TRUSTED REASONING-ROLE-BASED ACCESS CONTROL FOR CLOUD COMPUTING ENVIRONMENT

ABDUL RAUF

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JANUARY 2019

To my loving father, mother and to my wife and adorable children.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to Allah, the Almighty, for providing me knowledge, guidance and patience to achieve this goal. I would like to express my deep and sincere gratitude to my research supervisor, **Prof. Dr. Abdul Hanan Abdullah,** for giving me the opportunity to do research and providing invaluable guidance throughout this research. It was a great privilege and honor to work and study under his guidance. It would have been very difficult to complete this research successfully without his suggestions and thoughts. UTM management is highly appreciated for providing research incentives during this program. The members of Pervasive Computing Research Group are appreciated for their intellectual discussion and input in this thesis.

I am extremely grateful to my parents for their love, prayers, care and sacrifices for educating and preparing me for my future. Especially, I wish to acknowledge my father, Abdul Sattar Awan as being the source of inspiration in my studies. I owe my deepest gratitude towards my wife for her eternal support and understanding of my goals and aspirations. Her infallible love and support has always been my strength. I am thankful to my children Suniya, Maryam and Zainab for giving me happiness during my studies.

I show profound appreciation to my friends Dr. Gadaffi Abdul Salam and Dr. Omparkash for the keen interest shown by them to complete this thesis, successfully. Moreover, I am obliged to my friend, Dr. Imran Baig, Dr. Abdul Muteen, Federal Urdu University Islamabad, Pakistan for extending his helping hand during my time of struggle. Finally, my thankfulness for all those who have supported me to complete the research work directly or indirectly.

ABSTRACT

Cloud computing has become the new standard in the fast-growing industry of information technology. This poses new challenges to the existing access control models, as the new computing paradigm is highly-distributed and multi-tenancy. The existing access control models are not strong enough due to unavailability of strong multiple relationships between user and resources. In addition, monitoring activities of users to protect the cloud resources is weak. In these contexts, malicious user must be identified for the protection of sensitive data and to limit the access of the user to the resources. This research developed an enhanced access control model for cloud computing, namely Trusted Reasoning-Role-Based Access Control for Cloud Computing Environment (TR^{2}BAC) model. The model consists of four components. The first component is a dimensional domain for strong multiple relations between resources and user management, whereas the second component is reason-based access mechanism to limit users access based on defined reasoning principle. The third component is the trust module that identifies trusted/malicious users, and the fourth component ensures secure data access that classifies and labels the data according to the level of its sensitivity. The resources are then secured accordingly. Simulation results revealed that the performance of the proposed model improved in comparison to the existing state of the art techniques in terms of throughput by 25% and Permission Grants results by 35%. In terms of user authorization, the access time improved by 95% of the total access time which is about 7.5 seconds. In conclusion, this research has developed an enhanced access control model for cloud computing environment that can be used to protect the privacy of users as well as cloud resources from inside and outside attacks.

ABSTRAK

Pengkomputeran awan telah menjadi piawaian baru dalam industri teknologi maklumat yang berkembang pesat. Ini menimbulkan cabaran baru kepada model kawalan akses yang sedia ada, kerana paradigma pengkomputeran yang baru sangat teragih dan berbilang sewaan. Model kawalan akses yang sedia ada tidak cukup teguh disebabkan oleh ketiadaan hubungan berganda yang kuat antara pengguna dan sumber. Di samping itu, aktiviti pemantauan pengguna untuk melindungi sumber awan adalah lemah. Dalam konteks ini, pengguna yang berniat jahat mesti dikenal pasti untuk melindungi data sensitif dan untuk menghadkan akses pengguna ke sumber. Kajian ini membangunkan model kawalan akses yang dipertingkatkan untuk pengkomputeran awan, iaitu Kawalan Akses Berasaskan-Penaakulan-Peranan yang dipercayai (TR^{2}BAC). Model ini terdiri daripada empat komponen. Komponen pertama adalah domain dimensi untuk hubungan berganda yang kuat antara sumber dan pengurusan pengguna manakala komponen kedua adalah mekanisme akses berdasarkan taakulan untuk menghadkan akses pengguna berdasarkan prinsip penaakulan yang jelas. Komponen ketiga adalah modul amanah, yang mengenal pasti pengguna yang dipercayai / jahat dan komponen keempat memastikan akses data yang selamat yang mengklasifikasi dan melabel data mengikut tahap kepekaannya. Sumber-sumber ini kemudiannya dijamin keselamatan dengan sewajarnya. Hasil simulasi menjelaskan bahawa prestasi model yang dicadangkan lebih baik berbanding dengan teknik terkini sedia ada dari segi truput meningkat sebanyak 25% dan tahap meningkatkan Pemberian Kebenaran sebanyak 35%. Dari segi keizinan pengguna, masa akses meningkat sebanyak 95% dari jumlah masa akses iaitu kira-kira 7.5 saat. Sebagai kesimpulan, kajian ini telah membangunkan model kawalan akses yang dipertingkat untuk persekitaran pengkomputeran awan yang digunakan untuk melindungi kerahsiaan pengguna serta sumber awan dari serangan dalam dan luar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAC	-	Authority Authorization Centre
ABAC	-	Attribute Based Access Control
AC	-	Access Control
ARBAC	-	Attribute Role Based Access Control
C#	-	C-Sharp .Net Programming Language
CA	-	Certificate Authority
CAACM	-	Context Aware Access Control Model
CA-RBAC	-	Context Aware Role Based Access Control
CLA	-	Cyber Live Application
CRBAC	-	Contact Role Based Access Control
DAC	-	Discretionary Access Control
DD	-	Dimensional Domain
DDM	-	Dimensional Domain Manager
DRS	-	Dimensional Reasons
DRSR	-	Dimensional Reason Role
DSD	-	Dynamic Separation of Duties
EDSS	-	Environment Decision Support System
GLH	-	Generalized Location Hierarchy
IaaS	-	Infrastructure as a Service
IAM	-	Identity and Access Management
IdM	-	Identity Management
LDAP	-	Lightweight Directory Access Protocol
LL	-	Logical Location
MAC	-	Mandatory Access Control

