Website : jurnal.umj.ac.id/index.php/icecream

Attribute Based Access Control In Infrastructure As A Service Case Study

Dilawar Singh[1], Vikas Thada[2], Jaswinder Singh [3]
[1] Phd Scholar ASET, Amity University Gurugram, Haryana, India,
[2] Associate Professor ASET, Amity University, Gurugram, Haryana, India,
[3]Associate Professor DCSE, GJUST Hissar, Haryana, India
dilawar.yadav@gmail.com

ABSTRACT

Perhaps the main difficulties that have undermined cloud computing and caused its lethargic reception is security. Since clouds have assorted gatherings of clients with various arrangements of safety prerequisites, confining the clients' accesses and shielding data from unapproved accesses have become the most troublesome errands. To address these basic difficulties, in this paper initially formalize Attribute Based Access Control (ABAC) and propose another access control model, called Attribute-Rule ABAC (AR-ABAC), for cloud computing to meet basic access control necessities in clouds. Our model backings the attribute decides that arrangement with the relationship among clients and items, just as the capacity for accessing objects based on their affectability levels. The attribute- decides to indicate an understanding that figures out what sort of attributes ought to be utilized and the quantity of attributes considered for settling on access choices. Likewise, our model guarantees secure asset dividing between potential untrusted inhabitants and supports distinctive access consents to a similar client at a similar meeting.

Keywords—Cloud Computing, ABAC, Authorization and authentication.

1. Introduction

Although cloud computing brings many benefits, it may suffer from conventional distributed systems' security attacks Moreover, a cloud has brought new concerns such as moving resources and storing data in the cloud which may reside in another country that should fulfill different regulations. This paper focus on addressing access control issues in cloud Infrastructure-as-a-Service (IaaS). Access control is an essential mechanism that controls what operations the user may or may not be able to do. The basic goal of any access control system is to restrict a user to exactly what s/he should be able to do and protect information from unauthorized access. A robust access control model must cope with some basic issues due to the cloud computing nature, such as:

- Pooling the cloud resources to serve many users with different classifications that can handle diverse permissions associated with the same cloud user.
- Giving the user the ability to use multiple services with respect to authentication and login time.
- Transferring users' credentials across layers to access services and resources; and
- Using multi-tenancy where different resources are dynamically allocated and de-allocated on demand while the location of each resource is being unknown.

These realities unmistakably show the need of a viable access control model for cloud computing. Our inspiration is to formalize the Attribute-Based Access Control (ABAC) that obliges some uncommon destinations. It ought to be referenced that there is not generally acknowledged formal ABAC model as there are for DAC, MAC, and RBAC. It uses a

functioning ABAC definition expressed by NIST uncommon distribution 800-162 to express the formal ABAC definition. Additional proposal is another access control model for cloud computing based on the formal ABAC model, called Attribute Rule ABAC (AR-ABAC). AR-ABAC guarantees secure asset dividing between potential untrusted occupants and supports distinctive access authorizations to a similar client at a similar meeting. Likewise, our model is sufficiently adaptable to help a bunch of imperatives that address the fundamental necessities for the cloud access control model. At last, contrasted and existing cloud access control models, our model has sufficient adaptability to adapt to various access authorizations for a similar client.

Every one of the conventional access control models was proposed for a particular climate with a bunch of essential prerequisites:

Macintosh Model: Mandatory Access Control (MAC) model, where a focal authority oversees giving access choices to a client/subject mentioning access to objects. Macintosh gives assurance against data stream and aberrant data spillages yet doesn't ensure total mystery of the data. Likewise, this model is extravagant and hard to convey and doesn't uphold division of obligations, least advantage, and designation or legacy standards. Likewise, unique actuation of access rights for specific assignments isn't upheld. Also, it doesn't uphold time and area imperatives.

