 2018.
14. S. Washington, "The Benefits of Hybrid Cloud Computing", *mindcentric*, 2018.
15. N. E. N. Fernandes, "Homomorphic encryption, statistical machine learning and R software package", *The Intelligence of Information*, 2017.