NIST	-	National Institute of Standard and Technology
O	-	Object
Ont-RBAC	-	Ontology Role Based Access Control
OP	-	Operation
PA	-	Permission Assignment
PaaS	-	Platform as a Service
PL	-	Physical Location
PRBAC	-	Privacy Role Based Access Control
PS	-	Proof Statement
QA	-	Quality Assurance
QoS	-	Quality of Service
R	-	Role
R (PS)	-	Reliability of Proof Statement
RA	-	Role Assignment
RBAC	-	Role Based Access Control
RH	-	Role Hierarchy
S	-	Session
SaaS	-	Software as a Service
SAML	-	Security Assertion Markup Language
SBAC	-	Service Based Access Control
SLH	-	Specific Location Hierarchy
SOD	-	Separation of Duties
SRH	-	Super Role Hierarchy
SSD	-	Static Separation of Duties
TBAC	-	Trust Based Access Control
TM	-	Trust Management
TMAC	-	Team Mandatory Access Control
TRBAC	-	Task Role Based Access Control
U	-	User
UA	-	User Assignment
UBAC	-	Usage Based Access Control

UCON	-	Usage Control
XACML	-	Extensible Access Control Markup Language
XML	-	Extensible Markup Language

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cloud computing permits ubiquitous, convenient and on-demand network access to shared pool of configurable computing resources. The resources include open networks, servers, storage, applications, and services (Joshi *et al.*, 2014). Cloud computing has many advantages: Minimal management effort or interaction with service providers; and scalable, as it gives users unlimited processing and storage by providing broad network access. Cloud computing provides three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Garg *et al.*, 2013). There are four common cloud deployment models (Hsu *et al.*, 2014). The first is the public cloud model in which cloud services are delivered over the Internet through web applications and clients can easily access the services. The second is the private cloud in which the customers of specific enterprise only access the private enterprise's resources. Private cloud is implemented in a secure environment that is safeguarded by a firewall. The third is the community cloud in which community of clients use the cloud environment with mutually agreed protocols. Hybrid cloud is the fourth model which is the juxtaposition of public, private and/or community infrastructures.

Access control is critical to ensure security and privacy of a system in cloud computing environment. The traditional access control technology is not strong enough to cater to the security requirements in a dynamic cloud computing environment (Puthal *et al.*, 2015). An efficient strategy for effective and vulnerability-control access model is particularly significant to ensure security. Access control mechanism is also required, so that the data of users should be confidential, integrated and protected. The two security domains in the access control model are: the single domain - user access is based on traditional mechanism; and multiple domains- require role-based access control which changes dynamically, commensurate with interests of the entities within the cloud (Hogan *et al.*, 2011a).

The United State Government assigned the task to The National Institute of Standards and Technology (NIST) to make standards related to the adoption and development of cloud computing (Hogan *et al.*, 2011b). NIST recommended NIST-RBAC (National Institute of Standards and Technology – Role Based Access Control model, which consists of six basic components i.e. users, objects, operations, roles, session, and constraints (Liu *et al.*, 2011). The constraints in the NIST - RBAC are further divided into two categories: Dynamic Separation of Duty (DSD), and Static Separation of Duty (SSD). These components are used to form weak or strong relationships in terms of user-assignment, permission-assignment, role, user sessions, and role hierarchy. According to these relations, the relation among user and role is known as user assignment, whereas the relation among permission and role is called permission assignment. The subjects used in RBAC are the individual users who are linked with their respective roles. The RBAC mechanism involves the objects which are deployed via operations (e.g. data access operations) and referred to as resources of the system. NIST RBAC model (Ferraiolo *et al.*, 2001) is shown in Figure 1.1.