DAC Model: Discretionary Access Control (DAC) model awards the proprietors of items the capacity to limit access to their articles, or data in the articles based upon clients' characters or an enrollment in specific gatherings. DAC model is for the most part less secure than MAC model, so utilized in conditions don't need an undeniable degree of insurance DAC has many incidental effects when it is used in cloud computing, for instance, it doesn't can control data stream or manage Trojan ponies that can acquire access consents a client might pass her privileges to another client, and that can abuse the respectability and classification of items; lastly, it isn't adaptable enough for cloud computing.

Various leveled RBAC Model: Role-Based Access Control (RBAC) model is considered as a characteristic method to control access to assets in associations and undertakings. The inspiration driving RBAC comes from considering "a subject's liability is a higher priority than whom the subject is". RBAC neglects to adapt to the accompanying issues: the dynamic/irregular practices of clients; it likewise doesn't think about the time and area requirements; it doesn't uphold dynamic obligations as it doesn't separate errand’s structure jobs; it needs to manage an absence of refined semantic models to address and impart advantages; and prior to using the RBAC in cloud computing, it needs to guarantee allowing access choices in a sensible time.

ABAC Model: Attribute Based Access Control (ABAC) model depends on a bunch of attributes related with a requester or an asset to be accessed to settle on access choices. There are numerous approaches to characterize or utilize attributes in this model. An attribute can be a client's work start date, an area of a client, a job of a client, or every one of them. Attributes could conceivably be identified with one another. Nonetheless, agreeing about what sort of attributes ought to be utilized, and the number of attributes are considered for settling on access choices is a perplexing undertaking in cloud computing at long last, proposing a security strategy that can work precisely with the ABAC model is indispensable, on the grounds that the security strategy is answerable for choosing proper attributes that are used to settle on right access choices.

Hazard BAC Model: Risk-Based Access Control (R-BAC) was proposed by Brucker et al. to adapt to global associations that face different sorts of strategies and guidelines. R-BAC utilizes various types of hazard levels with natural conditions and uses the rule of "functional need" to settle on access choices. In any case, R-BAC is hard to be conveyed in cloud computing as a result of the measure of investigation required and the quantity of frameworks to be converged to register hazard levels. It needs ability that can manage the model effectively. At long last, security approaches and ecological conditions should be normalized as they assume a urgent part on settling on access choices.

With the development of large distributed systems attribute based access control (ABAC) has become increasingly important. According to the NIST "ABAC is an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions Attribute Based Encryption (ABE) is category of ABAC. ABE proposed to support fine- grained access control ABE can be viewed as an extension of Identity Based Encryption system. IBE has resolving the problem public key sharing in which an arbitrary string can be used as a public key (email, IP Address, phone number phone…).

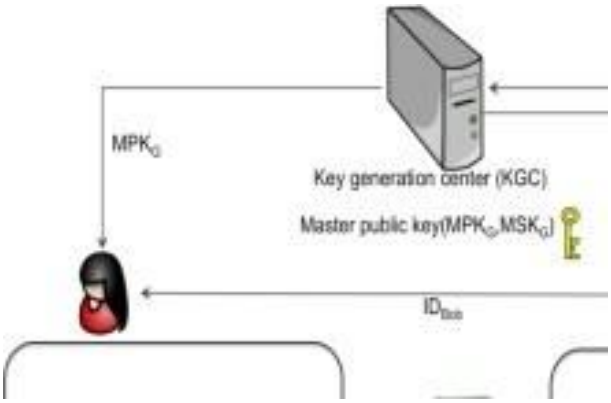
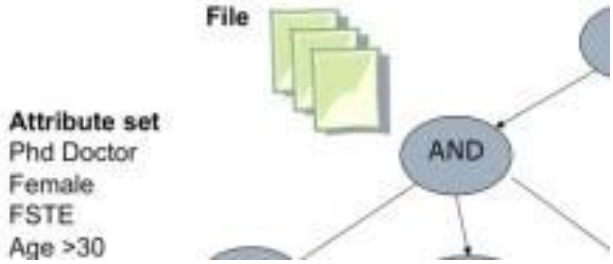


