Access control for on-demand provisioned cloud infrastructure services

Ngo, C.T.

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: http://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (http://dare.uva.nl)

Download date: 02 Dec 2018
Acronyms

AA  Attribute Authority.
ABAC Attribute-based Access Control.
ABE  Attribute-based Encryption.
ADF  Access Control Decision Function.
AEF  Access Control Enforcement Function.
AWS  Amazon Web Services.
BDD  Binary Decision Diagram.
CIM  Common Information Model.
CT  Combining Tree.
DAC  Discretionary Access Control.
DACI Dynamic Access Control Infrastructure.
DAG  directed acyclic graph.
FIA  Fine-grained Integration Algebra.
IaaS Infrastructure as a Service.
IAM  Identity and Access Management.
IDD  Interval Decision Diagram.
INDL Infrastructure and Network Description Language.
LIACL Logical Infrastructure Composition Layer.
MAC  Mandatory Access Control.
MIDD  Multi-datatype Interval Decision Diagram.
MT  Matching Tree.
MT-ABAC  Multi-tenant Attribute-based Access Control.
MT-RBAC  Multi-tenant Role-based Access Control.
MTBDD  Multi-Terminal Binary Decision Diagram.
MTIDD  Multi-Terminal Interval Decision Diagram.
NIST  US. National Institute of Standards and Technology.
PaaS  Platform as a Service.
PDP  Policy Decision Point.
PEP  Policy Enforcement Point.
PERMIS  PrivilEge and Role Management Infrastructure Standards.
PIP  Physical Infrastructure Provider.
RBAC  Role-based Access Control.
RDF  Resource Description Framework.
SaaS  Software as a Service.
SAML  Security Assertion Markup Language.
SLA  Service Level Agreement.
SWRL  Semantic Web Rule Language.
VI  Virtual Infrastructure.
VIO  Virtual Infrastructure Operator.
VIP  Virtual Infrastructure Provider.
VM  Virtual Machine.
VR  Virtual Resource.
X-MIDD  Multi-datatype Interval Decision Diagram for XACML.
XACML  eXtensible Access Control Markup Language.
XSD  XML Schema Definition.
Bibliography


98 BIBLIOGRAPHY


[56] GEANT project. 2010. URL: http://www.geant.net/.


[87] Redis key-value data store. 2013. URL: http://redis.io/.


Publications

Publications in peer-reviewed journals


Publications in peer-reviewed conference proceedings


Publication Authorship

Author contributions to the publications used in this thesis.

Chapter 2


  C.N. designed, implemented and performed the experiments. P.M. contributed the secure bootstrapping protocol section. Y.D. consulted the study and publication. C.d.L supervised the work.


  C.N. designed, implemented and performed the experiments. P.M. contributed the bootstrapping trust management section. Y.D. consulted the study and publication. C.d.L supervised the work.


  C.N. designed, implemented and performed the experiments. Y.D. and C.d.L supervised the work.

Chapter 3


  C.N. designed, implemented and performed the experiments. P.M. contributed the bootstrapping trust management section. Y.D. consulted the study and publication. C.d.L supervised the work.

C.N. designed, implemented and performed the experiments. Y.D. consulted the study and publication. C.d.L supervised the work.


C.N. designed, implemented and performed the experiments. Y.D. and C.d.L supervised the work.

Chapters 4 and 5


C.N. designed, implemented and performed the experiments. M.X.M consulted the study and publication. Y.D. and C.d.L supervised the work.


C.N. designed, implemented and performed the experiments. Y.D. and C.d.L supervised the work.
List of Figures

1.1 The NIST Cloud Computing conceptual reference model [9] . . . . 2
1.2 Scope of controls between provider and consumer in NIST cloud services [9] . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
1.3 GEYSERS reference model . . . . . . . . . . . . . . . . . . . . . . . 5
1.4 ISO 10181-3 access control framework [22] . . . . . . . . . . . . . 7
1.5 XACML 3.0 policy model [36] . . . . . . . . . . . . . . . . . . . . . 11

2.1 Overview of information model for cloud infrastructure resources . 22
2.2 Multi-tenant access control model for cloud infrastructure resources 24
2.3 An example of context relationships . . . . . . . . . . . . . . . . . . 29
2.4 Attribute-based policy model integration with INDL . . . . . . . . . 34
2.5 Defining policy template sample . . . . . . . . . . . . . . . . . . . . 35
2.6 A sample Boole-Shannon decision diagram . . . . . . . . . . . . . 37
2.7 X-MIDD representing authorization statements . . . . . . . . . . . 38
2.8 Dynamic Access Control Infrastructure using MT-ABAC model . . 41
2.9 Single cloud provider performance evaluation . . . . . . . . . . . . 44

3.1 An Intercloud scenario . . . . . . . . . . . . . . . . . . . . . . . . . 48
3.2 Exchanging tokens in Intercloud: grant token and access token . . 50

4.1 An example of the function decomposition . . . . . . . . . . . . . . 67
4.2 A decision diagram sample for the function decomposition . . . . . 68
4.3 Sample MIDDs of the Target elements . . . . . . . . . . . . . . . . . 69
4.4 MIDDs of the $R_0$ target expression . . . . . . . . . . . . . . . . . 74