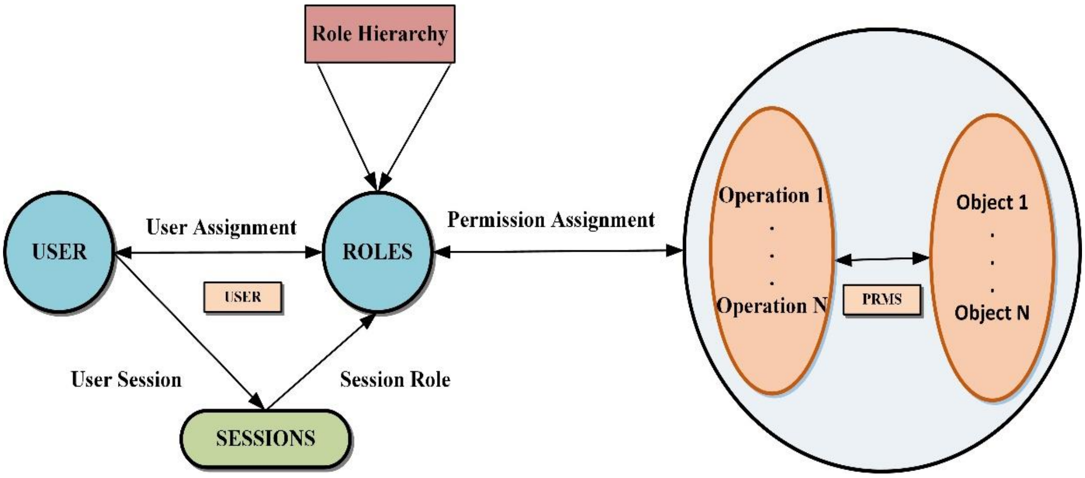

Figure 1.1 NIST Role Based Access Control Model (Ferraiolo *et al.*, 2001)

1.2 Access Control Policy

Access control policies are high-level requirements that specify how access is managed and who may access information under what conditions. Security models are formal presentations of security policy enforced by the system and are useful for proving theoretical limitations of a system. A system sets user attributes, which are authentication and authorization based on adapted policies, to control the access to services/resources. The user attributes are of two types, which are mutable and immutable. Patel *et al.* (2012) describe these attributes as dynamic during access operation, for example, spatial and usage state. Immutable attributes are static during access operation, for example, identity of user. Each domain has an attribute authority which screens the rights of the requesting user.

Access control policy in an organization is different from cloud computing environment, because cloud environment is highly distributed environment. Cloud computing access control policy requirements are different from traditional organization requirements. The cloud is comprised of cloud consumers and cloud service providers that have different access control requirements. Distributed virtualization, big-data processing, serviceability, traffic management, application security, access control, authentication are the main security issues in cloud computing service environment (Takabi *et al.*, 2010). Cloud services are Infrastructure as a Services (IaaS), Platform as a Services (PaaS) and Software as a Services (SaaS) (Pulier *et al.*, 2018), and these cloud computing services are distinguished by way of security policies because of differences in the allowed access right between service providers and users.

1.3 Problem Background

The Discretionary Access Control (DAC) by Li (2011) is a model in which the access control mechanism depends on the identity of subjects (users). DAC model employed in cloud system make it possible for the cloud system to become vulnerable to unauthorized users. Another access control model is Mandatory Access

Control (MAC) Osborn (1997), which depends on the classification of subjects (users) and objects (modules). MAC model protects itself from unauthorized users and objects by establishing a level of security vis-a-vis classification of its associated entities. The only downside of MAC and DAC models is that they lack flexible access control. The Role Based Access Control (RBAC) model presented (Ferraiolo *et al.*, 1999) depends solely on roles – roles are assigned to users and must be activated before accessing the required services. This model assigns roles to users ensuring secured access. The role assignment, authorization, and permission assignment are the predefined rules for RBAC.

In Li's RBAC model, access control depends on context technology, time constraints, and Authority Authorization Center (AAC) for providing authorization certificates (Li *et al.,* 2014). However, the limitation of this model is an incorrect measurement of trust level. However, the Cloud Optimized RBAC model proposed by Li *et al.* (2015) grants provision of diverse access permission to same user, and user can use multiple services securely. Distributed RBAC (Freudenthal *et al.*, 2002) uses a specific object-oriented technique for distributed system. However, it is unable to manage heterogeneity issues in distributed environment. Rizvi and Fong (2016) provide a solution to the same issue - typically persistent in all the variations of the RBAC model - associating semantic access control scheme. The limitation of their model is the inherent incapacity to deal with sensitive data in the complex cloud environment.

In order to deal with the complexity of the large cloud environment, Attribute Role Based Access Control (AR-ABAC) was presented by (Riad *et al.*, 2015). This mechanism was introduced with Extensible Access Control Markup Language by Rissanen (2013) to assure better security compared to previous RBAC models. In the Attribute Role Based Access Control (ARBAC) model, Authentications and Authorizations are attribute based. However, in AR-ABAC, the behavior of the user remains only partially controlled. The Usage Control (UCON) model by Xu *et al.* (2007), This model is based on the definitions of subjects and objects. Subjects can access the objects only according to their respective rights. Enforcement point module and the applications work independently but are based on rights to access.