Figure 1: Identity Based Encryption system

Contrasted and IBE in which, encoded information is focused on for unscrambling by single known client, in ABE framework, the client's personality is summed up to a bunch of clear attributes rather than a solitary string determining the character of the client. Contrasted and the character- based encryption, ABE enjoys a significant benefit since it makes a more adaptable encryption rather than one-on-one; it is viewed as a promising device to tackle the safe information sharing issue grained and decentralized access control. ABE is utilized in different applications, as Electronic Health records the executives (HER), and PHR (Personal Health Records). In the ABE framework the unscrambling key ought to be matched with the attributes of code text and the key will decode the code text. The private



keys are developed by the Access tree as in ABE frameworkroot hub.

Figure 2: ABE scheme

The cloud computing framework the single position will not be ready to control the various attributes for every client and all access rights, to resolve this issue for single power ABE, the multi-ABE framework is presented Because of this necessity the ABE framework has been separated into two classes of multi authority ABE framework: KP-ABE and CP-ABE.

2. LITERATURE REVIEW

Jaydip Sen (2012) Cloud computing changes the way data innovation (IT) is devoured and overseen, promising worked on cost efficiencies, sped up advancement, quicker an ideal opportunity to-showcase, and the capacity to scale applications on request (Leighton, 2009). As per Gartner, while the promotion developed dramatically during 2008 and proceeded since, plainly there is a significant shift towards the cloud computing model and that the advantages might be considerable (Gartner Hype-Cycle, 2012). Notwithstanding, as the state of the cloud computing is arising and growing quickly both adroitly and truly, the lawful/authoritative, monetary, administration quality, interoperability, security and protection gives present critical difficulties. In this section, we portray different assistance and arrangement models of cloud computing and distinguish significant difficulties. Specifically, we talk about three basic difficulties: administrative, security and protection issues in cloud computing. A few answers for moderate these difficulties are additionally proposed alongside a short show on the future patterns in cloud computing organization.

G.- J. Ahn and R. S. Sandhu. (2013) Cloud computing alludes to accessing, arranging and controlling the assets (like programming and equipment) at a far-off area (Patidar et al., 2012). Buyya et al. (2009) characterized the Cloud computing as far as conveyed computing "A Cloud is a sort of equal and circulated framework containing a bunch of interconnected and virtualized PCs that are progressively provisioned and introduced as at least one bound together computing assets based on assistance level arrangements set up through exchange between the specialist co-op and shoppers".

M. Al-Kahtani and R. Sandhu (2014) the principal classification is hypothetical access control models. Job based trust the board (RT) gives a bunch of job task qualifications. The lone attribute is job, and the approval strategy is equivalent to that in job-based access control and isn't configurable. Strategy Machine (PM) is proposed to give a bound together structure to help a wide scope of attribute-based strategies or strategy blends through a solitary system that requires changes just in its information design. The National Institute of Standards and Technology (NIST) as of late delivered a first draft ABAC model This draft gives itemized rules in different parts of big business ABAC while no proper model is given. The UCON use control model spotlights on use control where approvals are based on the attributes of the elaborate parts. It is attribute-based in any case, as opposed to managing center ABAC ideas, it centers around cutting-edge access control elements like impermanent attributes, persistent authorization, commitments and conditions.

R. Ausanka-Crues (2015) UCON pretty much accepts that an ABAC model is set up on top of which the UCON model is developed. Models' approval strategy of access control utilizing rationale programming with set limitations of a calculable set hypothesis Additionally with UCON, this work centers just around one part in ABAC which is approval It is based with the understanding that clients and articles are related with sets of attributes.

