Cloud computing security, blockchain technology

UDK 004.75:004.56

Yurii Balandiuk[1], Iryna Plavutska[2]

Ivan Pul'uj Ternopil National Technical University, [1]univ@tntu.edu.ua

Modern information infrastructure is based on a cloud computing model, which enables dynamic scaling and cost optimization. However, the consolidation of data in centralized architectures creates a unique landscape of cyber threats related to privacy breaches. Traditional protection methods prove insufficient in the face of intensifying sophisticated, targeted attacks and zero-day vulnerabilities. This necessitates the integration of decentralized mechanisms for verifying system integrity. Blockchain technology serves as a fundamental tool for building trusted environments thanks to its distributed architecture. The interaction of clouds and distributed ledgers enables the implementation of the concept of automated real-time computation auditing [1].

The aim of this work is to justify and develop blockchain-based architectural solutions to enhance the security of cloud environments through the implementation of decentralized verification protocols. The relevance of this research is underscored by the need to protect critical infrastructure from unauthorized access in the absence of complete trust in cloud providers.

The primary attack vectors remain unauthorized API exploitation and account takeover through token compromise. A specific vulnerability is the resource-sharing architecture, which allows for side-channel attacks between virtual machines. The lack of direct control over the physical level of data storage creates a “black box” problem for the customer. Internal threats from data center administrators remain a critical risk factor for the corporate sector. Massive DDoS attacks can exhaust capacity limits, causing a complete denial of service. Each of the outlined problems requires a shift from passive security measures to active decentralized architectures [2].

The scientific novelty of this research lies in the development of a hybrid integrity control model that combines the scalability of cloud computing with the mathematical invariance of distributed ledgers. Unlike known centralized monitoring systems, the proposed approach prevents the covert removal of breach traces through consensus-based verification of each record.

Blockchain technology is based on the principles of distributed consensus, where every node in the network verifies the integrity of the ledger. The cryptographic hash of the previous state in each block makes it computationally infeasible to alter data retroactively. The decentralized nature of the ledger eliminates the risk of a single point of failure in the security architecture. Smart contracts allow security business logic to be implemented directly into the data exchange protocol. Transaction transparency enables continuous technical auditing without interrupting core services. The persistence of records in a distributed ledger eliminates the possibility of covertly deleting traces of unauthorized activity. Minimal trust in the provider is offset by mathematical proof of the correctness of all transactions [3].

The implementation of the “Blockchain-as-a-Service” model enables the integration of decentralized nodes into cloud orchestration clusters. Blockchain acts as an identity management layer, replacing vulnerable centralized databases.

Distributed key management prevents the entire system from being compromised due to a data leak from a single segment. Smart contracts ensure the automatic enforcement of access policies based on verified subject attributes. Any attempt at unauthorized modification of the network configuration is automatically rejected by the consensus mechanism. This captures all infrastructure changes as code, preventing covert drift in security settings. Such integration enhances the system's resilience against attacks at the level of logical resource management.

A critical aspect is integrity control, where the hash values of objects are stored in an immutable distributed ledger. Automatic hash verification during read operations allows for the detection of tampering that bypasses management interfaces. Blockchain ensures full traceability of the information lifecycle with precise timestamps. The use of multi-signatures enhances control over critical operations involving large data sets. Decentralized storage further guarantees confidentiality through content fragmentation and encryption. The failure of some nodes does not result in data loss thanks to over-encoding algorithms. The user retains full control over the keys, preventing the provider from accessing encrypted information. Each integrity check is automatically recorded as a transaction, making it impossible for the monitoring system to be compromised without detection. The implementation of Merkle Tree mechanisms allows for the rapid verification of large data blocks without the need to download the entire array from the cloud. This significantly optimizes the load on network communication channels and increases the performance of verification nodes. The use of smart contracts enables the automatic restoration of damaged segments from mirrored network nodes. The system automatically detects anomalies in hash sums and isolates compromised memory segments until incident management is fully completed. Additional cryptographic redundancy ensures the architecture's resilience against targeted attempts to degrade service quality. This creates robust protection against man-in-the-middle attacks at the cloud storage infrastructure level. Therefore, blockchain transforms passive storage into an active ecosystem with built-in immunity to unauthorized modifications.

The study's findings show that, despite scalability challenges, blockchain integration significantly increases trust in cloud services. The industry's future prospects hinge on the adoption of post-quantum algorithms to protect against future threats. Zero-knowledge proof technologies enhance privacy without compromising the ability to validate data.

1. Gartner: Top Strategic Technology Trends for 2025–2026. URL: https://www.gartner.com/en/information-technology/topics/technology-trends (application date 10.11.2025).
2. Cloud Security Alliance (CSA): Top Threats to Cloud Computing. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/ (application date 08.06.2019).
3. IBM: What is blockchain security? URL: https://www.ibm.com/think/topics/blockchain-security (application date 05.06.2025).