Thus, UCON’s main feature is Attributed Mutability. However, its drawback is that it fails when the number of users increases. At the same time, UCON model for authorization occasionally performs the determination checks for user.

1.4 Problem Statement

The Role Based Access Control (RBAC) model is recommended by NIST for cloud computing environments. NIST-RBAC model has become the foundation of access control model for cloud computing. This model had many limitations and has been improved by different researchers. However, the NIST-RBAC model has no context-aware elements, and thus cannot provide dynamic access control for cloud computing environments. Context-aware means credential and spatial information of resources and users, which include session time, resources and user location, and user profiles. Dynamic access control - administrator controlled - implements access control permissions and constraint based on the organizational policy. Dynamic access control can manipulate the sensitivity of the resources, the role of the user, and the formation of the device that is used to access these resources.

Contract Role Based Access Control (C-RBAC) by Chen *et al.* (2013) presents cognitive RBAC mechanism for small heterogeneous networks in cloud computing. Despite that, it fails to prevent information leakages because it does not provide context determination for administrators or users. The set of location information is related to the different factors of cloud computing system (spatial state), which is not defined in C-RBAC. Cloud optimized RBAC by Younis *et al.* (2014) introduces the context based technology for secure access control in cloud computing environment. Nevertheless, this model does not cater to location constraints. Additionally, this model is unable to follow the principle of heterogeneity and is powerless to maintain security domains. The semantic RBAC model, also known as Service Based Access Control (SBAC) model (Tupakula *et al.*, 2009) is used for semantic relations among different entities in the cloud. In this model, the users need to remember separate credentials for each SaaS application. Despite this, it is prone to a higher level of security risk due to the transmission of user context information outside the enterprise. Team Mandatory Access Control (TMAC) (Georgiadis *et al.*, 2001) and Privacy Role-Based Access Control (PRBAC) (Dafa-Alla *et al.*, 2005) deal with privacy of the users but fail to deal with intruders.

Security services are provided to cloud users with the support of context-aware security manager in Context-Aware Role-Based Access Control Model (CA-RBAC) suggested by (Zhou *et al.*, 2013). However, the author acknowledged that the trust level platform loses its credibility due to the integrity breach. Therefore, it needs integrity assurance in the full life cycle of the system. In the Onto-ACM model presented by Choi *et al.* (2014), cloud environment can be secured by avoiding an illegal approach to access rights which ultimately safeguards access to resources. The limitations of this suggested model are that it stores the user's context-information in the database and takes more time to access the user information in queries as the number of users increases. At the same time, this model does not provide streamlined policy management. Reason-based use OWL engine in ontology, in modern database reason-based SQL command is used to implement least privilege principle (Beavin *et al.*, 2000).

Login information to access highly distributed cloud environment has proved insufficient. Thus, Trust Management (TM) model (Ray and Ray, 2014) categorizes concepts of trust relations between identity and behavior. Identity-based trust is responsible for ensuring the uniqueness of an individual and allowing authorized access to resources. Moreover, trust reasoning model presented by Sun *et al.* (2017) can be categorized trust into direct trust and indirect trust. Direct trust creates direct relationships between multiple resources, whereas indirect trust builds relationships with the support of a third-party. However, neither category provides registration manager for user registration.

The Mutual Trust Based Access Control (MTBAC) model (Lin *et al.*, 2014) considers user’s trust behavior and credibility of cloud server for secure access to the resources. These concepts support identification-based users access to specific resources. However, this suggested model supports unidirectional data distribution which cannot withstand the complexity of the today's distributed systems. Ferronato *et al.* (2016) modify RBAC model by introducing Reference Ontology Framework, which depends upon permission policies for user role assignment. There is a need in the unsecured environment to utilize identity at each step to maintain security and rights to access resources.

1.5 Research Questions

Based on the discussion in problem background, the research questions can be formulated as follows:

i. How can a strong relationship between resources and users be built on cloud computing environments?

ii. How can reason-based access mechanisms among multiple resources and users for controlled access be defined?

iii. How can the behaviour of the user, both inside as well as outside, be monitored?

iv. How can the malicious cloud client be denied access to the critical data on cloud computing environments?

1.6 Research Aim and Objective

Access control model is used to provide secure access control in cloud computing environment. The use of enhanced access control model - based on role-based access control - can provide the solution for hybrid cloud computing environments. It provides secure access control for two types of services i.e. software as a service, and infrastructure as a service. This study proposes an access control model for users and resources, where users can define multiple relationships for multiple entities. In projected access control model, the critical data is protected, and it fulfills all the security requirements of cross domain and mutually trusted cloud computing environments.

The research objectives are:

i. To design and develop dimensional domains and define the spatial state for cloud computing environments to build a strong relationship among resources and users.

ii. To design and develop a mechanism for reason-based access control, helping the concerned organization in understanding user operations on objects.

iii. To design and develop trust module for monitoring the behaviour of users.

iv. To design and develop a mechanism for secure data access control via sensitivity-based categorization and labelling of data.