D. Ringer and L. LaPadula(2016) the subsequent classification is on approval strategy detail dialects. SecPAL has a substantial punctuation comprising of straightforward articulations near normal language. DYNPAL and SMP empower determining adjustments to the framework state in approval. Proposes to determine approval strategies utilizing set hypothesis to guarantee consistency and fulfillment

Binder is an expansion to the datalog sensible programming language. In Soutei strategies and qualifications are written in an explanatory rationale-based security language. Proposes a proper system based on C-Datalog language. Rule-based arrangement determination empowers approval strategy detail based on framework conduct. Different models are SPKI/SDSI extensible access control markup language (XACML) and venture security approval language (EPAL) There has been impressive exploration based on XACML. Improves on XACML strategies by giving a cosmology-based attribute the executive's office Different models are strategy combination strategy assessment conformance checking and strategy determination Xu et al [2012] propose approval strategy mining. Policy Morth proposes a structure to help intuitive ABAC strategy determination and upkeep. In outline, every one of these work centers around how approval strategy can be indicated and assessed. While approval strategy is a significant segment of ABAC, these creators don't present far reaching formal models for ABAC.

The third classification is about worries on requirement of ABAC frameworks. This class manages issues like how to address, store, move and validate attributes. In certification- based access control attribute declarations of subject and climate are encoded in evident advanced accreditations gave by confided in outsider certifiers. Shows that ABAC can be utilized as an essential approval and validation component for inheritance or present-day venture frameworks, yet it is based distinctly on RT model. Akenti [2013] is an approval administration based on X.509. Data correspondence between administration requester and specialist co-op are examined. Policymaker proposes a way to deal with trust the executives. Featured discussion and SPKI/SDSIuse accreditations to assign authorizations. Mechanized trust exchange manages accreditation exposure before approval assessment. Presents an effective convention that secures both delicate accreditations and arrangements Manage security worries in requester attribute discharge. Examines general ABAC execution design for web administration. Albeit these works give devices to upholding ABAC, they don't present the full image of hypothetical part of ABAC like subject and client differentiation.

F. Cruz, R. Gjomemo, B. Lin, and M. Orsini (2015) the fourth classification is attribute based encryption (ABE). It is proposed to help fine-grained sharing of encoded information. In this sort of frameworks, figure writings are marked with sets of attributes and private keys are related with access structures. The unscrambling of a ciphertext hence is conceivable just if the arrangement of attributes of the client key matches the attributes of the ciphertext. considered unscrambling when essentially k attributes cross- over between a code text and a private key. Key-Policy Attribute-Based Encryption (KP-ABE) stretches out the above work to relate strategy tree rather than arrangements of attributes with private keys. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) then again empowers encryptor to relate strategy trees with figure text broadens KP-ABE so private keys can address non-droning access recipe over attributes.

S. Harris. Mike (2016) Firstly, we acquaint the connected work with client attribute organization model. There is exceptionally predetermined number of models proposed for this reason. Nonetheless, we track down that the regulatory model for client job task is profoundly related. Regulatory job-based access control (ARBAC97) oversees client job task, consent job task and job order for RBAC. The significant idea for client job task is that clients should be recently allocated to specific jobs to get new jobs. Job based trust the board characterizes qualifications for appointing client job task to outsiders to help circulated client job task. Nonetheless, these work center around a solitary attribute which is job and the association between attributes of a similar client isn't covered.

