Strategic Opportunities for Blockchain Authentication in Cloud Computing

Connor Ireland

10/15/2019

University of District of Columbia, SEAS

Girma’s Responses:

Based on the title of the paper "Strategic Opportunities for Blockchain Authentication in Cloud Computing" , I strongly advise you with the following feedback that can give you a clear directions moving forward.

[1] Current Cloud authentication issues that you have researched about.

RELEVANT SOURCES:

**Survey on Access Control Issues in Cloud Computing**

**R Charanya, M Aramudhan**

*Please note that this paper is very poorly written! But it has useful lists and tables that make further research easy.*

Organized by AC systems:

RBAC define, describe flaw(s)

IBAC define, describe flaw(s)

ABAC define, describe flaw(s)

Ciphertext policy based attributes based Encryption CP-ABE, define, describe flaw(s)

hierarchical identity based encryption(HIBE) , hierarchical identity based encryption define, describe flaw(s)

Hierarchical attribute set based Encryption HASBE define, describe flaw(s)

Multiauthority define, describe flaw(s)

[2] Try to point out the major existing authentication issues. I am strongly advising you to discuss how these issues could not be solved and which existing methodologies were used or recommended.

RELEVANT SOURCE:

**User Authentication Issues In Cloud Computing**

**Mrs. S.M.Barhate1, Dr.M.P.Dhore**

[3] Explain why and how the Blockchain authentication is the viable option according to your approach.

*Break it down into the two big subdomains*

A. Loss of transparency and control over the data.

B. Lack of trust and dependence on cloud provider

[4] Please discuss which algorithim (Methodology) you are planning to introduce to support your research.

RELEVANT SOURCES:

**A Blockchain-Based Access Control System for Cloud Storage**

**Ilya Sukhodolskiy, Sergey Zapechnikov**

[5] Discuss your research result and recommendation.

[6] Please update the abstract section by mentioning first the current cloud authentication issues and how the problem is affecting both the cloud service providers and especially the clients. Then, briefly discuss the objectives of your research paper, i.e., how your approach using those strategic opportunities of Block chain authentication could help solving the cloud authentication problems.

Thanks and would like to commend the idea you are trying to explore.

`

***Abstract – There exist potential opportunities in distributed computing for trustless authentication on block-chains. Cloud computing customers may benefit from such arrangements if they wish to offload their access control functions. The following will serve as a guide for strategic planners who are considering migrating access control to block-chain applications.***

1. ***Introduction***
2. *Block chain*
3. *Cloud Access Control*
4. ***Literature Review***
5. ***Methods***
6. *Past work in this field*

*existence of RBAV1*

1. *Current deficiency in this field*
2. ***Results***
3. *Strengths, weaknesses*
4. *Opportunities, threats*

*weaknesses in authentication, current solutions which are not entirely servicable, proving (or disproving!) a real need for this*

1. ***Discussion***
2. *Use Cases*
3. *Guide for implementation*
4. ***References***

Report on Post-Quantum Cryptography

<https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals’

# <https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals>

# Bitcoin and quantum computing

<https://arxiv.org/abs/1711.04235>

# QMA

<https://en.wikipedia.org/wiki/QMA>

A Novel Attribute-Based Access Control

Scheme Using Blockchain for IoT

A Blockchain-Based Access Control System for

Cloud Storage

An Access Control Model and Its Application in

Blockchain

The model uses the ciphertext

policy attribute based encryption (CP-ABE) idea and trust

evaluation method to embed a trust threshold for the role.

A blockchain based approach for the

definition of auditable Access Control systems 24 pp

Decentralizing Privacy: Using Blockchain to Protect

Personal Data

Distributed Access Control with Blockchain

https://medium.com/talo-protocol/how-to-secure-sensitive-data-on-an-ethereum-smart-contract-77f21c2b49f5

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-712.md

Survey on Access Control Issues in Cloud Computing

# 5 Intractable Problems Quantum Computing Will Solve

<https://interestingengineering.com/5-intractable-problems-quantum-computing-will-solve>

Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?

<https://cr.yp.to/hash/collisioncost-20090517.pdf>

# Why Will Quantum Computers be Slow?

<https://algassert.com/post/1800>

### Quantum Supremacy Using a Programmable Superconducting Processor

<http://www.spaceref.com/news/viewsr.html?pid=52862>

[Scott’s Supreme Quantum Supremacy FAQ!](https://www.scottaaronson.com/blog/?p=4317)

https://www.scottaaronson.com/blog/?p=4317