1.7 Research Contribution and Scope

To establish enhanced security through secure access control to cloud computing, this study develops and implements an access control model. It will ensure secure resources and effective user management. It also provides privileged authorization to the user without compromising the rights of the end users on cloud computing environments. Therefore, the Trusted Reasoning-Role-Based Access Control for Cloud Computing Environment (TR^{2}BAC) model is introduced to overcome the limitations discussed earlier. The main contribution of the research is to manage the resources and user in such a way that access control becomes more efficient. At the same time, access control mechanism is used to protect the privacy of users, as well as cloud resources, from inside and outside attacks. The scope of the study is as follows:

i. The proposed secure domain has the potential of establishing strong and secure role-based relationships between resources and users in cloud environments.

ii. The administrator must know the reasons (what and why) for a desire of the user to access data from multiple domains in the multi-tenancy cloud computing environment. This will provide a basis for creating user specific roles.

iii. The inherent complications in the role-based access control model can be reduced by classifying its users into classes or groups based on dynamic access control criteria.

iv. The trust module is used to identify users and provides protection against unauthorised user access to data.

v. The proposed model efficiently deals with manifold increase in number of users. It employs heterogeneity techniques.

vi. The trust module is used to monitor the behaviour of the user through imposing policies structured according to requirements of the concerned organization.

1.8 Organization of the Thesis

The organization of this research thesis is as follows:

Chapter 2 presents the extensive literature review of the area of the study, which is access level security for cloud computing environments, and discusses various existing access control models in a cloud computing environment. Chapter 3 discusses the research methodology, including the research framework that will be used in this research for the design and development of proposed access control model. Chapter 4 presents and describes relevant information about the dimension domain. (How resources and user are managed in various regions of a cloud. It describes the method of reason-based access mechanism, context reasoning, and dimensional reasoning criteria). Chapter 5 includes a trust module for user behavior monitoring. (It discusses a new way to secure the data access and to protect data leakage in hybrid cloud environments). Chapter 6 presents and describes the relevant information on the simulation and results obtained using XACML and C#. The simulation also shows some comparative results obtained using cloudsim. Finally, Chapter 7 concludes the research work and provides possible future research directions.

REFERENCES

Acharya, S., and Siddappa, M. (2016). A novel method of designing and implementation of security challenges in data transmission and storage in cloud computing. *Int J Appl Eng Res, 11*(4), 2283-2286.

Ahn, G.-J., and Hu, H. (2007). *Towards realizing a formal RBAC model in real systems.* Paper presented at the Proceedings of the 12th ACM symposium on Access control models and technologies, 215-224.

Almorsy, M., Grundy, J., and Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Aluvalu, R., Kamliya, V., and Muddana, L. (2016). HASBE access control model with Secure Key Distribution and Efficient Domain Hierarchy for cloud computing. *International Journal of Electrical and Computer Engineering, 6*(2), 770.

Anderson, A. (2005). Core and hierarchical role based access control (RBAC) profile of XACML v2. 0. *OASIS Standard*, 2005.

Arora, S., Song, E., and Kim, Y. (2012). *Modified hierarchical privacy-aware role based access control model.* Paper presented at the Proceedings of the 2012 ACM Research in Applied Computation Symposium, 344-347.

Aziz, A. A., and Osman, S. (2016). *Review the Types of Access Control Models for Cloud Computing Environment.* Paper presented at the Proceedings of the Informatics Conference.

Beavin, T. A., Hoa, P., Lin, F.-L., and Tie, H. S. (2000). Executing complex SQL queries using index screening for conjunct or disjunct index operations: Google Patents.

Bhatti, R., Bertino, E., and Ghafoor, A. (2005). A trust-based context-aware access control model for web-services. *Distributed and Parallel Databases, 18*(1), 83-105.

Carniani, E., D'Arenzo, D., Lazouski, A., Martinelli, F., and Mori, P. (2016). Usage Control on Cloud systems. *Future Generation Computer Systems, 63*, 37-55.

Chen, H.-C. J., Violetta, M. A., and Yang, C.-Y. (2013). Contract RBAC in cloud computing. *The Journal of Supercomputing, 66*(2), 1111-1131.

Chen, S., Thilakanathan, D., Xu, D., Nepal, S., and Calvo, R. (2015). *Self protecting data sharing using generic policies.* Paper presented at the Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on, 1197-1200.

Chinn, S. J., and Madey, G. R. (1997). A framework for developing and evaluating expert systems for temporal business applications. *Expert Systems with Applications, 12*(3), 393-404.

Choi, C., Choi, J., and Kim, P. (2014a). Ontology-based access control model for security policy reasoning in cloud computing. *The Journal of Supercomputing, 67*(3), 711-722.

Choi, C., Choi, J., and Kim, P. (2014b). Ontology-based access control model for security policy reasoning in cloud computing. *Journal of SuperComputing, 67*(3).

