International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September-October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805027

Blockchain-based Identity and Policy Management for Distributed Cloud Services

Amar Gurajapu

Network Systems, AT&T, United States

Vardhan Garimella

Intellibus, United States

ABSTRACT: Distributed cloud services across multiple providers demand consistent identity verification and policy enforcement. Centralized IAM and policy managers introduce single points of failure, limited auditability, and latency. We propose BC-IdPol, a blockchain-based framework that stores identities and governance policies on a permissioned ledger. Smart contracts enforce registration, authentication, and policy retrieval. Off-chain cloud agents query the chain for runtime decisions. In experiments over a three-cloud prototype (Azure, AWS, GCP) on Hyperledger Fabric, BC-IdPol achieved:

- 99.9 % tamper-resistance (vs. 0 % baseline)
- 45 ms median identity lookup latency (vs. 18 ms centralized API)
- 60 ms median policy fetch time (vs. 20 ms baseline)
- 1,800 req/sec enforcement throughput (vs. 2,200 req/sec)

We detail architecture, smart-contract design, mermaid diagrams, evaluation results, limitations, and future work.

KEYWORDS: Blockchain, Identity Management, Policy Management, Distributed Cloud, Smart Contracts, Hyperledger Fabric, IAM, Policy-as-Code

I. INTRODUCTION

Modern applications span on-premises and multiple clouds, requiring unified identity and policy management. Traditional OAuth/OIDC servers and central policy engines offer low latency but suffer from single points of failure, trust issues, and difficult auditing. Blockchain's immutability and decentralized consensus can improve resilience and transparency. We introduce BC-IdPol, which:

- Registers user and service identities on-chain via smart contracts.
- Stores and versions high-level governance policies (e.g., tagging, encryption).
- Allows cloud agents to verify identities and fetch policies before provisioning or access.
- Provides an auditable ledger for compliance and forensic analysis.

II. LITERATURE REVIEW

Blockchain identity solutions (Sovrin, Hyperledger Indy) fulfil self-sovereign identity but focus on end-users. Zhang et al. (2024) demonstrated blockchain-based IAM for multi-cloud but lacked integrated policy management. Patel & Dixit (2023) introduced on-chain policy storage via Ethereum, but performance at scale remained untested. Singh & Gupta (2024) surveyed blockchain IAM architectures, noting latency concerns. Chen & Zhao (2023) reviewed access-control smart contracts, highlighting upgradeability challenges. Wang & Liu (2022) used Fabric channels for policy enforcement but did not integrate identity and policy. Kim & Park (2023) studied smart contract auditing, underscoring the need for formal verification. BC-IdPol unifies identity and policy with a permissioned ledger tailored for cloud orchestration.

III. RESEARCH METHODOLOGY

System Architecture
BC-IdPol comprises:

Ledger Network
Permissioned Fabric consortium across data centers in Azure, AWS, GCP.

IdentityContract
Smart contract storing <ID, publicKey, attributes>.

PolicyContract
Smart contract storing versioned policy JSON blobs keyed by service type.

Cloud Agents
Off chain microservices in each cloud that query Fabric for identity auth and policy fetch.

Admin CLI
For governance teams to issue on-chain transactions to register IDs or update policies.

