論文内容の要旨

申請者氏名　　WIRAATMAJA CHRISTOPHER

In this dissertation, we explore various approaches to enhancing the security, privacy, and scalability of blockchain-based access control systems in the Internet of Things (IoT) environment. In our first work, we propose a layered Blockchain-Based Attribute-Based Access Control (ABAC) architecture that incorporates a blockchain oracle layer and a decentralized storage layer to achieve cost efficiency. Specifically, we offload access control metadata to the decentralized storage layer and bridge the two layers using the blockchain oracle layer. Experimental results demonstrate significant improvements in gas cost efficiency compared to similar architectures, while preserving robustness and auditability due to the previous design.

Starting from our second work, we address the privacy concern of the previous design by introducing zero-knowledge set-membership proofs into a blockchain-based authentication scheme. To ensure the security guarantee of the previous approach, we propose zero-knowledge named proof, a stateless replay attack prevention strategy that ensures the user's anonymity against malicious administrators in a scalable manner. This approach enables users to delegate authentication to an anonymous agent, which carries authentication proofs that can be verified by administrators through set-membership proofs. We evaluate the proposed scheme's scalability, as well as its time and monetary costs, under both ideal and realistic environments, demonstrating its practicality. Furthermore, we extend this framework to support a third-party authorization mechanism, highlighting its real-world applicability.

Finally, in our third contribution, we leverage the Matrix Lookup Argument (MLA), a recent advancement in zero-knowledge proofs, to extend our previous design into a Blockchain-Based ABAC scheme, the gold standard for access control in IoT ecosystems. By representing access control metadata as matrices and utilizing the MLA for set-membership verification, our scheme enables users to authenticate themselves anonymously while adhering to access policies. We implement our work to get concrete performance and investigate the cost profile of our proposal. Our experimental results show that this approach achieves orders-of-magnitude improvements in proving time, exceeding 1000x for complex policies, compared to previous techniques. This makes the proposed scheme particularly suitable for resource-constrained IoT devices.

論文審査結果の要旨

申請者氏名　　WIRAATMAJA CHRISTOPHER

令和6年12月19日に開催した公聴会の結果を参考に令和7年2月7日に博士論文の審査を行った. 以下の通り, 本博士論文は, 提案者が独立した研究者として研究活動を続けていくための十分な素養を備えていることを示すものと認める.

Wiraatmaja Christopher君は, 本博士論文において, ブロック・チェーンを基にした大規模IoTネットワーク向けアクセス制御の主要件であるセキュリティ・プライバシー保護・拡張性を強化するアプローチとして, (1)オラクルベースのオンチェーン・オフチェーン・ハイブリッド型属性ベース・アクセス制御 (Attribute-Based Access Control: ABAC), (2)ゼロ知識証明を用いたプライバシー保護方式, (3)ゼロ知識証明を組み込んだプライバシー保護型ABAC, について, 方式設計と計算機シミュレーションによる定量的評価を行なっている. 本論文の貢献は以下のようにまとめることができる.

1. 大規模IoTネットワークを利用する莫大な数のユーザ情報をブロック・チェーン上で記録・管理することは高コストとなることが知られている. ユーザ情報の記録をブロック・チェーン外で管理する手法として, ブロック・チェーン・レイヤ, オラクル・レイヤ, ストレージ・レイヤの三層構造を持つABAC方式を提案し, IoT向けブロック・チェーン・フレームワークであるIOTAを用いた実装による計算機実験を通じてアクセス制御にかかる処理時間と発生コストについて定量的な評価を行い, 提案方式の優位性と有効性を確認した.

2. 従来の無効化 (nullfier) 技術を用いたリプレイ攻撃防止策はスマートコントラクト内にデータを格納する必要があり, 高コストの一因となっていた. ここでは低コスト化と高スケーラビリティを同時に実現する認証方式として, ゼロ知識証明の一手法であるゼロ知識集合メンバーシップ証明を用いた匿名認証方式zkNamedProof を提案した. 提案方式は認証リクエストを特定のエージェントに委任することでリプレイ攻撃を防ぎつつ, 同時に匿名性を確保しており, 高い有用性が認められる.

3. zkNamedProof のセキュリティ強度について, 暗号理論を基にした定式化を通じて攻撃耐性を理論的に証明するとともに, 計算機実験を通じて証明処理にかかる処理時間と発生コストを定量的に精査し, 提案方式が低コスト化と高スケーラビリティの両方を同時に実現していることを確認した. また, zkNamedProofに委任エージェントの属性確認を機能拡張として追加することで, サードパーティによる認証方式に対してリプレイ攻撃に耐性を持たせられることを示した.

4. CP-zkSNARKフレームワークを活用して行列ルックアップ証明を導入したモジュール型ABAC方式を提案した. 行列ルックアップ証明はゼロ知識証明を応用して行列内の要素の存在性を証明する手法であり, 行列ルックアップ証明を提供するLocq技術を組み込んだABACを開発するとともに, 計算機実験を通じてアクセス制御の通信コストおよび証明検証コストの低減化が実現できていることを定量的に確認した.

提案された二つのブロック・チェーン・ベースのアクセス制御方式はいずれもセキュリティ・プライバシー・拡張性の三要素の高度化を目指した方式であり, ゼロ知識証明を活用した認証方式では攻撃耐性を暗号理論に基づいて厳密に証明するとともに, 計算機実験を通して低処理遅延と低コストの達成が確認されており, 今後の大規模IoTネットワークのセキュリティ保証のための基盤技術として有用性が高く, 計算機科学と情報工学の両分野に対する貢献に加えて実学的観点からも高い意義が認められる. よって, 本論文は, 博士(理学)の学位論文として価値あるものと認める.