Dafa-Alla, A. F., Kim, E. H., Ryu, K. H., and Heo, Y. J. (2005). *PRBAC: An extended role based access control for privacy preserving data mining.* Paper presented at the Computer and Information Science, 2005. Fourth Annual ACIS International Conference on, 68-73.

Danwei, C., Xiuli, H., and Xunyi, R. (2009). *Access control of cloud service based on ucon.* Paper presented at the IEEE International Conference on Cloud Computing, 559-564.

Das, P. K., Ghosh, D., Jagtap, P., Joshi, A., and Finin, T. (2016). Preserving User Privacy and Security in Context-Aware Mobile Platforms. *Mobile Application Development, Usability, and Security*, 166-193.

Das, V. V. (2008). *Architecture for Secure Knowledge Management over the Network.* Paper presented at the Information and Automation for Sustainability, 2008. ICIAFS 2008. 4th International Conference on, 361-365.

Di Pietro, R., Lombardi, F., and Signorini, M. (2016). Computing Technology for Trusted Cloud Security. *Cloud Computing Security: Foundations and Challenges*, 331.

Downs, D. D., Rub, J. R., Kung, K. C., and Jordan, C. S. (1985). *Issues in discretionary access control.* Paper presented at the Security and Privacy, 1985 IEEE Symposium on, 208-208.

Fadhel, A. B., Bianculli, D., and Briand, L. (2015). A comprehensive modeling framework for role-based access control policies. *Journal of Systems and Software, 107*, 110-126.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., and Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security, 13*(2), 113-170.

Ferraiolo, D., Chandramouli, R., Kuhn, R., and Hu, V. (2016). *Extensible access control markup language (XACML) and next generation access control (NGAC).* Paper presented at the Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control, 13-24.

Ferraiolo, D. F., Barkley, J. F., and Kuhn, D. R. (1999). A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security (TISSEC), 2*(1), 34-64.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC), 4*(3), 224-274.

Ferreira, A., Chadwick, D., Farinha, P., Correia, R., Zao, G., Chilro, R., et al. (2009). *How to securely break into RBAC: the BTG-RBAC model.* Paper presented at the Computer Security Applications Conference, 2009. ACSAC'09. Annual, 23-31.

Ferronato, A. C., Pires, F. R., and Bernardini, F. C. (2016). *A Model for Data Integration and Availability in Health Government Area.* Paper presented at the Proceedings of the XII Brazilian Symposium on Information Systems on Brazilian Symposium on Information Systems: Information Systems in the Cloud Computing Era-Volume 1, 17.

Freudenthal, E., Pesin, T., Port, L., Keenan, E., and Karamcheti, V. (2002). *dRBAC: distributed role-based access control for dynamic coalition environments.* Paper presented at the Distributed Computing Systems, 2002. Proceedings. 22nd International Conference on, 411-420.

Garg, S. K., Versteeg, S., and Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems, 29*(4), 1012-1023.

Georgiadis, C. K., Mavridis, I., Pangalos, G., and Thomas, R. K. (2001). *Flexible team-based access control using contexts.* Paper presented at the Proceedings of the sixth ACM symposium on Access control models and technologies, 21-27.

Ghazi, Y., Masood, R., Shibli, M. A., and Khurshid, S. (2016). Usage-Based Access Control for Cloud Applications. In *Innovative Solutions for Access Control Management* (pp. 197-223): IGI Global.

Habib, M. A., Mahmood, N., Shahid, M., Aftab, M. U., Ahmad, U., and Faisal, C. M. N. (2014). *Permission Based Implementation of Dynamic Separation of Duty (DSD) in Role Based Access Control (RBAC).* Paper presented at the Signal Processing and Communication Systems (ICSPCS), 2014 8th International Conference on, 1-10.

Habiba, U., Masood, R., Shibli, M. A., and Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling, 2*(1), 5.

Harmon, P., and Sawyer, B. (1990). *Creating expert systems for business and industry*: John Wiley & Sons, Inc.

Hendre, A., and Joshi, K. P. (2015). *A semantic approach to cloud security and compliance.* Paper presented at the Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, 1081-1084.

Hogan, M., Liu, F., Sokol, A., and Tong, J. (2011a). Nist cloud computing standards roadmap. *NIST Special Publication, 35*.

Hogan, M., Liu, F., Sokol, A., and Tong, J. (2011b). Nist cloud computing standards roadmap. *NIST Special Publication, 35*, 6-11.

Hosseinzadeh, S., Virtanen, S., Díaz-Rodríguez, N., and Lilius, J. (2016). *A semantic security framework and context-aware role-based access control ontology for smart spaces.* Paper presented at the Proceedings of the International Workshop on Semantic Big Data, 8.

Hsu, P.-F., Ray, S., and Li-Hsieh, Y.-Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management, 34*(4), 474-488.

Ibrahim, A. S., Hamlyn-Harris, J., and Grundy, J. (2016). Emerging security challenges of cloud virtual infrastructure. *arXiv preprint arXiv:1612.09059*.

Iwata, T. (2003). Comments on “On the security of XCBC, TMAC and OMAC” by Mitchell. *Comments to NIST, September, 19*.

