November 12, 2018

A Homotopy-Theoretic Method for the Purpose of Intelligent Cloud Authorization

Lei Liu

A HOMOTOPY-THEORETIC METHOD FOR THE PURPOSE OF INTELLIGENT CLOUD AUTHORIZATION

Introduction:

The present disclosure provides systems and methods for intelligent cloud authorization. At present, cloud authorization is done without intelligence, and there is no known intelligent cloud authorization being proposed. The present disclosure aims to develop standardized intelligent cloud authorization APIs and performance metrics. In particular, the present disclosure establishes a theoretical foundation, standard framework, an original inference-learn-deny model, and homotopy analytics for intelligent cloud authorization. In this way, the present disclosure can enhance cloud identity access management standards.

Summary:

In general, cloud authorization faces several practical difficulties. For example, the characteristics of distributed computing in terms of service availability, reliability, scalability, and manageability can reduce the strength of cloud authorization. Any changes in services, resources, or actions; updates to roles, or role assignments; deletions and/or purging of identities; reclassifications; and authorization migrations require homotopy-based authorizations. As another example, penetrated identities or internal attacks can cause false negative authorizations (FNAs). As another example, failure updates, error retries, quota thresholds, service time of synchronous processing, queuing latency, and scheduled flume batch updates can cause both FNAs and false-positive denials (FPDs). As another example, weakness and errors of existing authorization rules, missing authorization rules, rule conflicts, and unknown authorization rules can cause uncertainty of authorization.

The present disclosure provides for an original and unique theoretical foundation, standard framework, model, and techniques to develop intelligent cloud authorization. The present disclosure provides for an original treatment to cloud authorization by topos generalization. The present disclosure sets up the theoretical foundation, develops the standard framework, and derives an inference-learn-deny model for intelligent cloud authorization. The present disclosure reinforces that topoi is an alternative universe in which homotopy analytics for intelligent cloud authorization is developed. The present disclosure develops the internal homotopy techniques of intelligent cloud authorization, and unifies intelligent cloud authorization with the standard construction and formalizes synthetics of authorization as univalence and a scheme of inductive types. The present disclosure models the corresponding semantics of intelligent cloud authorization as Kan complex and a cell monad with parameters. The standardization derives two (co)monadic APIs for intelligent cloud authorization.

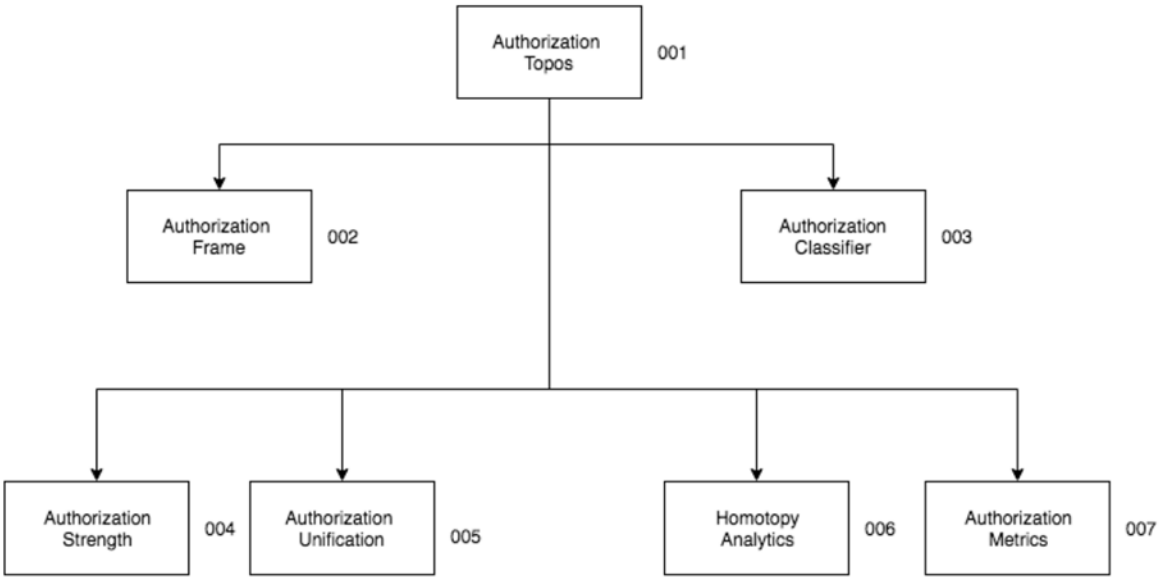
The present disclosure characterizes intelligent cloud authorization in two different ways. As a first characterization, the present disclosure develops the authorization frame by constructing a weak tree and an appropriate normalization procedure to encode minimal information by an n-graph for cloud authorization. As a second characterization, the present disclosure develops an artificial intelligence (AI) procedure to construct the authorization classifier in presence of uncertainty and additional information. The authorization frame and the authorization classifier are used as the topos for intelligent cloud authorization. The present disclosure shows that classical geometric properties are reflected in the internal homotopy of authorization. The present disclosure also develops the homotopy dimension as the strength of intelligent cloud authorization measures. The present disclosure selects the public metrics as authorization metrics. The public metrics can include, for example, precision and sensitivity of

authorization, a combined *F* score, authorization false rate, and time to authorize from a dual notion locale.

The present disclosure addresses the practical difficulties of cloud authorization and provides several advantages over cloud authorization that is done without intelligence. For example, the present disclosure standardizes intelligent cloud authorization in terms of APIs, performance metrics, and strength of measures, and defines intelligent cloud authorization as the authorization frame and classifier. In this way, the present disclosure can enable intelligent cloud authorization that can handle penetrated attacks, internal attacks, rule errors, missing rules, unknown rules, conflicts, etc.; false positive denials and false negative authorizations due to service time, latency, and thresholds; and both delta and full updates at runtime and provisioning phases. Additionally, the present disclosure can enable intelligent cloud authorization in case of both minimal information and uncertainty or with additional information. The present disclosure enables intelligent cloud authorization that is built upon the original theoretical foundation, standard framework, and model with duality constructions.

The attached appendix provides further detail of the present disclosure, and examples that implement the developed framework of the intelligent cloud authorization frame and classifier as the inference-learn-deny model.

Drawings:


Authorization Topos
001
Authorization Frame
002
Authorization Classifier
003
Authorization Strength
004
Authorization Unification
005
Homotopy Analytics
006
Authorization Metrics
007

Abstract:

The present disclosure describes an original and unique theoretical foundation, standard framework, model, and techniques for intelligent cloud authorization. The present disclosure provides for an original treatment to cloud authorization by topos generalization. The present disclosure sets up the theoretical foundation, develops the standard framework, and derives an inference-learn-deny model for intelligent cloud authorization. The present disclosure reinforces that topoi is an alternative universe in which homotopy analytics for intelligent cloud authorization is developed. The standardization derives two (co)monadic APIs for intelligent cloud authorization. The present disclosure characterizes intelligent cloud authorization in two different ways. First, the present disclosure develops the authorization frame by constructing a weak tree and an appropriate normalization procedure to encode minimal information by an *n*-graph for cloud authorization. Second, the present disclosure develops an artificial intelligence (AI) procedure to construct the authorization classifier in presence of uncertainty and additional information. Keywords associated with the present disclosure include: intelligent cloud authorization; cloud identity access management standards; topos generalization; inference-learn-deny model; homotopy analytics; APIs for intelligent cloud authorization; authorization frame; authorization classifier.