L. Sun, H. Wang, J. (2017) Yong Secondly, we present the connected work for reachability examination for client attributes. The nearest classification of this work is the job reachability investigation on the job based managerial model ARBAC97. Li et al [2011] introduced calculations and intricacy results for investigation of two confined adaptations of ARBAC97–AATU and AAR. Be that as it may, this work didn't think about regrettable preconditions. Sasturkar et al [124] and Jha et al [76] introduced calculations and intricacy results for investigation of ARBAC strategies subject to an assortment of limitations on how the arrangement can be determined. Stoller et al [129] proposed the main fixed-boundary manageable calculation for examining ARBAC arrangements. In any case, the calculation just applies to rules with one sure precondition and genuine job denial. Stoller et al [2010] investigated security on defined RBAC and ARBAC97. Albeit the boundaries of job can be considered as client attributes, all boundaries are treated as nuclear esteemed and are just changed along with the adjustment of job. Comparable works are which introduced representative investigation for attribute RBAC models. Our work is on a very basic level unique in relation to these regarding organization of various attributes including nuclear esteemed attributes, though the ARBAC97 investigation just arrangements with a solitary set-esteemed attribute called job. The subsequent class is strategy examination in attribute-based models. Gupta et al [2013] proposed rule-based regulatory approach model that controls expansion and expulsion of the two guidelines and realities, and a representative investigation calculation for noting reachability inquiries. Current realities of clients might be named as attributes. In any case, the model doesn't recognize nuclear and set esteemed attributes and the current rendition of the calculation is fragmented.

Li et al [2014] examined security investigation in job based trust the executives (RT). It is not quite the same as our work in that the attention is on designation and trust. Likewise, just one attribute, for example job, is thought of. Jajodia et al [2014] proposed an arrangement language to communicate positive and negative approvals and determined approvals, and they give polynomial-time calculations to check consistency and culmination of a strategy. Told the best way to wipe out approach mis-arrangements utilizing information mining. Introduced security imperative examples for demonstrating security framework design and confirming whether required security limitations are accurately authorized. Nonetheless, this structure works with plan and arrangement of safety polices instead of run-time security examination.

3. ATTRIBUTE BASED ACCESS CONTROL IN CLOUD IAAS aa

As a rule, limitations are a significant and incredible instrument for spreading out more

elevated level security approaches. For example, in an association, imperatives can determine more significant level strategies to put limitation on the conduct of its representatives, for example, partition of obligation requirements in job-based access control whereby a specific worker can't take both 'software engineer' and 'analyzer' jobs for a similar undertaking. Such an imperative in the end keeps the worker from at the same time chipping away at both creating and testing code for same undertaking. In this thesis, we foster requirements detail in attribute-based access control (ABAC) and cloud framework as-a-administration (IaaS). Generally, ABAC manages consents of clients or subjects to access framework assets powerfully based on related approval rules with a specific authorization.

L. Sun, H. Wang, J. (2014) Yong A client can practice a consent on an item if the attributes of the client's subject and the article have an arrangement fulfilling the approval decide determined for that authorization. Henceforth, appropriate task of attribute esteems (or basically attribute task) to these elements is critically significant in an ABAC framework for forestalling accidental accesses. In this exposition, we center on imperatives determination as a significant level arrangement particular on attributes task to elements in an ABAC based framework as a component to figure out which substance ought to get which attribute esteems. By elements, we allude to clients, subjects and articles, which are normal in access control frameworks. A client is a deliberation of a person. A subject is a launch of a client and can allude to a specific meeting similar as in job- based access control (RBAC) and an item is an asset in the framework. While ABAC is strategy nonpartisan, it is additionally mind boggling to oversee since its access the executives relies upon approval controls as well as allocated attributes to the elements. Forcing requirement child attribute esteem tasks can relieve this intricacy by forcing midway planned and arranged limitations on the decentralized interaction by which explicit attribute esteems are allocated to singular substances.