Javanmardi, S., Amini, M., and Jalili, R. (2006). *An access control model for protecting semantic web resources.* Paper presented at the Web policy workshop.

Joshi, K. P., Yesha, Y., and Finin, T. (2014). Automating cloud services life cycle through semantic technologies. *IEEE Transactions on Services Computing, 7*(1), 109-122.

Kalloniatis, C., Mouratidis, H., and Islam, S. (2013). Evaluating cloud deployment scenarios based on security and privacy requirements. *Requirements Engineering, 18*(4), 299-319.

Khan, A. R. (2012). Access control in cloud computing environment. *ARPN Journal of Engineering and Applied Sciences, 7*(5), 613-615.

Klager, A. D., and Rhudy, R. L. (2015). System and method for transferring data between a user space and a kernel space in a server associated with a distributed network environment: Google Patents.

Lazouski, A., Mancini, G., Martinelli, F., and Mori, P. (2012). *Usage control in cloud systems.* Paper presented at the Internet Technology And Secured Transactions, 2012 International Conference for, 202-207.

Li, B., Tian, M., Zhang, Y., and Lv, S. (2014). Strategy of domain and cross-domain access control based on trust in cloud computing environment. In *Computer Engineering and Networking* (pp. 791-798): Springer.

Li, H., Wang, S., Tian, X., Wei, W., and Sun, C. (2015). *A survey of extended role-based access control in cloud computing.* Paper presented at the Proceedings of the 4th International Conference on Computer Engineering and Networks, 821-831.

Li, N. (2011). Discretionary access control. In *Encyclopedia of Cryptography and Security* (pp. 353-356): Springer.

Li, N., Mitchell, J. C., and Winsborough, W. H. (2002). *Design of a role-based trust-management framework.* Paper presented at the Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on, 114-130.

Lin, G., Wang, D., Bie, Y., and Lei, M. (2014). MTBAC: a mutual trust based access control model in cloud computing. *China Communications, 11*(4), 154-162.

Lindqvist, H. (2006). Mandatory access control. *Master's Thesis in Computing Science, Umea University, Department of Computing Science, SE-901, 87.*

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., et al. (2011). NIST cloud computing reference architecture. *NIST special publication, 500*(2011), 292.

Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J. (2016). Fine-grained two-factor access control for web-based cloud computing services. *IEEE Transactions on Information Forensics and Security, 11*(3), 484-497.

Lo, N. W., Yang, T. C., and Guo, M. H. (2015a). An Attribute-Role Based Access Control Mechanism for Multi-tenancy Cloud Environment. *Wireless Personal Communications*, 1-16.

Lo, N. W., Yang, T. C., and Guo, M. H. (2015b). An attribute-role based access control mechanism for multi-tenancy cloud environment. *Wireless Personal Communications, 84*(3), 2119-2134.

Lorch, M., Proctor, S., Lepro, R., Kafura, D., and Shah, S. (2003). *First experiences using XACML for access control in distributed systems.* Paper presented at the Proceedings of the 2003 ACM workshop on XML security, 25-37.

Matthies, M., Giupponi, C., and Ostendorf, B. (2007). Environmental decision support systems: Current issues, methods and tools. *Environmental Modelling & Software, 22*(2), 123-127.

Mushtaq, F., and Aranganathan, S. (2015). Secure Access Control Requirement Analysis in Cloud Computing. *International Journal, 3*(3).

Naik, N., and Jenkins, P. (2016). *A secure mobile cloud identity: Criteria for effective identity and access management standards.* Paper presented at the Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2016 4th IEEE International Conference on, 89-90.

Narayanan, H. A. J., and Güneş, M. H. (2011a). *Ensuring access control in cloud provisioned healthcare systems.* Paper presented at the Consumer Communications and Networking Conference (CCNC), 2011 IEEE, 247-251.

Narayanan, H. A. J., and Güneş, M. H. (2011b). *Ensuring access control in cloud provisioned healthcare systems.* Paper presented at the 2011 IEEE Consumer Communications and Networking Conference (CCNC), 247-251.

Nasim, R., and Buchegger, S. (2014). *XACML-based access control for decentralized online social networks.* Paper presented at the Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 671-676.

Nemati, H. (2012). *Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies*: IGI Global.

Oh, S., and Park, S. (2000). *Task-role based access control (T-RBAC): An improved access control model for enterprise environment.* Paper presented at the Database and Expert Systems Applications, 264-273.

Osborn, S. (1997). *Mandatory access control and role-based access control revisited.* Paper presented at the Proceedings of the second ACM workshop on Role-based access control, 31-40.

Patel, S. C., Umrao, L. S., and Singh, R. S. Policy-based Access Control in Cloud Computing.

Pei, X., Yu, H., and Fan, G. (2015). *Achieving Efficient Access Control via XACML Policy in Cloud Computing.* Paper presented at the SEKE, 110-115.

Pulier, E., Martinez, F., and Hill, D. C. (2018). System and method for a cloud computing abstraction layer: Google Patents.