5.1 X-MIDDs of rules $R_1$ and $R_2$ . . . . . . . . . . . . . . . . . . . . 81
5.2 X-MIDD represents the sample policy $P_0$ . . . . . . . . . . . . . . 81
5.3 Average evaluation response times . . . . . . . . . . . . . . . . . . . 86
5.4 Standard deviation of evaluation response times . . . . . . . . . . . 86
5.5 SNE-XACML micro-benchmarks . . . . . . . . . . . . . . . . . . . . . 87
5.6 SNE-XACML evaluation time fractions . . . . . . . . . . . . . . . . . 88
# List of Tables

1.1 Access control models comparisons ......................................... 8

2.1 Administrative commands for MT-ABAC system ........................... 32
2.2 DACI integration APIs ..................................................... 41
2.3 Tenant policy administration APIs ......................................... 42
2.4 VI Datasets ........................................................................... 43

4.1 XACML abstract syntax .......................................................... 60
4.2 XACML combining algorithms .................................................. 61
4.3 XACML evaluation values for elements: Match, AllOf, AnyOf, Target and Condition .......................................................... 61
4.4 XACML decision values for Rule, Policy and Policyset elements ... 61
4.5 XACML rule evaluation specification ........................................... 63
4.6 XACML Policy/Policyset evaluation specification ......................... 63

5.1 Sample Policy Datasets ........................................................... 85
Access control is an important part of information security. It aims to preserve the confidentiality, integrity and availability by restricting access to protected resources and information via authorization. Depending on specific designs of computer systems, different access control models and mechanisms have been introduced.

The evolution of Cloud Computing brings advantages to both customers and service providers to utilize and manage computing and network resources more efficiently with virtualization, service-oriented architecture technologies, and automated on-demand resource provisioning. However, these advantages come with challenges on how to securely and efficiently protect customer resources in cloud environments. Service providers need to provide elastic and flexible cloud resources to their large numbers of customers based on the multi-tenancy model while ensuring reliable isolation on shared infrastructures. Therefore, designing and integrating access control mechanisms into cloud resource management is not trivial. Although many approaches have been proposed, they still suffer some drawbacks. First, they lack flexibility and interoperability with information models from management systems of on-demand provisioned cloud resources. Second, their policies and access control mechanisms are either coarse-grained, or do not have sufficient performance for large-scale cloud deployments.

This thesis contributes to the mentioned research field by investigating requirements of the access control for cloud infrastructure systems composed of compute and networking components. Based on these findings we propose a flexible and efficient access control approach that not only protects distributed cloud resources but also takes into account cloud infrastructure topology and characteristics.

Our work contains the following contributions:

We introduce a multi-tenant access control system with fine-grained authorization for cloud service management. It supports integration with the information model of cloud infrastructure management for providers. The proposed solution allows customers to dynamically create access control service instances together with policy definitions constrained in a SLA (Service Level Agreement) while deploying provisioned clouds. The approach supports on-demand provisioning and rescaling of cloud resources. It can regenerate policies to reflect changes in resource model descriptions. For Intercloud scenarios with clouds across multiple providers, we propose the authorization token exchange approach to solve distributed, inter-domain authorization and security context management problems. It allows users to established dynamic, fine-grained trust relationships with the
chain of involved providers who may not have direct trust relations. The proposed solutions are implemented as a part of the GEYSERS project prototype and testbed. It demonstrates that our approach is flexible in supporting elastic resource scaling and re-planning scenarios. Experiments also prove that the performance of our prototype is acceptable for cloud providers with thousands of customers.

Moreover, to solve the bottleneck problems when using the XACML policy language in high performance authorization systems, we propose and implement a novel approach that includes modeling, analyzing and optimizing XACML policy elements. The proposed approach decomposes policies, aggregates and reduces the scattering of complex attribute criteria using interval processing mechanisms. It then constructs custom decision diagrams for XACML that increase efficiency of policy evaluation. We demonstrate our approach in our open source high performance policy evaluation engine developed for the XACML 3.0 standard. It not only achieves magnitudes of throughputs improvement comparing to previous work but also retains original XACML policy semantics and expressiveness.
Samenvatting

Toegangscontrole is een belangrijk onderdeel van de informatiebeveiliging. Het doel is om de vertrouwelijkheid, integriteit en beschikbaarheid te behouden door het.authoriseren van toegang tot beveiligde bronnen en informatie. Afhankelijk van specifieke eigenschappen van computersystemen zijn in het verleden verschillende toegangscontrole modellen en authorisatie mechanismen geïntroduceerd.


In deze dissertatie dragen we aan het genoemde gebied bij door onderzoek aan de eisen van de toegangscontrole voor cloud-infrastructuur. Wij stellen een flexibele en efficiënte toegangscontrole benadering voor dat niet alleen gedistribueerde cloud resources beschermt maar ook rekening houdt met cloud topologie en eigenschappen van de infrastructuur.