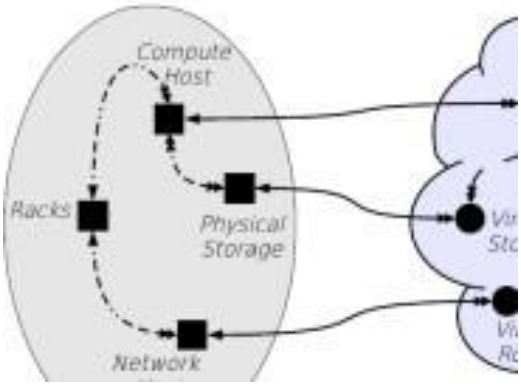


Figure 3: Cloud Resources Mapping Relation

Wang et al (2012) in 2004 proposed a construction that models an ABAC structure using reasoning programming with set necessities of a measurable set theory. Referencing distant organizations in a person less open structure requires that plans of attributes be acquainted with procure accesses to resources. To do accordingly, they propose a characterized reasoning programming-based framework to show ABAC plans where varieties of attribute and organization options are shown as sets in a measurable hereditarily restricted set speculation. Their systems are sans failure, consistent and complete. To update runtime execution, they change ABAC polices so that adjusted techniques have the comparable runtimes as executing seemed rules. Their ceaseless work examines other processable set theories and successful executions.

Access Control Approach for Cloud IaaS

L. Sun, H. Wang, J. Yong (2016) the customers who team up with cloud IaaS in an organization or administrative breaking point

are arranged into different sorts (showed in four ovals in figure 2). A cloud root customer is a customer who manages cloud resources for the CSP. For straightforwardness of show we expect there is a single all- fantastic cloud root customer who is portrayed as doing various limits. Eventually numerous components of the cloud root customer would be robotized and set off by liability of portion, with respect to oneself help on-demand perspective.

L. Sun, H. Wang, J. (2012) Yong on the occupant side, we have there three kinds of IT customers. By IT customer we mean a customer in an affiliation that gives IT support to that affiliation. An occupant root customer tends to an IT customer who has root access to the inhabitant. For straightforwardness of show, we acknowledge that for every tenant, there is only one root customer who has full assents in the occupant. The inhabitant root customer is made by the cloud root customer. A tenant director customer tends to a definitive IT customer with administrative approvals in the occupant. Legitimate approvals license the leaders of standard IT customers (discussed under) and their attributes in an occupant. A tenant common customer is a typical IT customer with approvals for standard IT errands, for instance, making and deleting virtual machines, storing volumes, associations, etc, for the good of the occupant. Note that in figure 2 an administrative model is imperative to coordinate the L. Sun, H. Wang, J. Yong endeavors of occupant root and administrative IT customers while a useful model is fundamental for managing the tasks of normal IT customers. The administrative model works with making and reviving attributes while the utilitarian model works with demonstrating endorsement moves toward that control the exercises of common IT customers. We stress that non-IT customers of a tenant who simply interface with the cloud for using the VMs and various organizations are not considered in figure 2. They don't manage any cloud IaaS resources and are controlled by access control frameworks inside the VMs and inside applications running in VMs.

Bonatti, Clemente Galdi (2010) An enhanced expansive collaboration for a relationship to move to cloud is according to the accompanying. To use cloud benefits, the underlying advance is that an affiliation's representative (say Alice) gets a record from the CSP normally through some modernized cycle which is an intermediary for the cloud root customer. In this manner the affiliation transforms into a tenant of the CSP with Alice as that occupant's root customer. As of now it isn't realistic for Alice to make and manage all of the resources herself. Taking everything into account, in the second step Alice sets up occupant unequivocal access control and administrative game plans using the CSP-gave workplaces and makes some number of tenant chairman customers. Then, the occupant manager customers make standard IT customers and deal with their attributes. Finally, standard IT customers would then have the option to make and direct virtual resources as per the game plans showed by the occupant root customer and attribute regards oversaw by tenant overseer customers.

4. CONCLUSION

In this paper, we have given the conventional meaning of ABAC model that obliges some exceptional goals. We likewise have proposed another access control model for cloud computing based on ABAC model, supporting attribute rule called Attribute-Rule ABAC (AR-ABAC). AR- ABAC can satisfy a bunch of obligatory prerequisites for different access control models being conveyed in cloud computing, particularly cloud IaaS, as closed here The trial results have shown that AR-ABAC is reasonable for cloud IaaS, where the

normal time for token age in Keystone including 24 attributes is expanded with about 25% more than including zero attributes. Consequently the increment isn't critical. Additionally, the normal time for Nova imparting the AR-ABAC strategy motor increments by expanding the quantity of attributes just as by expanding the quantity of simultaneous solicitations at similar number of attributes At last, AR-ABAC can satisfy the fundamental and obligatory access control necessities, which are needed for any access control model that will be executed in cloud computing. As our future work, we will coordinate our proposed model with the Neutron administration and other Open Stack administrations, based on the genuine private cloud climate.

