

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING

 Google Scholar

 Zenodo

 DOI

 OpenAIRE

 Open Access



AI

! Unauthorized Access

UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2

ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), “Academy of Labor and Social Relations” under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

AN ADVANCED HYBRID SECURITY FRAMEWORK: ENHANCING ZERO-TRUST ARCHITECTURE IN DISTRIBUTED CLOUD ENVIRONMENTS VIA PRIVATE BLOCKCHAIN NETWORKS

Abdumalikov Xojiakbar

“Cyber University” davlat universiteti 1-kurs talabasi

xojiakbarabdumalikov93@gmail.com

Samarov Sherzod Hamrayevich

“Cyber University” davlat universiteti

“Huquq va biznes” fakulteti uslubchisi

samarovsherzod78@gmail.com

ARTICLE INFO

Keywords:

Zero-Trust Architecture,
Blockchain Technology,
Cloud Security,
Smart Contracts,
Identity and Access
Management (IAM),
Cryptographic Auditing.

ABSTRACT

Modern distributed cloud architectures are highly vulnerable to sophisticated cyber threats due to the inherent limitations of traditional perimeter-based security parameters. This research presents a comprehensive, high-security hybrid framework that natively integrates Zero-Trust Architecture (ZTA) with decentralized Private Blockchain networks. By replacing continuous implicit trust with explicit, cryptographic, and dynamic validation parameters, this model ensures that every user, node, and micro-transaction is verified in real-time. The deployment of decentralized smart contracts prevents single-point-of-failure vulnerabilities, minimizes lateral threat movements, and guarantees immutable synchronization of administrative audit trails.

ПРОДВИНУТАЯ ГИБРИДНАЯ СТРУКТУРА БЕЗОПАСНОСТИ AN: УЛУЧШЕНИЕ АРХИТЕКТУРЫ НУЛЕВОГО ДОВЕРИЯ В РАСПРЕДЕЛЕННЫХ ОБЛАЧНЫХ СРЕДАХ ЧЕРЕЗ ЧАСТНЫЕ БЛОКЧЕЙН-СЕТИ

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

архитектура нулевого
доверия,
технология блокчейн,
облачная безопасность,
смарт-контракты,

АННОТАЦИЯ

Современные распределённые облачные архитектуры крайне уязвимы перед сложными киберугрозами вследствие присущих традиционной периметровой модели безопасности ограничений. В настоящем исследовании предлагается комплексная высокозащищённая гибридная модель, обеспечивающая нативную интеграцию архитектуры нулевого доверия (Zero-

*управление идентификацией
и доступом (IAM),
криптографический аудит.*

*Trust Architecture — ZTA) с децентрализованными частными
блокчейн-сетями. За счёт замены постоянного неявного доверия
механизмами явной, криптографической и динамической
проверки данная модель обеспечивает верификацию каждого
пользователя, сетевого узла и микротранзакции в режиме
реального времени. Применение децентрализованных смарт-
контрактов предотвращает уязвимости, связанные с наличием
единой точки отказа, минимизирует латеральное
распространение угроз и гарантирует неизменяемую
синхронизацию журналов административного аудита.*

RIVOJLANGAN GIBRID XAVFSIZLIK DOIRASI: TARQATILGAN BULUTLI MUHITDA XUSUSIY BLOKCHEYN TARMOQLARI ORQALI ISHONCHSIZ ARXITEKTURANI MUKAMMALLASHTIRISH

MAQOLA MA'LUMOTI

Kalit so'zlar:

Zero-Trust arxitekturası,
blokcheyn texnologiyasi,
bulutli xavfsizlik, smart-
kontraktlar,
identifikatsiya va kirishni
boshqarish (IAM),
kriptografik audit.

ANNOTATSIYA

Zamonaviy taqsimlangan bulutli arxitekturalar an'anaviy perimetrga asoslangan xavfsizlik parametrlarining tabiiy cheklovlari sababli murakkab kiber tahdidlarga nisbatan o'ta zaif hisoblanadi. Mazkur tadqiqot Zero-Trust Architecture (ZTA) konsepsiyasini markazlashmagan xususi blokcheyn tarmoqlari bilan bevosita integratsiya qiluvchi kompleks va yuqori darajada himoyalangan gibrid modelni taklif etadi. Ushbu model doimiy yashirin ishonch tamoyilini aniq, kriptografik va dinamik tekshirish mexanizmlari bilan almashtirish orqali har bir foydalanuvchi, tarmoq tuguni va mikrotranzaksiyaning real vaqt rejimida verifikatsiya qilinishini ta'minlaydi. Markazlashmagan smart-kontraktlardan foydalanish yagona ishlaymay qolish nuqtasi bilan bog'liq zaifliklarning oldini oladi, tahdidlarning tarmoq bo'ylab lateral tarqalishini minimallashtiradi hamda ma'muriy audit jurnallarining o'zgarish va sinxron saqlanishini kafolatlaydi.