Puthal, D., Sahoo, B., Mishra, S., and Swain, S. (2015). *Cloud computing features, issues, and challenges: a big picture.* Paper presented at the Computational Intelligence and Networks (CINE), 2015 International Conference on, 116-123.

Ray, I., and Ray, I. (2014). Trust-based access control for secure cloud computing. In *High Performance Cloud Auditing and Applications* (pp. 189-213): Springer.

Riad, K., Yan, Z., Hu, H., and Ahn, G.-J. (2015). *AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing.* Paper presented at the Collaboration and Internet Computing (CIC), 2015 IEEE Conference on, 28-35.

Rissanen, E. (2013). extensible access control markup language (xacml) version 3.0. *OASIS standard, 22*.

Rittinghouse, J. W., and Ransome, J. F. (2016). *Cloud computing: implementation, management, and security*: CRC press.

Rizvi, S. Z. R., and Fong, P. W. (2016). *Interoperability of Relationship-and Role-Based Access Control.* Paper presented at the Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, 231-242.

Samarati, P., and de Vimercati, S. C. (2000). *Access control: Policies, models, and mechanisms.* Paper presented at the International School on Foundations of Security Analysis and Design, 137-196.

Sandhu, R., and Munawer, Q. (1998). *How to do discretionary access control using roles.* Paper presented at the Proceedings of the third ACM workshop on Role-based access control, 47-54.

Sookhak, M., Yu, F. R., Khan, M. K., Xiang, Y., and Buyya, R. (2016). Attribute-based data access control in mobile cloud computing: Taxonomy and open issues. *Future Generation Computer Systems*.

Srinivsan, S. M., and Chaillah, C. (2014). Information Interpretation Code For Providing Secure Data Integrity On Multi-Server Cloud Infrastructure. *International Journal of Modern Education and Computer Science, 6*(12), 26.

Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11.

Sun, D., Zhao, H., and Cheng, S. (2017). A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS. *Security and Communication Networks*.

Sun, L., Wang, H., Yong, J., and Wu, G. (2012). *Semantic access control for cloud computing based on e-Healthcare.* Paper presented at the Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on, 512-518.

Takabi, H., Joshi, J. B., and Ahn, G.-J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8*(6), 24-31.

Tang, B., Li, Q., and Sandhu, R. (2013). *A multi-tenant RBAC model for collaborative cloud services.* Paper presented at the Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on, 229-238.

Thirunarayan, K., Anantharam, P., Henson, C., and Sheth, A. (2014). Comparative trust management with applications: Bayesian approaches emphasis. *Future Generation Computer Systems, 31,* 182-199.

Tsai, S.-C., Liu, I.-H., Lu, C.-T., Chang, C.-H., and Li, J.-S. (2017). *Defending cloud computing environment against the challenge of DDoS attacks based on software defined network.* Paper presented at the Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the

Twelfth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Nov., 21-23, 2016, Kaohsiung, Taiwan, Volume 1, 285-292.

Tupakula, U. K., Varadharajan, V., and Vuppala, S. K. (2009). *SBAC: Service based access control.* Paper presented at the Engineering of Complex Computer Systems, 2009 14th IEEE International Conference on, 202-209.

Wang, W., Han, J., Song, M., and Wang, X. (2011). *The design of a trust and role based access control model in cloud computing.* Paper presented at the Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on, 330-334.

Xu, M., Jiang, X., Sandhu, R., and Zhang, X. (2007). *Towards a VMM-based usage control framework for OS kernel integrity protection.* Paper presented at the Proceedings of the 12th ACM symposium on Access control models and technologies, 71-80.

Yadav, D. S., and Doke, K. (2016). Mobile Cloud Computing Issues and Solution Framework.

Yang, K., and Jia, X. (2014). DAC-MACS: Effective data access control for multi-authority cloud storage systems. In *Security for Cloud Storage Systems* (pp. 59-83): Springer.

Yin, K. Z., and Wang, H. H. (2015). *Mcacm: A cloud storage access control model for multi-clouds environment based on XACML.* Paper presented at the Applied Mechanics and Materials, 2451-2454.

Younis, Y. A., Kifayat, K., and Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications, 19*(1), 45-60.

Zhang, C.-x., Hu, Y.-x., and Zahng, G. (2006). Task-role based dual system access control model. *International Journal of Computer Science an Network Scurity, 6*, 211-215.

Zheng, Z., Wu, X., Zhang, Y., Lyu, M. R., and Wang, J. (2013). QoS ranking prediction for cloud services. *IEEE transactions on parallel and distributed systems, 24*(6), 1213-1222.

Zhou, Z., Wu, L., Hong, Z., Liang, Z., Jun, L., Sheng-Jun, X., et al. (2013a). Context-aware access control model for cloud computing. *International Journal of Grid and Distributed Computing, 6*(6), 1-12.

Zhou, Z., Wu, L., Hong, Z., Liang, Z., Jun, L., Sheng-Jun, X., et al. (2013b). Context-aware access control model for cloud computing. *International Journal of Grid and Distribution Computing, 6*(6), 1-12.