5. REFERENCES

1. G.-J. Ahn. The Rcl 2000 Language for Specifying Role-based Authorization Constraints. PhD thesis, Fairfax, VA, USA, 2000.

2. G.-J. Ahn and R. S. Sandhu. Role-based authorization constraints specification. ACM Transactions on Information and System Security (TISSEC), 3(4):207–226, November 2000.

3. M. Al-Kahtani and R. Sandhu. A model for attribute-based user-role assignment. In 18th Annual Computer Security Applications Conference, 2002. Proceedings, pages 353–362, 2002.

4. R. Ausanka-Crues. Methods for access control: advances and limitations. Harvey Mudd College; 2004. Retrieved December 07, 2012.

5. D. Bell and L. LaPadula. Secure computer systems: mathematical foundations. Bedford, MA. Retrieved February 04, 2013, from: Secure computer systems: mathematical foundations; 1973.

6. D. Brucker, L. Br ¨ugger, P. Kearney, and B. Wolffy. An approach to modular and testable security models of real-world health-care applications. In SACMAT'11. Proceedings of the 16th ACM symposium on Access Control Models and Technologies, pages 133–142. SACMAT, 2011.

7. F. Cruz, R. Gjomemo, B. Lin, and M. Orsini. Collaborative Computing Networking, Applications and Worksharing, volume 10 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, chapter A Constraint and Attribute Based Security Framework for Dynamic Role Assignment in Collaborative Environments, pages 322–339. Springer Berlin Heidelberg, 2009.

8. S. Harris. Mike meyers cissp(r) certification passport. first edition. United States: McGraw-Hill, page 422, 2002.

9. V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. Guide to attribute-based access control (abac) definition and considerations. Special Publication 800-162, U.S. Department of Commerce, January 2014. National Institute of Standards and Technology.

10. L. Sun, H. Wang, J. Yong, and G. Wu. Semantic access control for cloud computing based on e-healthcare. In 16th International Conference on: Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE, pages 512–518, May 2012.

11. Z. Tianyi, L. Weidong, and S. Jiaxing. An efficient role-based access control system for cloud computing. In 11th International Conference on: Computer and Information Technology (CIT), 2011 IEEE, pages 97–102, Augest 2011.

12. Elisa Bertino, Barbara Catania, Elena Ferrari, and Paolo Perlasca. A logical framework for reasoning about access control models. ACM Trans. Inf. Syst. Secur., 2003.

13. Elisa Bertino, Elena Ferrari, and Vijay Atluri. The specification and enforcement of authorization constraints in workflow management systems. ACM TISSE, 1999.

14. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In IEEE SP'07, pages 321–334, 2007.

15. Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D Keromytis. The role of trust management in distributed systems security. In Secure Internet Programming, pages 185– 210. Springer, 1999.

16. Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In 1996 IEEE

Symposium on Security and Privacy, pages 164–173. IEEE, 1996.

17. Bonatti, Clemente Galdi, and Davide Torres. ERBAC: Event-driven RBAC. In ACM SACMAT, pages 125–136, 2013.

18. Piero A. Bonatti and P. Samarati. Regulating service access and information release on the web. In ACM CCS, 2000.

19. Piero A. Bonatti and P. Samarati. A uniform framework for regulating service access and information release on the web. J. Comp. Secur., 2002.

20. T. Bylander. The computational complexity of propositional STRIPS planning. Artificial Intelligence, pages 165–204, 1994.