Blockchain-Based Access Control for Security Measures

With an Observation in IoT Device Implementation

Author: Mario J. Montoya Torres
Advisor: Prof. Nelliud D. Torres Batista
CS Dept. – Master's in Computer Science - Cybersecurity

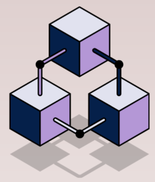
Abstract

This project explores the implementation of blockchain technology as an access control and identity management system to enhance security and data protection, especially in environments with increasing IoT device deployments. A proof-of-concept blockchain was developed using C++ and OpenSSL, focusing on trust-based access control for user authentication and authorization in a physical headquarters scenario. The study also discusses scalability challenges and future directions, including the integration of IPFS and DAG technologies to optimize storage and transaction efficiency in large-scale IoT deployments.

Introduction

Organizations face challenges in securing sensitive data and maintaining compliance with growing IoT device deployments. Blockchain offers a decentralized, cryptographically secure solution for access control and identity management. The project developed a prototype blockchain to analyze use cases, design considerations, and scalability challenges.

Relevant Work



Blockchain Fundamentals:

- Data structure of chained blocks, cryptographic security, and distributed ledgers.
- Consensus algorithms ensure ledger authenticity across nodes.

Access Control Models:

- **Transaction-Based (BAC):** Uses blockchain for secure, auditable access permission transactions.
- **Smart Contract-Based (SC-BAC):** Automates access control with programmable rules and policy enforcement.
- **Trust-Based Access Control:** Relies on digital signatures and certificates for user verification and dynamic trust assessment.

Methodology

Prototype Development:

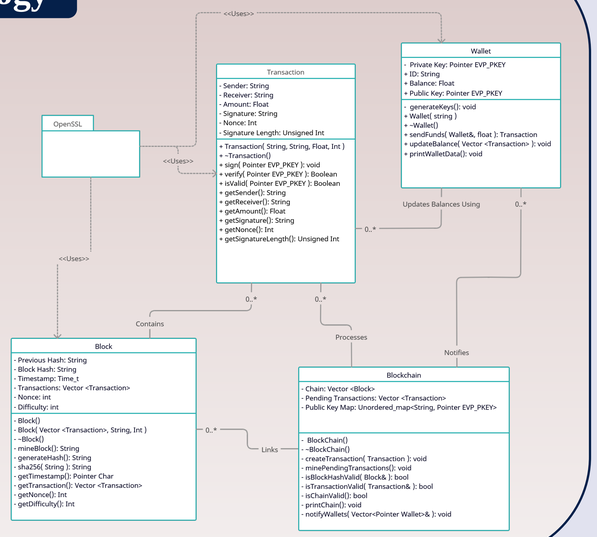
- Implemented in C++ with the OpenSSL library for cryptographic key management and block and transaction hashing for the blockchain.
- Adapted open-source blockchain code for authentication and policy management.

IoT Integration:

- Each IoT device maintains a copy of the ledger and is expected to have the resources available to do so, as well as manage computational overhead for authentication tasks.
- A peer-to-peer network must be present to ensure consensus and auditability.

Access Control Mechanisms:

- Flexible policy assignment (transaction-based, smart contract-based, and trust-based are options available to developers).
- Digital identities use particular user data and cryptographic verification for secure access.



Key Observations

Security:

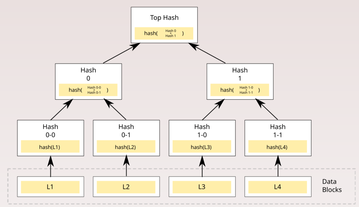
- Decentralized ledgers prevent single points of failure.
- Tamper-resistant records ensure data integrity and auditability.

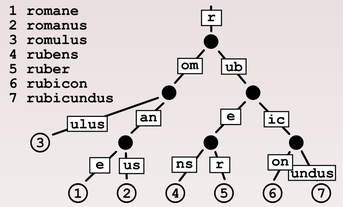
Scalability:

- High transaction volume can cause computational overhead.
- Merkle Trees and Patricia Tries are recommended for efficient transaction management.

Trust-Based Control:

- Dynamic trust evaluation using certificates, reputation, and transaction history.
- Enables fine-grained, auditable access for physical and logical resources.





Challenges and Future Directions

Scalability:

- Integrating Interplanetary File System (IPFS) and Dynamic Access Graph (DAG) technology for distributed storage and improved efficiency.

Usability:

- Balancing security with ease of deployment in resource-constrained IoT environments.

Further Research:

- Exploring multi-layer and judge-like contract architectures like smart contracts for dynamic policy enforcement and arrangements.

Conclusion

Blockchain-based access control systems offer robust, decentralized, and auditable solutions for IoT security. Trust-based models, leveraging cryptographic identity and dynamic trust assessment, provide a promising approach for scalable and secure access management in distributed environments. Current findings also highlight how a blockchain's architectural constraints can impact performance and efficiency in real-world deployments.

Acknowledgements

Student Contact:
Mario J. Montoya Torres #107156
Master's in Computer Science – Cybersecurity
Polytechnic University of Puerto Rico
Montoya_107156@students.pupr.edu

Mentor & Advisor:
Prof. Nelliud D. Torres Batista
neitorres@pupr.edu

Article Revision by:
Dra. Denisse M. Cobian Quiñones
dcobianquinones@pupr.edu

References

i. Y Zhu, F Xu, "Application Research on Blockchain-Based Access Control." at *2021 2nd Int. Conf. on Comput. Sci. and Manage. Technol. (ICCSMT)*, Shanghai, China. Nov. 13, 2021. [Online Library]. Available: https://ieeexplore.ieee.org/document/9786969. [Accessed: November 15, 2024].

ii. A. Quaddah, A. Ouahman, A. Elkalam. "Fairness: A New Blockchain-based Access Control Framework for The Internet of Things." in *Secur. and Commun. Netw. LLC, ResearchGate*, February 02, 2017. [Online Publication]. Available: https://www.researchgate.net/publication/313847688_FairAccess_a_new_Blockchain-based_access_control_framework_for_the_Internet_of_Things_FairAccess_a_new_access_control_framework_for_IoT. [Accessed: November 15, 2024].

iii. Y. Zhang, A. Memariani, N. Bidikar. "A Review on Blockchain-based Access Control Models in IoT Applications." at *IEEE 16th Int. Conf. Paper*, Singapore. October 9-11, 2020. [Online Library]. Available: https://ieeexplore.ieee.org/document/9264499. [Accessed: November 17, 2024].

iv. S. Nakamoto. "Bitcoin: A peer-to-peer Electronic Cash System" *White paper*, October 31, 2008. [Online Article]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: November 15, 2024].

v. Z. Miao, C. Ye*, P. Yang, Y. Chen, Y. Chen. "Blockchain-based Electronic Evidence Storage and Efficiency Optimization" at *2022 6th Int. Conf. on Cryptography, Secur. and Privacy (CSP)*, Tianjin, China, January 14-16, 2022. [Online Library]. Available: https://ieeexplore.ieee.org/document/9845257. [Accessed: February 20, 2025].

vi. OpenSSL Corp. Apr. 8, 2025. "OpenSSL Library", in GitHub Repository. [Online]. Available: https://github.com/openssl/openssl/tree/openssl-3.5.0. [Accessed: December 10th, 2024].