Ons werk bestaat uit de volgende bijdragen:

We introduceren een multi-provider toegangs controle systeem met fijnmazige authorisatie voor cloud service management. Dit systeem maakt integratie met het informatie model voor cloud beheer door aanbieders mogelijk. De voorgestelde oplossing stelt klanten in staat om controle op de toegang tot infrastructuur instanties dynamisch te creëren inclusief de policy definities gelimiteerd door de afgesproken SLA (Service Level Agreement) op het moment dat de cloud instantie actief gemaakt wordt. De aanpak ondersteunt het instant beschikbaar maken en herschalen van cloud instanties door regeneratie van policies als gevolg van veranderingen in de resource-model beschrijvingen. Voor Intercloud scenario’s met
clouds over meerdere aanbieders verspreid, stellen wij de token gebaseerde aut-
orisatie uitwisseling voor om gedistribueerde inter-domein autorisatie en veilighei-
dscontext problematiek op te lossen. Het stelt gebruikers in staat om dynamische,
fijnkorrelige vertrouwensrelaties op te zetten met de keten van betrokken providers,
die wellicht geen onderlinge vertrouwensrelaties hebben. De voorgestelde oplossin-
gen zijn geïmplementeerd als een onderdeel van het GEYSERS project prototype en
testbed. Hierbij is aangetoond dat onze aanpak flexibel is in de ondersteuning van
elastische cloud aanbiedingen en herplanning scenario’s. Experimenten toonden
ook aan dat de prestaties van onze prototype acceptabel werkt voor cloud providers
met duizenden klanten.

Daarenboven, om knelpunten op te lossen bij het gebruik van de XACML policy-
taal in hoge aantal transactie systemen, introduceren en implementeren wij een
nieuwe benadering die het modelleren, analyseren en optimaliseren van XACML
elementen omvat. De voorgestelde aanpak ontleedt policies, neemt aggregaties
en vermindert de verstrooiing van complexe XACML attribute criteria door ge-
bruikmaking van interval verwerking mechanismen. Via deze aanpak komen we
dan met voor de actuele situatie specifieke beslissing diagrammen voor XACML
die de efficiëntie van de policy evaluatie enorm verhogen. We presenteren een
implementatie van onze open source policy evaluator gebaseerd op de XACML
3.0-standaard. We tonen aan dat onze aanpak in een high performance policy
evaluatie module niet alleen enige orden van grootte performance verbetering geeft
 vergeleken met eerder werk, maar ook de originele XACML policy semantiek en
expressiviteit behoudt.
Acknowledgements

Pursuing the PhD is a long journey in my life. When writing these lines, I am please that my PhD is almost accomplished. Actually, it would not be possible without help of many people that encourage, help and guide me along the way.

I would like to thank my promoter, Prof. Cees de Laat, for accepting me as a PhD student into the System and Network Engineering group and the GEYSERS research project. I would like to express my deepest gratitude for your endless guidance, support and valuable insights into my research directions.

I am truly thankful for my supervisor, Dr. Yuri Demchenko, for his support, continuous guidance and encouragements throught out my PhD. You patiently guide me into the research field, created opportunities to participate and work with people in the field. Without you I cannot accomplish this journey.

A special thanks to Prof. Pieter Adriaans for your critical questions and constructive advice in the field of mathematical logic to improve my thesis. I cannot finish my thesis without your kind support.

I thank all my colleagues in our research group for their intellectual dicussions and comments on my work: Paola, Cosmin, Mattijs, Marc, Ralph, Wibi, Daniel, Zhiming, Jeroen, Peter, Hao, Karel, Naod, Chariklis, Rudolf, Guido, Arie, Adam, Mikolaj, Reggie, Spiros, Fahime, Merijn, Ana Maria, Ana Lucia, Miroslav, Souley and Gerben. It was my pleasure to work, drink, hang out and play sports with you during four years at UvA. I also thank for people helping me on my teaching assistant work: Jaap, Niels and Toto.

I also thank for people in the GEYSERS project that I work with: Joan A., Jordi, Ester and Sergi at i2CAT, Spain; Shuping and Eduard at Essex, UK; Florian and Philip at SAP, Switzerland; Giada and Nicola at Nextworks, Italy; Jens at IBBT, Belgium; Damian, Krzysztof, Lukasz and Artur at PSNC, Poland and many others in the project. I have a chance to work with you in an international setting, where I can learn many useful things.

A special thanks to my colleagues at Hippo for your flexibility and support when I need to take some time off for my thesis completion. I also thank Arthur for helping me translate the summary to Dutch language.

I am grateful for all of my Vietnamese friends in the Netherlands for their friendship and for the great time we had in the last five years, from playing football, photography, catan, hanging around, travels, etc. All of them make my PhD life balanced and colorful.

Above all, I would like to thank my family: my parents, my brother and my
sister-in-law for their love and constant support. Huge thanks, love and appreciation go to my wife Van who was always there with grace and generosity. Thank our little son Kien who makes my life full of emotions and joys.

Canh Ngo
Amsterdam, January 2016.