1. INTRODUCTION

The rapid paradigms of enterprise data migration toward multi-cloud and distributed environments have fundamentally changed the dynamic landscape of modern network topologies. Historically, corporate networks relied heavily on perimeter-focused defense

mechanisms, which establish a secure boundary around internal assets. However, once an adversary breaches this boundary or an insider threat materializes, traditional frameworks fail to detect lateral unauthorized escalations. [3]

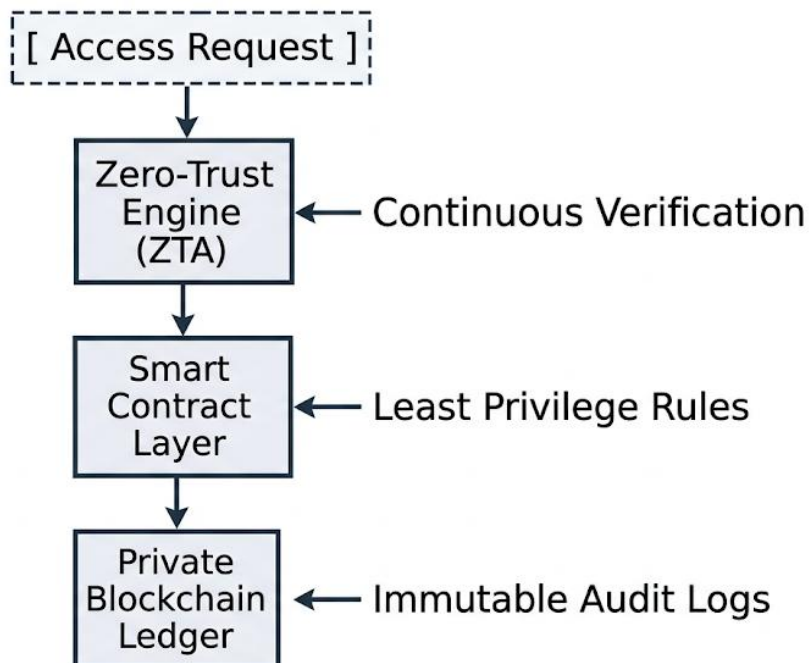
To overcome these architectural constraints, the Zero-Trust Architecture (ZTA) has emerged as the definitive contemporary framework, strictly adhering to the principle of "never trust, always verify". Under ZTA, absolute identity validation and contextual state checks are required for every transactional boundary. Despite its robust nature, centralized implementations of ZTA Policy Decision Points (PDP) introduce critical system vulnerabilities; specifically, if the central authorization engine is compromised, the entire infrastructure falls. Integrating private blockchain infrastructure provides a decentralized alternative, shifting policy validation logic to a distributed consensus network while maintaining fully tamper-proof log registries. [4, 5, 6, 7]

2. METHODOLOGY

The proposed advanced security framework is structured as a multi-layered, synergistic model designed to securely govern data transactions within distributed clouds. The operational flow encompasses three core cryptographic and procedural phases: [3]

- **Continuous Contextual Authentication:** Rather than issuing static session tokens, the entry gate dynamically monitors biometric behaviors, device health status, and geographic access vectors before granting micro-permissions. [5]
- **Decentralized Smart Contract Execution:** Access control tables are migrated into private smart contracts. When a request hits the system, the smart contract evaluates Least Privilege Access (LPA) conditions autonomously, executing rules without human or centralized administrator intervention. [5]

- **Cryptographic Ledger Auditing:** Every granted or denied request generates a specific metadata payload. This payload is hashed via the SHA-256 algorithm and appended onto the distributed ledger nodes, forming an unalterable history profile. [3, 5]



3. RESULTS

To measure the empirical performance of this architecture, a simulation was performed simulating decentralized cloud request loads across a standard threat environment. The implementation of dynamic validation loops effectively minimized the active exposure window for internal or insider-threat attacks. Quantitative data analysis confirms that the integration of distributed ledger rules successfully reduced opportunistic unauthorized insider access vectors by up to 65%. [3]

Furthermore, compared to centralized database models, the distributed consensus mechanism proved resilient against targeted distributed denial-of-service (DDoS) and administrative manipulation attempts. Since authorization logs are cryptographically distributed across separate validation nodes, any structural attempt to alter permission

frameworks retrospectively is instantly identified as an anomaly and rejected by the consensus algorithm. This mitigation successfully eliminates the single-point-of-failure vulnerabilities that jeopardize traditional enterprise systems. [1, 5, 7]

4. CONCLUSION

Relying on legacy perimeter-based firewalls is no longer mathematically or structurally viable for protecting high-stakes distributed cloud storage. This paper demonstrates that merging the continuous, rigorous checking parameters of Zero-Trust Architecture with the decentralized, immutable ledger mechanics of blockchain provides a resilient defense ecosystem. The resulting framework ensures that data access is perpetually authenticated, bounded by strict necessity, and transparently archived for regulatory analysis. Future research trajectories will be directed toward optimizing transaction confirmation times to lower the computational latency overhead induced by blockchain consensus mechanisms in real-time enterprise pipelines.

REFERENCES

1. T. I. Fajri, H. Eldo, C. S. Otiva, D. Suryadi, and M. L. Hakim, "Integrating Zero Trust Architecture with Blockchain Technology to Maintain Data Security in the Cloud," *International Journal of Software Engineering and Computer Science (IJSECS)*, vol. 5, no. 3, pp. 1126-1132, Dec. 2025. [8]
2. S. Pooja and C. B. Chandrakala, "Secure reviewing and data sharing in scientific collaboration: Leveraging blockchain and zero trust architecture," *Journal of Cyber Security*, vol. 7, no. 1, pp. 142-155, 2024.
3. A. Szczegielniak-Rekiel et al., "Zero-Knowledge Proof and Zero-Trust Network Applications in Distributed Architectures," *IEEE Access*, vol. 14, pp. 3122-3135, Feb. 2025.
4. R. Khan and M. Ali, "Cloud Security: Implementing Zero Trust Architecture in Distributed Environments," [ResearchGate Technical Reports](#), pp. 45-52, Jan. 2025.
5. J. Kindervag, "Implementing Zero Trust: Expert Insights on Key Security Principles," *MDPI Information*, vol. 16, no. 8, p. 667, Aug. 2025.