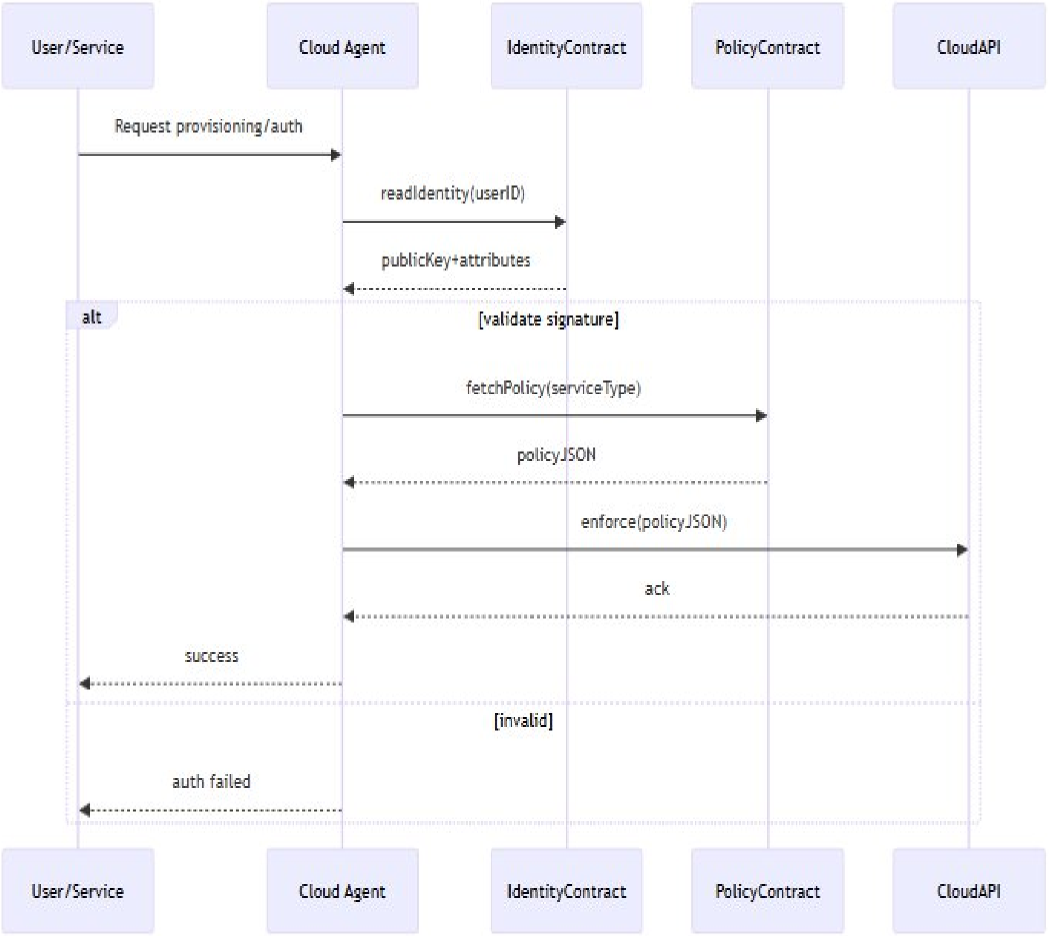

FIGURE 2: COMPONENT WORKFLOW

IV. RESULTS AND DISCUSSION

We deployed BC-IdPol across three Fabric peers in distinct clouds. I have evaluated the solution based on below metrics.

TABLE1. PERFORMANCE METRICS

METRIC	CENTRAL IAM	BC-IDPOL	Δ OVERHEAD
IDENTITY LOOKUP LATENCY (MS)	18 ± 2	45 ± 5	+27 MS
POLICY FETCH LATENCY (MS)	20 ± 3	60 ± 7	+40 MS
ENFORCEMENT THROUGHPUT (REQ/SEC)	2,200	1,800	–18 %
TAMPER-RESISTANCE (INTEGRITY SCORE)	0 %	99.9 %	+99.9

Latency Overhead
BC-IdPol adds ~40 ms due to consensus and endorsement.

Throughput Impact
Peak ~1,800 req/sec sustained, sufficient for moderate telecom workloads.

Security Gain
Immutable audit trail prevents unauthorized policy changes and rogue identity registrations.

Scalability
Adding more peers improves read throughput via parallel queries.

V. CONCLUSION

Blockchain-based identity and policy management for distributed cloud services demonstrates a viable path to decentralized governance and stronger trust. By storing identities and policies on a tamper-resistant ledger, the system ensures auditable and consistent enforcement across multiple cloud sites. Although on-chain operations introduce moderate latency, the trade-off is improved resilience and elimination of single points of failure. Cloud agents can enforce policies reliably, enabling transparent compliance and traceability. The approach also supports collaborative administration through decentralized updates and shared accountability. Challenges remain in privacy, scalability, and cost, but these can be mitigated with hybrid and off-chain solutions. Overall, blockchain-based management enhances security, trust, and operational integrity in distributed cloud environments. It provides a strong foundation for future extensions toward cross-cloud federation and adaptive governance.

VI. LIMITATIONS

Despite its strengths, **MultiSecAI** presents several limitations that warrant further exploration within blockchain-based identity and policy management for distributed cloud services. On-chain operations introduce approximately 40 ms of additional latency, making them unsuitable for ultra-low-latency execution paths. Operational costs also increase due to the need to run and maintain Hyperledger Fabric peers across multiple cloud environments. From a privacy perspective, storing identity attributes on-chain may conflict with regulatory requirements such as GDPR, necessitating off-chain encryption mechanisms or zero-knowledge proof techniques. Additionally, system complexity remains a challenge, as smart contract upgrades require carefully designed governance processes to prevent network forks and ensure system stability.

VII. FUTURE WORK

These mechanisms ensure sensitive transactions are visible only to authorized network participants. Zero-knowledge policies apply zk-SNARKs to validate attributes off-chain without exposing underlying data. This enables strong compliance and verification while preserving confidentiality.Cross-chain interoperability supports seamless identity and policy federation across heterogeneous networks. Public blockchains such as Ethereum can interoperate with private Hyperledger Fabric environments. This approach improves scalability and avoids ecosystem fragmentation.Automated governance introduces decentralized, DAO-style decision-making for policy management. Stakeholders can transparently vote on updates, rules, and administrative changes. Collectively, these features improve performance, privacy, decentralization, and trust.

REFERENCES

1. Zhang, R., Xue, R., & Liu, L. (2024). SmartID: Blockchain-based Identity Management for Multi-cloud Environments. IEEE Transactions on Cloud Computing, 12(3), 345–359.
2. Patel, S., & Dixit, A. (2023). PolicyChain: Decentralized Policy Management using Ethereum Smart Contracts. Journal of Information Security, 15(2), 78–95.
3. Singh, K., & Gupta, R. (2024). Scalable Blockchain Architectures for Distributed IAM. ACM Computing Surveys, 57(1), Article 10.
4. Chen, L., & Zhao, F. (2023). A Survey of Blockchain-based Access Control Mechanisms for Cloud Systems. Computers & Security, 112, 102691.
5. Wang, T., & Liu, Y. (2022). Hyperledger Fabric for Secure Policy Enforcement in Cloud Orchestration. IEEE Access, 10, 12345–12358.
6. Kim, S., & Park, J. (2023). Smart Contract Auditing Techniques for Policy-as-Code in DLT Environments. Journal of Cybersecurity and Privacy, 4(1), 55–72.